



# Combating money laundering and the financing of terrorism

Home > Financial oversight > Combating money laundering and the financing of terrorism

Communication NBB\_2020\_14 / Communication COVID-19

Communication NBB\_2018\_04 / New section "Combating money laundering and the financing of terrorism" on the website

Tree structure of the AML/CFT website

## Introduction

## Scope

## Definitions

## Risk-based approach and overall risk assessment

## Organisation and internal control

Organisation and internal control in financial institutions

Organisation and internal control in groups

Performance of obligations by third parties

Brexit

## Customer and transaction due diligence

Individual risk assessment

Anonymous or numbered accounts and contracts

Identification and identity verification

Identification of the customer's characteristics and of the purpose and nature of the business relationship or the occasional transaction

Ongoing due diligence and detection of atypical facts and transactions

Special cases of enhanced due diligence

Due diligence requirements and compliance with other legislation

## **Analysis of atypical transactions and reporting of suspicions**

Analysis of atypical facts and transactions

Reporting of suspicions

Prohibition of disclosure

Protection of reporting entities

## **Transfers of funds**

## **Financial embargoes and assets freezing**

## **Retention and protection of data and documents**

## **Restriction of the use of cash**

## **Supervision by the NBB**

Reporting by financial institutions

External whistleblowing

Supervisory powers and measures of the NBB

National cooperation

International cooperation

## **Sanctions**

Administrative sanctions

Criminal sanctions

## **Useful links and documents**

Main reference documents

Other useful links

Successive versions of the AML/CFT website

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



# Introduction

Home > Financial oversight > Combating money laundering and the financing of terrori...

## Contents

- Background
- Objectives
- Methodology

## Background

In recent years, the preventive framework for combating money laundering and terrorist financing (“AML/CFT”) has undergone significant developments at the international, European and Belgian level.

The main developments are related to the publication:

- of the International Standards of the Financial Action Task Force (“FATF”) on combating money laundering and the financing of terrorism and proliferation, revised in February 2012 (“the 40 FATF recommendations”);
- of the fourth AML/CFT Directive, i.e. Directive (EU) 2015/849 of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (“Directive 2015/849”);
- of the Law of 18 September 2017 on the prevention of money laundering and terrorist financing and on the restriction of the use of cash (“the Anti-Money Laundering Law”), which transposes the aforementioned Directive 2015/849;
- of the Regulation of the National Bank of Belgium (“NBB”) of 21 November 2017 on the prevention of money laundering and terrorist financing, which is applicable to the Belgian financial institutions falling under its supervisory competence (“the Anti-Money Laundering Regulation of the NBB”);

and of the mutual evaluation of Belgium by the FATF in 2014 and 2015.

Please refer to the Explanatory Memorandum of the Anti-Money Laundering Law (general explanation) for an overview of the key changes introduced by the revision in 2012 of the 40 FATF recommendations and by Directive 2015/849 to the European AML/CFT framework, as well as to the results of the evaluation of Belgium by the FATF.

## Objectives

This section of the website of the NBB (“AML/CFT website”) has two objectives:

- i. collecting all relevant AML/CFT texts (the Law, regulations, preparatory work, European and international guidelines, etc.) and grouping them by topic in order to provide financial institutions falling under the competence of the NBB and the public with complete, accessible and regularly updated information on the legal and regulatory AML/CFT obligations of these financial institutions;

- ii. specifying any additional comments and recommendations from the NBB for a correct and effective implementation of the provisions of the Anti-Money Laundering Law and Regulation by these financial institutions. In this context, it replaces Circular CBFA\_2010\_09 of 6 April 2010 on customer due diligence, preventing the use of the financial system for the purposes of money laundering and terrorist financing and preventing the financing of arms proliferation (**fully repealed on 21 December 2018**).

## Methodology

The structure of the AML/CFT website follows that of the Anti-Money Laundering Law as closely as possible

Each page starts with references to the parts of the Anti-Money Laundering Law, of the Anti-Money Laundering Regulation of the NBB and of the Explanatory Memorandum of the Anti-Money Laundering Law that are relevant to financial institutions falling under the supervisory competence of the NBB, as well as to the Belgian, European and international reference documents on the relevant topic, followed by any additional comments and recommendations from the NBB. **It should be noted that the Explanatory Memorandum of the Anti-Money Laundering Law already contains numerous specifications on the manner in which the provisions of the said Law should be interpreted to be implemented effectively. Financial institutions are therefore strongly urged to consult this explanatory memorandum, whether or not it is completed by comments and/or recommendations from the NBB.** For commentary on the provisions of the Anti-Money Laundering Law that are not relevant to financial institutions falling under the supervisory competence of the NBB, please refer to the full text of the explanatory memorandum of this Law, which is available under the “Main reference documents” tab, which also contains other useful documents.

The AML/CFT website was developed in multiple stages. At its launch, it contained at least, for each topic covered, the information listed in point (i) of the objectives described above. Subsequently, the NBB gradually completed the information provided by including any comments and recommendations for the effective implementation of the legal and regulatory obligations (point (ii) of the objectives described above). In addition, it will update this website whenever it deems it necessary, particularly to take into account the evolution of the standards and recommendations of the international bodies competent with regard to AML/CFT, of the European and national legal and regulatory framework, of the interpretation of the rules applicable, etc. An overview of the updates to the website and an archive of its successive versions is available under the “Successive versions of the AML/CFT website” tab at the bottom of the website’s homepage.

**Insofar as necessary, attention is drawn to the fact that the NBB’s approach – i.e. having collected all relevant texts (law, regulations, preparatory work, European and international guidelines, etc.) applicable with regard to AML/CFT (see the first objective of this website above), in addition to its own comments and recommendations, on this AML/CFT website – is purely educational and informative in nature. As a result, any lack of updates or later updates to one of those texts included on this website are without prejudice to its applicability to financial institutions.**

It should also be recalled, where necessary, that other policy documents not covered in the context of this AML/CFT website may be relevant and applicable (notably regarding audit, shareholder structure, governance, outsourcing, etc.). Moreover, this website is without prejudice to the competences of the other authorities that are competent with regard to AML/CFT (CTIF/CFI, FSMA, Treasury, FPS Economy, etc.).

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



## Scope

Home > Financial oversight > Combating money laundering and the financing of terrori...

**This AML/CFT website is intended for the entities which fall under the supervisory competence of the NBB and which are referred to in Article 5, § 1, 4° to 10° of the Anti-Money Laundering Law and in Article 2 of the Anti-Money Laundering Regulation of the NBB. These institutions, which are collectively referred to as 'financial institutions' on this website, include:**

1. a) credit institutions as referred to in Article 1, § 3, first paragraph, of the Law of 25 April 2014 on the legal status and supervision of credit institutions and stockbroking firms, which are governed by Belgian law;  
b) branches in Belgium of credit institutions as referred to in Article 1, § 3, first paragraph, of the same law, which are governed by the law of another Member State or of a third country;  
c) credit institutions as referred to in Article 1, § 3, first paragraph, of the same Law, which are governed by the law of another Member State and rely on a tied agent established in Belgium in order to perform investment services and/or activities within the meaning of Article 2, 1°, of the Law of 25 October 2016 on access to the activity of investment services and on the legal status and supervision of portfolio management and investment advice companies as well as ancillary services within the meaning of Article 2, 2°, of the same Law in Belgium;
2. a) insurance companies governed by Belgian law as referred to in Book II of the Law of 13 March 2016 on the legal status and supervision of insurance or reinsurance companies, which are authorised to engage in the life insurance activities referred to in Annex II of the same Law;  
b) branches in Belgium of insurance companies governed by the law of another Member State or of a third country, as referred to, respectively, in Articles 550 and 584 of the same Law, which are authorised to engage in the life insurance activities referred to in Annex II of the same Law in Belgium;
3. a) payment institutions governed by Belgian law as referred to in Book 2, Chapter 1, Title 2 of the Law of 21 December 2009 on the legal status of payment institutions and electronic money institutions, access to the activity of payment service provider, access to the activity of issuing electronic money, and access to payment systems;  
b) branches in Belgium of payment institutions governed by the law of another Member State or of a third country, as referred to, respectively, in Articles 39 and 46 of the same Law;  
c) payment institutions granted exemption under Article 48 of the same Law;  
d) payment institutions as referred to in Article 4(4) of Directive 2015/2366/EU of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, governed by the law of another Member State and offering payment services in Belgium through one or more persons established in Belgium who represent the institution for that purpose;
4. a) electronic money issuers as referred to in Article 59, 4° and 5° of the aforementioned Law of 21 December 2009;  
b) electronic money institutions governed by Belgian law as referred to in Book 3, Chapter 1, Title 2, of the same Law;  
c) branches in Belgium of electronic money institutions governed by the law of another Member State or of a third country as referred to, respectively, in Article 91 and in Book 3, Chapter 3, Title 2 of the same Law;  
d) electronic money institutions granted exemption under Article 105 of the same Law;  
e) electronic money institutions as referred to in Article 2(1) of Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC, governed by the law of another Member State and distributing electronic

money in Belgium through one or more persons established in Belgium who represent the institution for that purpose;

5. settlement institutions as referred to in Article 36/26, § 1, 3° and 4° of the Law of 22 February 1998 establishing the organic statute of the National Bank of Belgium;
6. central securities depositories as defined in Article 36/26/1 of the Law of 22 February 1998 establishing the organic statute of the National Bank of Belgium;
7. mutual guarantee societies as referred to in the Royal Decree of 30 April 1999 on the legal status and supervision of mutual guarantee societies;
8. a) stockbroking firms as referred to in Article 1, § 3, second paragraph, of the Law of 25 April 2014 on the legal status and supervision of credit institutions and stockbroking firms governed by Belgian law;  
b) branches in Belgium of stockbroking firms as referred to in Article 1, § 3, second paragraph, of the same Law which are governed by the law of another Member State or of a third country;  
c) stockbroking firms as referred to in Article 1, § 3, second paragraph, of the same Law, which are governed by the law of another Member State and rely on a tied agent established in Belgium in order to perform investment services and/or activities within the meaning of Article 2, 1°, of the Law of 25 October 2016 on access to the activity of investment services and on the legal status and supervision of portfolio management and investment advice companies as well as ancillary services within the meaning of Article 2, 2°, of the same Law in Belgium.

For the financial institutions for which this website is intended, the applicability of the Law and of the Anti-Money Laundering Regulation of the NBB and the scope of this AML/CFT website are determined by two factors:

- the **nature of the professional activity** exercised by the entity concerned;
- the **establishment on Belgian territory**.

It follows from the principle of territorial application of the legal and regulatory AML/CFT provisions that the provisions of the Law and of the Anti-Money Laundering Regulation of the NBB apply to and that this AML/CFT website concerns the following entities:

- financial institutions governed by Belgian law;
- financial institutions governed by the law of another EEA Member State or of a third country and established on Belgian territory in order to offer financial services or products in Belgium, irrespective of whether that establishment takes the form of:
  - a branch in Belgium;
  - one or more tied or independent agents or distributors established in Belgium who act in the framework of agency contracts with the financial institution, that does not itself have another form of establishment on Belgian territory. This covers (i) credit institutions and stockbroking firms which are governed by the law of another EEA Member State and rely on a tied agent established in Belgium in order to perform investment services and/or activities, and (ii) payment institutions and electronic money institutions governed by the law of another EEA Member State or of a third country and respectively offering payment services or distributing electronic money in Belgium exclusively through agents or distributors.

The financial institutions governed by the law of another EEA Member State or of a third country that offer financial services or products in Belgium without having any form of establishment in Belgium, are however subject to the legal and regulatory provisions of the country by whose law they are governed and of the other countries in which they may have an establishment. The provisions of the Law and the Anti-Money Laundering Regulation of the NBB do not apply to them and a fortiori they do not belong to the target group of this website.

For more information on the general scope of the Anti-Money Laundering Law, see the comments in the Explanatory Memorandum of Article 5 of the Anti-Money Laundering Law.

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



# Anti-Money Laundering Law of 18 September 2017 - Article 5

## Art. 5

§1. The provisions of this Law shall apply to the following obliged entities, acting in the exercise of their professional activities:

1° the National Bank of Belgium;

2° [...]

*§ 1, 2° repealed by Article 111, 1° of the Law of 30 July 2018 – Belgian Official Gazette of 10 August 2018;*

3° the limited company under public law bpost, hereinafter referred to as “bpost”, for its postal financial services or for the issuance of electronic money;

4° a) credit institutions as defined in Article 1, § 3, first subparagraph, of the Law of 25 April 2014 on the legal status and supervision of credit institutions and stockbroking firms, which are governed by Belgian law;

b) branches in Belgium of credit institutions as defined in Article 1, § 3, first subparagraph, of the same Law, which are governed by the law of another Member State or of a third country;

[c) credit institutions as referred to in Article 1, § 3, first subparagraph, of the same Law, which are governed by the law of another Member State and rely on a tied agent established in Belgium in order to perform investment services and/or activities within the meaning of Article 2, 1°, of the Law of 25 October 2016 on access to the activity of investment services and on the legal status and supervision of portfolio management and investment advice companies as well as ancillary services within the meaning of Article 2, 2°, of the same Law, in Belgium;]

*§ 1, 4°, c) inserted by Article 111, 2° of the Law of 30 July 2018 – Belgian Official Gazette of 10 August 2018*

5° a) insurance companies governed by Belgian law as referred to in Book II of the Law of 13 March 2016 on the legal status and supervision of insurance or reinsurance companies, which are authorised to engage in the life insurance activities referred to in Annex II of the same Law;

b) branches in Belgium of insurance companies governed by the law of another Member State or of a third country, as referred to, respectively, in Articles 550 and 584 of the same Law, which are authorised to engage in the life insurance activities referred to in Annex II of the same Law in Belgium;

[6° a) payment institutions governed by Belgian law as referred to in Book II, Title II, Chapter 1 of the Law of 11 March 2018 on the legal status and supervision of payment institutions and electronic money institutions, access to the activity of payment service provider and to the activity of issuing electronic money, and access to payment systems;

b) branches in Belgium of payment institutions governed by the law of another Member State or of a third country, as referred to, respectively, in Articles 120 and 144 of the same Law;

c) registered payment institutions as referred to in Book II, Title II, Chapter 2 of the same Law;

d) payment institutions as referred to in point (4) of Article 4 of Directive 2015/2366/EU of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, governed by the law of another Member State and offering payment services in Belgium through one or more persons established in Belgium who represent the institution for that purpose;]

*§ 1, 6° replaced by Article 101 of the Law of 2 May 2019 – Belgian Official Gazette of 21 May 2019*

[7° a) electronic money issuers as referred to in Article 163, 4° and 5° of the aforementioned Law of 11 March 2018;

b) electronic money institutions governed by Belgian law as referred to in Book IV, Title II, Chapter 1 of the same Law;

c) branches in Belgium of electronic money institutions governed by the law of another Member State or of a third country as referred to, respectively, in Articles 218 and 228 of the same Law;

d) limited electronic money institutions as referred to in Article 201 of the same Law;

e) electronic money institutions as referred to in point 1 of Article 2 of Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC, governed by the law of another Member State and distributing electronic money in Belgium through one or more persons established in Belgium who represent the institution for that purpose;]

*§ 1, 7° replaced by Article 101 of the Law of 2 May 2019 – Belgian Official Gazette of 21 May 2019*

8° [settlement institutions as referred to in Article 36/26, § 1, 3° and 4° of the Law of 22 February 1998 establishing the organic statute of the National Bank of Belgium;]

*§ 1, 8° repealed by Article 111, 3° of the Law of 30 July 2018 – Belgian Official Gazette of 10 August 2018 (entry into force on the date set by the King and no later than 1 January 2020)*

[8°/1 central securities depositories as defined in Article 36/26/1 of the Law of 22 February 1998 establishing the organic statute of the National Bank of Belgium;]

*§ 1, 8°/1 inserted by Article 111, 4° of the Law of 30 July 2018 – Belgian Official Gazette of 10 August 2018*

9° mutual guarantee societies as referred to in the Royal Decree of 30 April 1999 on the legal status and supervision of mutual guarantee societies;

10° a) stockbroking firms as referred to in Article 1, § 3, second subparagraph, of the Law of 25 April 2014 on the legal status and supervision of credit institutions and stockbroking firms which are governed by Belgian law;

b) branches in Belgium of stockbroking firms as referred to in Article 1, § 3, second subparagraph, of the same Law which are governed by the law of another Member State or of a third country;

[c) stockbroking firms as referred to in Article 1, § 3, second subparagraph, of the same Law, which are governed by the law of another Member State and rely on a tied agent established in Belgium in order to perform investment services and/or activities within the meaning of Article 2, 1°, of the Law of 25 October 2016 on access to the activity of investment services and on the legal status and supervision of portfolio management and investment advice companies as well as ancillary services within the meaning of Article 2, 2°, of the same Law, in Belgium;]

*§ 1, 10°, c) inserted by Article 111, 5° of the Law of 30 July 2018 – Belgian Official Gazette of 10 August 2018*

11° a) investment firms governed by Belgian law which are authorised as portfolio management and investment advice companies within the meaning of Article 6, § 1, 2° of the Law of 25 October 2016 on access to the activity of investment services and on the legal status and supervision of portfolio management and investment advice companies;

b) branches in Belgium of foreign portfolio management and investment advice companies governed by the law of another Member State as referred to in Article 70 of the same Law and branches in Belgium of foreign portfolio management and investment advice companies governed by the law of a third country as referred to in Title III, Chapter II, Section III of the same Law;

12° a) management companies of undertakings for collective investment governed by Belgian law as referred to in Part 3, Book 2 of the Law of 3 August 2012 on undertakings for collective investment which satisfy the conditions laid down in Directive 2009/65/EC and institutions for investments in receivables;

b) management companies of alternative investment funds governed by Belgian law as referred to in Article 3, 12° of the Law of 19 April 2014 on alternative investment funds and their managers;

c) branches in Belgium of management companies of foreign undertakings for collective investment as referred to in Article 258 of the aforementioned Law of 3 August 2012;

d) branches in Belgium of management companies of foreign alternative investment funds as referred to in Articles 114, 117, 163 and 166 of the aforementioned Law of 19 April 2014;

13° a) investment firms governed by Belgian law as referred to in Article 3, 11° of the aforementioned Law of 3 August 2012, provided that and to the extent that these firms trade their securities themselves, within the meaning of Article 3, 22°, c) and 30° of the same Law;

b) debt investment firms governed by Belgian law as referred to in Article 505 of the aforementioned Law of 19 April 2014, provided that and to the extent that these firms trade their securities themselves, within the meaning of Article 3, 22°, c) and 30° of the aforementioned Law of 3 August 2012;

c) debt investment firms governed by Belgian law as referred to in Article 271/1 of the aforementioned Law of 3 August 2012, provided that and to the extent that these firms trade their securities themselves;

d) investment firms governed by Belgian law as referred to in Article 3, 11° of the aforementioned Law of 19 April 2014, provided that and to the extent that these firms trade their securities themselves, within the meaning of Article 3, 26° of the same Law;

14° alternative funding platforms as referred to in the Law of 18 December 2016 regulating the recognition and definition of crowdfunding and containing various provisions relating to finance;

[15° market operators as referred to in Article 3, 3° of the Law of 21 November 2017 on infrastructures for markets in financial instruments and transposing Directive 2014/65/EU, organising the Belgian regulated markets, except for their public tasks;]

*§ 1, 15° replaced by Article 111, 6° of the Law of 30 July 2018 – Belgian Official Gazette of 10 August 2018*

16° persons established in Belgium who, by way of their business activity, carry out spot purchases and sales of foreign currency in the form of cash or cheques expressed in foreign currencies, or by using a credit or payment card, as referred to in Article 102, second subparagraph, of the Law of 25 October 2016 on access to the activity of investment services and on the legal status and supervision of portfolio management and investment advice companies;

17° intermediaries in banking and investment services as referred to in Article 4, 4°, of the Law of 22 March 2006 on intermediation in banking and investment services and on the distribution of financial instruments, and branches in Belgium of persons engaged in equivalent activities that are governed by the law of another Member State;

18° independent financial planners as referred to in Article 3, § 1 of the Law of 25 April 2014 on the legal status and supervision of independent financial planners and the provision of expertise in financial planning by regulated companies, and branches in Belgium of persons engaged in equivalent activities that are governed by the law of another Member State;

19° insurance intermediaries as referred to in Part 6 of the Law of 4 April 2014 on insurance, that exercise their professional activities without any exclusive agency contract in one or more of the classes of life insurance referred to in Annex II of the aforementioned Law of 13 March 2016, and branches in Belgium of persons engaged in equivalent activities that are governed by the law of another Member State;

20° lenders within the meaning of Article I.9, 34° of the Code of Economic Law, that are established in Belgium and are engaged in consumer credit or mortgage credit activities as referred to in Book VII, Title 4, Chapters 1 and 2 of the same Code, and branches in Belgium of persons engaged in equivalent activities that are governed by the law of another Member State;

21° persons as referred to in Article 2, § 1 of Royal Decree 55 of 10 November 1967 regulating the legal status of companies engaged in lease financing, and branches in Belgium of persons engaged in equivalent activities that are governed by the law of another Member State;

22° natural or legal persons, other than those referred to in points 4° to 21°, that are engaged in Belgium in at least one of the activities referred to in Article 4, first subparagraph, 2) to 12), 14) and 15) of the Law of 25 April 2014 on the legal status and supervision of credit institutions and investment firms, and branches in Belgium of persons engaged in equivalent activities that are governed by the law of another Member State and that are designated by the King;

23° natural or legal persons operating in Belgium that are registered or recorded in the public register held by the *Institut des réviseurs d'entreprises / Instituut der Bedrijfsrevisoren* (Institute of company auditors), in accordance with Article 10 of the Law of 7 December 2016 on the organisation of the profession and the public supervision of auditors, natural persons that are trainee external auditors as referred to in Article 11, § 3 of the aforementioned law, and audit firms and persons exercising the profession of statutory auditor;

24° natural or legal persons on the list of external chartered accountants (*experts-comptables*) and on the list of external tax consultants referred to in Article 5, §1, of the Law of 22 April 1999 on accounting and fiscal professions, as well as natural or legal persons on the list of trainee external chartered accountants and trainee external tax consultants referred to in Article 4 of the aforementioned Law;

25° natural or legal persons on the list of external chartered accountants and on the list of external tax consultants referred to in Article 44, fifth subparagraph, of the aforementioned Law of 22 April 1999, as well as natural or legal persons on the list of trainee external chartered accountants (*experts-comptables*) and trainee external tax consultants referred to in the same Article of the aforementioned Law of 22 April 1999;

26° notaries;

27° bailiffs;

28° lawyers:

a) when they assist their client in planning or carrying out transactions concerning the:

i) buying and selling of real property or business entities;

ii) managing of client money, securities or other assets;

iii) opening or management of bank, savings or securities accounts;

iv) organisation of contributions necessary for the creation, operation or management of companies;

v) creation, operation or management of fiducies or trusts, companies, foundations, or similar structures;

b) or when they act on behalf of and for their client in any financial or real property transaction;

29° company service providers referred to in Article 3, 1°, of the [Law of 29 March 2018 on the registration of company service providers];

§ 1, 29° modified by Article 12 of the Law of 29 March 2018 – *Belgian Official Gazette of 2 May 2018*

30° estate agents, referred to in Article 2, 5° and 7°, of the Law of 11 February 2013 on the organisation of the profession of estate agent, who are listed on the official roll referred to in Article 3 of the same Law or the roll referred to in Article 3 of the Law of 11 May 2003 establishing the Federal Councils of certified land surveyors;

31° dealers in diamonds referred to in Article 169, §3, of the Programme Law of 2 August 2002;

32° security companies referred to in Article 4 of the Law of 2 October 2017 regulating private and special security, that provide services of surveillance referred to in Article 3, 3°, a), b) of c) of the same Law;

33° natural or legal persons that operate one or several games of chance referred to in Article 2 of the Law of 7 May 1999 on games of chance, betting, gaming establishments and the protection of players, excluding natural or legal persons referred to in Article 3 and 3bis of the same Law;

§ 2. The King may, by Decree deliberated in the Council of Ministers, based on an adequate risk assessment conducted by the Belgian Gaming Commission for the games of chance referred to in Article 4, 36°, exempt licensees as defined in Article 25, 1/1 to 9 of the Law of 7 May 1999 on games of chance, betting, gaming establishments and the protection of players, from applying some or all of the provisions of book II of the same Law, on the basis of the low risk of operating these services, due to their nature and, where appropriate, due to their scale.

The risk assessment referred to the first subparagraph will take into account the degree of vulnerability of the transactions involved, in particular with regard to the payment methods used.

The competent Minister shall notify the European Commission of any decree taken in accordance with the first subparagraph, with grounds based on a specific risk assessment referred to in the same subparagraph, indicating how the relevant conclusions of the report drafted by the European Commission in accordance with Article 6, first paragraph, of Directive 2015/849, were taken into account.

§ 3. The King may, by Decree deliberated in the Council of Ministers, based on Article 85 and an adequate risk assessment exempt natural or legal persons from applying some or all of the provisions of Book II of this Law that engage in a financial activity referred to in Article 4, 2) to 12), and 14), of the Law of 25 April 2014 on the status and supervision of credit institutions and stock broking firms, which are not money transfers as referred to in Article I.9, 14°, of the Code of Economic Law, on an occasional or very limited basis, provided that all of the following criteria are met:

1° the financial activity is limited in absolute terms;

2° the financial activity is limited on a transaction basis;

3° the financial activity is not the main activity of such persons and the turnover of this financial activity does not exceed five percent of this person's total turnover;

4° the financial activity is ancillary and directly related to the main activity of such persons;

5° the main activity of such persons is not an activity referred to paragraph 1, 23° to 30° or 33°;

6° the financial activity is provided only to the customers of the main activity of such persons and is not generally offered to the public.

When the King uses the power granted in accordance with the first subparagraph He shall:

1° determine, for the purpose of the first subparagraph, 1°, the amount of the total turnover which it may not exceed. This amount is fixed at national level, depending on the type of financial activity. It is sufficiently low to significantly reduce the ML/TF risk;

2° determine, for the purpose of the first subparagraph, 2°, a maximum amount per customer and per transaction, whether carried out in a single or in several apparently related transactions. This amount is fixed at national level, depending on the type of financial activity. It is sufficiently low to ensure that these transactions are not a suitable or efficient method for money laundering or terrorist financing, and does not exceed EUR 1 000;

3° designate the competent authority referred to in Article 85, which He shall task with supervising of compliance with the conditions for the exemption granted in accordance with the first subparagraph and establishing the specific supervisory rules by regulation.

The competent minister informs the European Commission of any decision taken in accordance with the first subparagraph.

§ 4. The King may, by Decree deliberated in the Council of Ministers, upon the advice of the coordinating bodies and taking into account the national risk assessment referred to in Article 68, extend the implementation of all or some of the provisions of book II to categories of entities not referred to in paragraph 1 and whose activities could be used for money laundering or terrorist financing purposes.

The competent minister informs the European Commission of the extension of the scope of this Law in accordance with the first subparagraph.

§ 5. The Royal Decrees issued pursuant to paragraphs 2 to 4 will cease to apply if they are not confirmed by law within twelve months from the date of commencement. The confirmation is retroactive to the date of commencement of the Royal Decrees.

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



# NBB anti-money laundering regulation of 21 November 2017 - Article 2

## Article 2

This Regulation shall apply to obliged entities as referred to in Article 5, § 1, 4° to 10°, of the Law.

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



## Definitions

Home > Financial oversight > Combating money laundering and the financing of terrori...

The terms used on this AML/CFT website have the same meaning as in Articles 2 to 4 of the Anti-Money Laundering Law and in Article 1 of the Anti-Money Laundering Regulation of the NBB.

In particular, "**money laundering**" is defined in Article 2 of the Anti-Money Laundering Law, and "**terrorist financing**" in Article 3 of the same Law. As regards the other definitions, we refer to the following legal and regulatory provisions:

- "**Criminal activity**": see Article 4, 23° of the Anti-Money Laundering Law
- "**AMLCO**": see Article 1, 4° of the Anti-Money Laundering Regulation
- "**Supervisory authorities**": see Article 4, 17° of the Anti-Money Laundering Law
- "**European Supervisory Authorities**" or "**ESAs**": see Article 4, 11° of the Anti-Money Laundering Law
- "**(A)ML/(C)FT**": see Article 4, 1 of the Anti-Money Laundering Law
- "**(A)ML/(C)FTP**": see Article 4, 2° of the Anti-Money Laundering Law
- "**Beneficial owner**": see Article 4, 27° of the Anti-Money Laundering Law
- "**Binding provisions on financial embargoes**": see Article 1, 6° of the Anti-Money Laundering Law
- "**Goods**": see Article 4, 24° of the Anti-Money Laundering Law
- "**NBB**": the National Bank of Belgium
- "**Financial intelligence unit**": see Article 4, 15° of the Anti-Money Laundering Law
- "**Ministerial Committee tasked with coordinating the fight against the laundering of money of illicit origin**": see Article 4, 12° of the Anti-Money Laundering Law
- "**Numbered account or contract**": see Article 1, 7° of the Anti-Money Laundering Regulation
- "**National Security Council**": see Article 4, 13° of the Anti-Money Laundering Law
- "**Life insurance contract**": see Article 4, 25° of the Anti-Money Laundering Law
- "**Professional counterparty**": see Article 1, 8° of the Anti-Money Laundering Regulation
- "**CTIF-CFI**": see Article 4, 16° of the Anti-Money Laundering Law
- "**Directive 2015/849**": see Article 4, 3° of the Anti-Money Laundering Law
- "**Obligated entity**": see Article 4, 18° of the Anti-Money Laundering Law
- "**Obligated entity established in another Member State or in a third country**": see Article 4, 19° of the Anti-Money Laundering Law
- "**Obligated entity governed by the law of another Member State**": see Article 4, 20° of the Anti-Money Laundering Law
- "**Obligated entity governed by the law of a third country**": see Article 4, 21° of the Anti-Money Laundering Law
- "**Member State**": see Article 4, 7° of the Anti-Money Laundering Law
- "**Managerial functions**": see Article 4, 39° of the Anti-Money Laundering Law
- "**Group**": see Article 4, 22° of the Anti-Money Laundering Law
- "**Financial Action Task Force**" or "**FATF**": see Article 4, 10° of the Anti-Money Laundering Law
- "**Obligated financial institutions**": the entities referred to in Article 5, § 1, 4° to 10° of the Anti-Money Laundering Law and in Article 2 of the Anti-Money Laundering Regulation of the NBB, or the entities referred to on this AML/CFT website
- "**Games of chance**": see Article 4, 36° of the Anti-Money Laundering Law
- "**Business day**": see Article 4, 40° of the Anti-Money Laundering Law
- "**Anti-Money Laundering Law**": the Law of 18 September 2017 on the prevention of money laundering and terrorist financing and on the restriction of the use of cash
- "**Family member**": see Article 4, 29° of the Anti-Money Laundering Law
- "**Senior management**": see Article 4, 31° of the Anti-Money Laundering Law

- **"Implementing measures of Directive 2015/849"**: see Article 4, 4° of the Anti-Money Laundering Law
- **"Electronic money"**: see Article 4, 35° of the Anti-Money Laundering Law
- **"Atypical transaction"**: see Article 1, 6° of the Anti-Money Laundering Regulation
- **"Occasional transaction"**: see Article 1, 5° of the Anti-Money Laundering Regulation
- **"Coordinating bodies"**: see Article 4, 14° of the Anti-Money Laundering Law
- **"International organisation"**: see Article 4, 32° of the Anti-Money Laundering Law
- **"Third country"**: see Article 4, 8° of the Anti-Money Laundering Law
- **"High-risk third country"**: see Article 4, 9° of the Anti-Money Laundering Law
- **"Persons known to be close associates"**: see Article 4, 30° of the Anti-Money Laundering Law
- **"Politically exposed person"**: see Article 4, 28° of the Anti-Money Laundering Law
- **Anti-Money Laundering Regulation of the NBB**: Regulation of the NBB of 21 November 2017 on the prevention of money laundering and terrorist financing
- **"European Regulation on transfers of funds"**: see Article 4, 5° of the Anti-Money Laundering Law
- **"Business relationship"**: see Article 4, 33° of the Anti-Money Laundering Law
- **"Correspondent relationship"**: see Article 4, 34° of the Anti-Money Laundering Law
- **"Managerial responsibilities"**: see Article 4, 38° of the Anti-Money Laundering Law
- **"Shell bank"**: see Article 4, 37° of the Anti-Money Laundering Law
- **"Trust"**: see Article 4, 26° of the Anti-Money Laundering Law

For more information on the definitions contained in the Anti-Money Laundering Law, see the comments on Articles 2 to 4 of the Anti-Money Laundering Law in the Explanatory Memorandum of this Law.

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



# Risk-based approach and overall risk assessment

Home > Financial oversight > Combating money laundering and the financing of terrori...

## Legal and regulatory framework

- Anti-Money Laundering Law
  - Article 7: risk-based approach
  - Articles 16 to 18 and Annexes I to III: overall risk assessment
- Anti-Money Laundering Regulation of the NBB
  - Articles 3 and 5: overall risk assessment by financial institutions
  - Article 6: overall risk assessment at group level

## Explanatory Memorandum of the Anti-Money Laundering Law

- Articles 7 and 16 to 18

## Supranational risk assessment (SNRA)

- ESAs Joint Opinion dated 4 October 2019 on the risks of money laundering and terrorist financing affecting the Union's financial sector
- Report from the Commission to the European Parliament and the Council dated 24 July 2019 on the assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border activities
  - Annex (Commission Staff Working Document)

## National risk assessment (NRA)

(not yet published)

## Risk factors to be taken into account

- ESAs Risk Factor Guidelines dated 4 January 2018

## Other reference documents

- FATF Guidance dated 26 October 2018 for a Risk-Based Approach for the Securities Sector
  - Highlights
- FATF Guidance dated 25 October 2018 for a Risk-Based Approach for the Life Insurance Sector
  - Highlights
- BCBS Guidelines dated June 2017 on Sound management of risks related to money laundering and financing of terrorism
- ESAs Guidelines dated 7 April 2017 on risk-based supervision
- FATF Guidance dated 23 February 2016 for a Risk-Based Approach for Money or Value Transfer Services
- FATF Guidance dated 23 October 2015 for a Risk-Based Approach: Effective Supervision and Enforcement by AML/CFT Supervisors of the Financial Sector and Law Enforcement
- FATF Guidance dated 27 October 2014 for a Risk-Based Approach for the Banking Sector

## Comments and recommendations by the NBB

- Communication NBB\_2020\_002 of 23 January 2020 containing the conclusions of the horizontal analysis of a sample of summary tables of the overall assessment of the risks of money laundering and/or terrorist financing
- Comments and recommendations

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



# Anti-Money Laundering Law of 18 September 2017 - Article 7

## Art. 7

Unless otherwise stipulated, the competent authorities and the obliged entities, in accordance with the provisions of this Law, shall implement the preventive measures referred to in Book II, in a differentiated manner, according to their ML/TF risk assessment.

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



# Anti-Money Laundering Law of 18 September 2017 - Articles 16 to 18

## Art. 16

Obligated entities shall take measures that are appropriate and commensurate with their nature and their size to identify and assess the ML/FT risks to which they are exposed, by taking into account in particular the characteristics of their customers, the products, services or transactions offered by them, the countries or geographical areas concerned and the distribution channels used by them.

In their overall risk assessment referred to in the first subparagraph, they shall at least take into consideration the variables set out in Annex I. Moreover, they make take into account the factors that are indicative of a potentially lower risk set out in Annex II, and shall at least take into account the factors that are indicative of a potentially higher risk set out in Annex III.

They shall also take into account the relevant conclusions of the report drawn up by the European Commission pursuant to Article 6 of Directive 2015/849, and of the report drawn up by the coordinating bodies pursuant to Article 68, each in its own ambit, as well as all other relevant information at their disposal.

## Art. 17

The overall risk assessment referred to in Article 16 shall be documented, updated and kept at the disposal of the supervisory authorities competent pursuant to Article 85.

Obligated entities must be able to demonstrate to their supervisory authority competent by virtue of Article 85 that the policies, procedures and internal control measures developed by them in accordance with Article 8, including, where appropriate, their customer acceptance policies, are appropriate in view of the ML/FT risks they have identified.

Updating the overall risk assessment implies, where appropriate, also updating the individual risk assessments referred to in Article 19, § 2, first subparagraph.

## Art. 18

Supervisory authorities competent pursuant to Article 85 may decide that individual documented risk assessments are not required where the specific risks inherent to the activities concerned are clear and understood.

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



# Anti-Money Laundering Law of 18 September 2017 - Annexes I to III

**The annexes to this Law form an integral part of the Law. They consist of articles. When articles from an annex are referred to, this is explicitly stated.**

---

## Annex I

Article 1. When conducting their overall risk assessment pursuant to Article 16, second subparagraph, the obliged entities shall at least consider the following variables:

- 1° the purpose of an account or relationship;
- 2° the level of assets to be deposited by a customer or the size of transactions undertaken;
- 3° the regularity or duration of the business relationship.

## Annex II

Article 1. The factors that are indicative of a potentially lower risk, as referred to in Articles 16, second subparagraph and 19, § 2, are the following:

1° customer risk factors:

- a) public companies listed on a regulated market and subject to disclosure requirements (either by regulated market rules or through laws or enforceable means), which impose requirements to ensure adequate transparency of beneficial ownership;
- b) public administrations or enterprises;
- c) customers that are resident in geographical areas of lower risk as set out under 3°;

2° product, service, transaction or delivery channel risk factors:

- a) life insurance policies for which the premium is low;
- b) insurance policies for pension schemes if there is no early surrender option and the policy cannot be used as collateral;
- c) a supplementary pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages, and the scheme rules do not permit the assignment of a member's interest under the scheme;
- d) financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes;
- e) products where the ML/FT risks are managed by other factors such as purse limits or transparency of ownership

(e.g. certain types of electronic money);

3° geographical risk factors:

- a) Member States;
- b) third countries having effective AML/CFT systems;
- c) third countries identified by credible sources as having a low level of corruption or other criminal activity;
- d) third countries which, on the basis of credible sources such as mutual evaluations, detailed assessment reports or published follow-up reports, have AML/CFT requirements consistent with the revised FATF Recommendations and effectively implement those requirements.

## Annex III

Article 1. The factors that are indicative of a potentially higher risk, as referred to in Articles 16, second subparagraph and 19, § 2, are the following:

1° customer risk factors:

- a) the business relationship is conducted in unusual circumstances;
- b) customers that are resident in geographical areas of higher risk as set out under 3°;
- c) legal persons or arrangements that are personal asset-holding vehicles;
- d) companies that have nominee shareholders or shares in bearer form;
- e) businesses that are cash-intensive;
- f) the ownership structure of the company appears unusual or excessively complex given the nature of the company's business;

2° product, service, transaction or delivery channel risk factors:

- a) private banking services;
- b) products or transactions that might favour anonymity;
- c) non-face-to-face business relationships or transactions, without certain safeguards such as electronic signatures;
- d) payment received from unknown or unassociated third parties;
- e) new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products;

3° geographical risk factors:

- a) without prejudice to Article 38, countries identified by credible sources, such as mutual evaluations, detailed assessment reports or published follow-up reports, as not having effective AML/CFT systems;
- b) countries identified by credible sources as having significant levels of corruption or other criminal activity;
- c) countries subject to sanctions, embargoes or similar measures issued by, for example, the European Union or the United Nations;
- d) countries providing funding or support for terrorist activities, or that have designated terrorist organisations

operating within their country.

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



# NBB anti-money laundering regulation of 21 November 2017 - Articles 3 and 5

## Art. 3

The overall risk assessment referred to in Article 16 of the Law shall meet the following requirements:

1° it shall be carried out under the responsibility of the AMLCO and approved by the senior management;

2° it shall cover all activities carried out by the obliged financial institution in Belgium, as well as activities carried out by way of freedom to provide services in another Member State or in a third country;

3° it shall be subject to a specific procedure to determine its conditions, including those governing its update as laid down in Article 17 of the Law. This update shall be carried out whenever an event occurs that is likely to have a significant impact on one or more risks. The AMLCO shall also verify at least once a year whether the risk assessment is still up to date, and shall report his/her conclusions, as well as any possible updates to be made, in the report referred to in Article 7.

## Art. 5

Obliged financial institutions shall keep a record in writing, on paper or electronically, of the way in which any ML/FT risks that they have identified and assessed pursuant to Article 16 of the Law, are taken into consideration in policies, including the customer acceptance policy referred to in Title 3 of this Regulation, in procedures and internal control measures that they establish in accordance with Article 8 of the Law. They shall keep this document available for the Bank, in order to meet the requirement of Article 17, second paragraph, of the Law.

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



## NBB anti-money laundering regulation of 21 November 2017 - Article 6

§ 1. Obligated financial institutions established in another Member State or in a third country, or which have subsidiaries that are obliged financial institutions in Belgium, shall take appropriate measures to ensure that their branches and subsidiaries carry out, each for its own account, an overall assessment of the ML/FT risks to which they are exposed in their country of establishment, and that they report back with this overall risk assessment.

§ 2. The obliged financial institutions referred to in Article 5, § 1, 6°, a) to c), and 7°, a) to d), of the Law, shall also ensure that an overall assessment be made of ML/FT risks associated with the activities that they carry out in another Member State or third country through one or several persons who are established and represent them there.

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**

# Explanatory Memorandum to the Anti-Money-Laundering Law of 18 September 2017 - Article 7

## Art. 7

As already specified above (see the general explanation above), one of the most important developments, both in the FATF Recommendations and in the European regulatory framework, is that it is emphasised more expressly and more generally than before that a risk-based approach should be used as the cornerstone for the mechanisms to prevent ML/TF, and not only by the obliged entities but also by the competent authorities. This development is as a consequence reflected in the present draft Law too, transposing Directive 2015/849, and in particular:

- as regards the definition of the national policy on AML/CFT, by formalising a national risk assessment (see Book IV, Title 1, below), which must be based on the Supranational Risk Assessment conducted by the European Commission, in accordance with Article 6 of the Directive;
- as regards preventive measures taken by the obliged entities, by conducting a two-tier risk assessment, in particular:
  - a general assessment of the risks to which the obliged entities are exposed, based on the nature of their activities, the characteristics of the customers they deal with, and the characteristics of the channels through which these customer relations occur, etc. (cf. Book II, Title 2, below). This assessment must allow them in particular to establish policies and procedures for AML/CFT which are in proportion to and differentiated on the basis of the risks;
  - assessment of the risks associated with each client, which will determine the level of intensity of the due diligence measures that must be taken on a case-by-case basis (cf. Article 19, § 2, below).
- as regards the exercise of supervision by the competent authorities on compliance by the obliged entities with the obligations pertaining to AML/CFT, by defining a risk-assessment-based supervisory model per obliged entity that falls under their supervision (cf. Article 87, below).

The goal of this general application of a risk-based approach is to promote optimal allocation of the resources available for AML/CFT at all levels and to make prevention as effective as possible.

It should also be emphasised that, although the risk-based approach is applied for a very large proportion of the mechanisms for AML/CFT provided for by this draft Law, for certain aspects of these mechanisms, a more traditional approach is nevertheless followed based on compliance with the rules ("rules-based approach"). This applies for example to the obligation to report information to the CTIF-CFI (cf. Book II, Title 4, Chapter 2, below).

It should also be noted that this risk-based approach does not extend to the provisions of other laws or to European regulations that are also relevant based on the intended objectives of this draft Law, and that are based exclusively on the rules-based principle. This applies in particular for application of the European Funds Transfer Regulation or the binding provisions on financial embargos, as defined in draft Article 4, 5° and 6° (see below).

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**

# Explanatory Memorandum to the Anti-Money-Laundering Law of 18 September 2017 - Articles 16 to 18

## Article 16

As stated previously, the reinforcement of the risk-based approach with a view to the enforcement of effective mechanisms to combat ML/TF is one of the major developments, both in the FATF Recommendations and, consequently, in the European regulatory framework regarding AML/CFT. For obliged entities, it means, in particular, that all measures of any nature whatsoever that they take, both at the level of their organisation and of their relationship with all customers individually must be focused, more clearly and strongly than in the past, on mitigating the risk that they could be misused for ML/TF purposes.

This risk-based approach must enable obliged entities to take less extensive measures in situations where the risks are low, to be able to dedicate the resources that have thereby been freed up to apply enhanced measures for situations in which the risks are higher, and must, thanks to this optimisation of the allocation of available resources, result in enhanced effectiveness of AML/CFT.

Achieving this objective does, however, require the obliged entities to have an as thorough and up-to-date as possible understanding of the risks to which they are exposed.

In accordance with Article 8, paragraph 1, of Directive 2015/849, which is transposed by this Article, Article 16 of the draft Law consequently imposes the obligation for all obliged entities to take appropriate measures commensurate with their nature and scale to identify and assess the ML/TF risks to which they are exposed. This general (or 'business-wide') risk assessment involves the obliged entity conducting an analysis of the characteristics of its customers, of the products, services or transactions it offers, of the countries or geographical areas in which the entity offers its services or with which the customer is associated, and of the delivery channels used by the obliged entity.

Just like the Directive it transposes, this draft Law includes, in Annexes I, II and III, lists of variables and factors that indicate a potentially higher or lower risk, which the obliged entities must take into consideration in their general risk assessment. They must also take account of the relevant results of the Supranational Risk Assessment for the European Union, which must be drawn up by the European Commission in accordance with Directive 2015/849, as well as of the relevant results of the national risk assessment referred to in Article 68 of the draft Law.

Obliged entities that belong to the financial sector must also take into account the advice on the ML/TF risks for the EU's financial sector, which will need to be drafted by the ESAs pursuant to Article 6, paragraph 5 of Directive 2015/849, and the 'guidelines' that the ESAs will have to publish regarding the factors that indicate a lower risk (pursuant to Article 17 of the Directive) and the factors that indicate a higher risk (pursuant to Article 18, paragraph 4 of the Directive).

This general risk assessment will be essential to enable the obliged entities to show the relevance of the organisational measures they establish and implement in accordance with Title I above, and therefore to ascertain the pertinence of the individual risk assessments required in accordance with Article 19, § 2 of the present draft Law.

It should also be noted that, in accordance with the first paragraph of draft Article 16, the measures that must be taken to be able to conduct such a general risk assessment should be commensurate with the nature and scale of the obliged entity conducting the assessment.

## Article 17

Draft Article 17 specifies that the general risk assessment must be documented and updated and kept available for the supervisory authorities, and that obliged entities must be able to demonstrate to them that the organisational measures they establish and apply are appropriate to reduce the ML/TF risks identified.

## Article 18

Finally, draft Article 18, just like Article 8, paragraph 2 of Directive 2015/849, which is transposed by this Article, stipulates that the supervisory authorities may allow derogations from the obligation to conduct a general risk assessment. This power may be used either for an individual obliged entity which so requests itself or, upon the initiative of the supervisory authority, for a category of obliged entities that it determines. This derogation may also only apply to one or more very specific activities. However, this derogation may only be permitted in cases where conducting a general risk assessment is of no real use, insofar as the ML/TF risks are actually well-known and properly understood by the obliged entities even without such a risk assessment.

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**

# Risk-based approach and overall risk assessment: Comments and recommendations by the NBB

Home > Financial oversight > Combating money laundering and the financing of terrori...

## Contents

- 1. Background
- 2. Governance
- 3. Process
- 4. Communication to the NBB

## 1. Background

The requirement to adopt a risk-based approach for the prevention of ML/FT, the basis of which is laid down in Article 7 of the Anti-Money Laundering Law, is one of the key elements in the FATF Recommendations as revised in 2012 and in Directive 2015/849. At the Belgian level, this requirement has inter alia resulted, with regard to the preventive measures to be implemented by obliged entities, in the obligation to perform a dual risk assessment, namely:

- *an overall assessment of the risks to which they are exposed*, in accordance with the provisions of Articles 16 and 17 of the Anti-Money Laundering Law on the one hand, and of Title 2 of the Anti-Money Laundering Regulation of the NBB on the other hand (see below);
- *an assessment of the risks associated with each customer* (see the page “Individual risk assessment”).

Article 16 of the Anti-Money Laundering Law requires the obliged entities to take measures that are appropriate and commensurate with their nature and their size to identify and assess the ML/FT risks to which they are exposed. In doing so, they should take into account the characteristics of their customers, the products, services or transactions offered, the countries or geographical areas concerned and the distribution channels used.

The overall risk assessment (or business-wide risk assessment) to be carried out by the financial institutions should enable them to identify the inherent ML/FT risks to which their business exposes them and to manage these risks in an appropriate manner or, where necessary, to mitigate them. The risk-based approach also allows institutions to take less far-reaching measures in situations which present a low ML/FT risk, and to use the resources thus freed for the compulsory application of enhanced measures in situations where the risks are higher. Thus, the allocation of available resources can be optimised.

As the overall risk assessment should enable the financial institution to ensure that its policies, procedures and internal control measures and, in general, its organisation, are appropriate and sufficiently granular to address the generic ML/FT risks to which its business exposes it, this overall risk assessment is clearly different from the individual risk assessment carried out in accordance with Article 19 of the Law in order to decide, on a case-by-case basis, taking adequate account of the possible specificities of each individual case, on the intensity of the due diligence measures to be applied or, where appropriate, to refuse to enter into the business relationship or to carry out the proposed occasional transaction.

It also follows from the above that an appropriate risk-based approach starts with acquiring thorough and up-to-date knowledge of the ML/FT risks to which the institution is exposed and understanding these risks.

In accordance with Article 3, 3°, of the Anti-Money Laundering Regulation of the NBB, the overall risk assessment should cover all activities of the financial institution established in Belgium which is subject to the ML/FT legislation, including its cross-border activities conducted under the freedom to provide services in another Member State or in a third country. If the institution operates through a group, Article 6 of the Anti-Money Laundering Regulation of the NBB stipulates that all its branches and subsidiaries should submit their overall risk assessment to the institution, so that the latter can take it into account when determining the general risk policy at the level of the group. In this context, payment institutions and electronic money institutions must also ensure that an overall risk assessment is carried out of the ML/FT risks associated with the activities conducted by them in another Member State or third country through one or more persons established in that member state or third country and representing the institution concerned (e.g. network of agents, etc.).

As far as relevant for their sector, financial institutions should take into account at least the following elements in their overall risk assessment (see the reference documents mentioned above):

- the variables set out in Annex I of the Anti-Money Laundering Law;
- the factors that are indicative of a potentially higher risk, as referred to in Annex III of the same Law;
- ESAs Joint Opinion dated 20 February 2017 on the risks of money laundering and terrorist financing affecting the Union's financial sector, issued pursuant to Article 6(5) of Directive 2015/849, and the guidelines published by the ESAs on the factors that are indicative of a lower risk (pursuant to Article 17 of the Directive) and the factors that are indicative of a higher risk (pursuant to Article 18(4) of the Directive) ("ESAs Risk Factor Guidelines dated 4 January 2018");
- the relevant conclusions of the report drawn up by the European Commission pursuant to Article 6 of Directive 2015/849 ("Report from the Commission to the European Parliament and the Council dated 24 July 2019 on the assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border activities");
- the report drawn up by the coordinating bodies pursuant to Article 68 of the Anti-Money Laundering Law, each in its own ambit, and
- all other relevant information at their disposal.

In addition, the Anti-Money Laundering Law also provides the possibility to take account in the aforementioned assessment of the factors listed in its Annex II (potentially lower risk).

The overall ML/FT risk assessment should be carried out under the responsibility of the AMLCO (see the page "Governance") and approved by the senior management (Article 3, 1°, of the Anti-Money Laundering Regulation of the NBB).

Article 17 of the Anti-Money Laundering Law also provides that the overall risk assessment should be documented, updated and kept at the disposal of the NBB. In this respect, financial institutions should be able to demonstrate to the NBB that the policies, procedures and internal control measures developed by them in accordance with Article 8 of the Law, including, where appropriate, their customer acceptance policies (see the page "Policies, procedures, processes and internal control measures"), are appropriate in view of the ML/FT risks they have identified. Updating the overall risk assessment implies, where appropriate, also updating the individual risk assessments referred to in Article 19, § 2, first paragraph of the Law (see the page "Individual risk assessment").

Finally, it should be noted that the overall risk assessment to be carried out by the financial institutions under Article 16 of the Anti-Money Laundering Law is not a one-off exercise but a continuous process. This risk assessment - and, where appropriate, also the individual risk assessment - should be updated whenever one or more events occur that could have a significant impact on the risks (see Article 3, 3°, of the Anti-Money Laundering Regulation of the NBB and point 3.4 below).

## 2. Governance

As mentioned above, the overall risk assessment should be presented in a written document (in paper or electronic form) that is kept available to the NBB (see Article 17 of the Anti-Money Laundering Law). This document should also contain a description of the process used to perform the overall risk assessment, including:

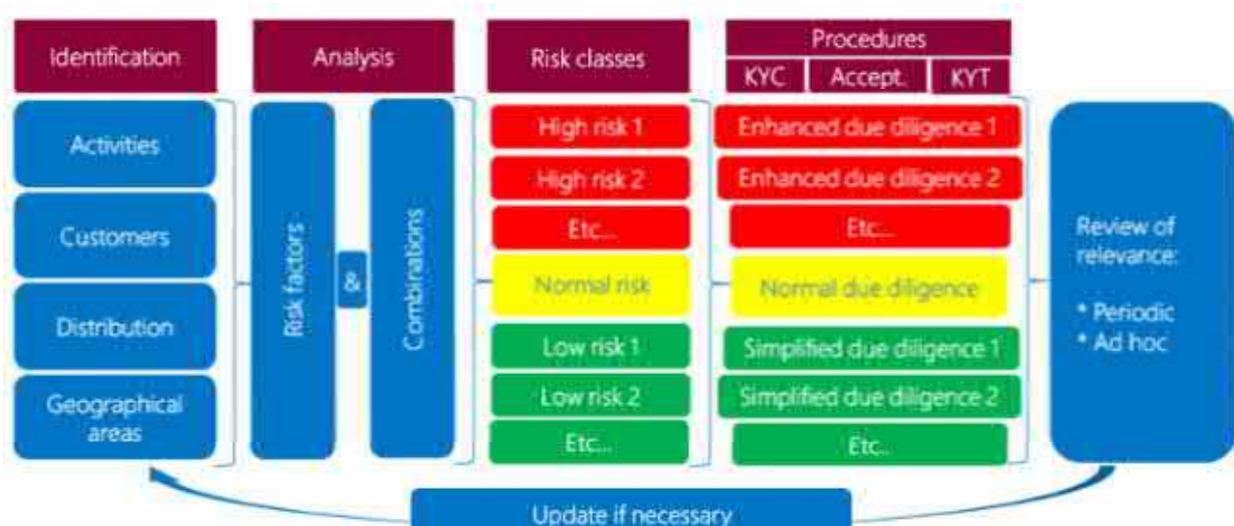
- the methodology used to perform the overall risk assessment, which is expected to include at least the key elements referred to in point 3 below;

- the manner in which this process has been integrated into the institution's broader risk management system and in its corporate governance, including the manner in which the group dimension, if any, has been incorporated in the assessment;
- a description of the procedures for monitoring and timely updating the risk assessment process in order to ensure its permanent accuracy;
- a description of the extent to which the AMLCO, the compliance officer, senior management, and any other parties have been involved in the identification and analysis of the risks, the development of the actual risk assessment and any related measures, or the acknowledgement and validation of the process as a whole.

### 3. Process

The overall risk assessment should be carried out in three successive phases:

- identification and analysis of risks associated with money laundering and terrorist financing and compliance with the rules on international sanctions, embargoes and other restrictive measures, to which the institution is exposed ("risk identification phase");
- analysis and assessment of the adequacy of the existing relevant risk management measures ("gap analysis");
- if necessary, taking new or additional risk management measures to control the risks that are not or not adequately covered ("adjustment phase").



The way in which the institution applies and implements this process, as well as the degree of granularity, must be proportionate to its nature and size.

In its Communication NBB\_2020\_002 of 23 January 2020 containing the conclusions of the horizontal analysis of a sample of summary tables of the overall assessment of the risks of money laundering and/or terrorist financing, the NBB emphasises the importance of following the different steps of the overall risk assessment in methodological order. In this Communication, the NBB also includes findings related to these different steps of the overall risk assessment process, in methodological order.

#### 3.1 Risk identification phase

##### 3.1.1. Risk classes – Subcategories

As mentioned above, a good overall risk assessment requires, in the first instance, a thorough knowledge and understanding of **all** ML/FT risks to which the institution is exposed. The institution will therefore have to identify all relevant ML/FT risks and to classify them into categories and subcategories, based on one or more of the characteristics defined in Article 16 of the Anti-Money Laundering Law. Besides the characteristics referred to in Article 16, the institution should also take into account any other additional characteristics that might apply to its specific situation, such as specific risks that might arise from intra-bank relationships with other group entities, risks associated with activities conducted on the institution's own account (for example, the dealing room), etc.

For examples of good practices encountered by the NBB during its horizontal analysis of a sample of summary tables of the overall risk assessment, see Communication NBB\_2020\_002 (in particular point IV.a).

### **3.1.2. Risk exposure**

Once the institution has identified and classified the various risks, it must assess the inherent risk by combining the probability of the risk occurring with the impact of any such materialisation of the risk, taking into account the activity effectively performed. In doing so, the institution should take into account the minimum variables and factors referred to in point 1 above, and any other variables and factors that might be appropriate to its specific situation.

The NBB does not prescribe the values or units to be used by the financial institution, the main objective being that the financial institution (and the NBB) can obtain a coherent and comprehensible view of its risk exposure. This should enable the financial institution to then define risk management measures in accordance with the risk appetite determined by its board of directors. In all cases, the NBB would like it to be clear from the documentation on the overall risk assessment process how the probability of the risk occurring and the impact of any such materialisation of the risk are scored.

With regard to the probability of risk occurrence, financial institutions should take care not to underestimate their risks. For example, a credit institution can have few customers who are politically exposed persons in its customer base in absolute terms, but this number can nevertheless represent a substantial percentage of its total customer base.

For more information on this subject, see Communication NBB\_2020\_002 (in particular point IV.b).

## **3.2 Gap analysis**

### **3.2.1. Existing risk management measures**

In a second phase, the institution should make an inventory of the risk management measures it already applies to manage or limit the various risks identified. This inventory of the risk management measures (which cover all due diligence and reporting obligations and can therefore relate to one or more of the following elements: the identification and verification obligation, the ongoing due diligence obligation, the analysis of atypical transactions and the reporting of suspicions and additional information to the CTIF/CFI) should also include compliance with the legal framework laid down in the Anti-Money Laundering Law and Regulation of the NBB (i.e. control of the compliance risk, see in particular Article 8 of the Anti-Money Laundering Law and the page "Governance" ).

### **3.2.2. Adequacy of risk management**

Next, the institution must subject these internal procedures and controls to a critical examination, either to conclude that they are sufficient in view of the inherent risks detected or to identify the (potentially substantial) improvements to be made in order to effectively reduce the risks (mitigation and question of residual risk). In doing so, account must also be taken of the way in which these risk management measures are actually applied and observed in practice. Furthermore, the institution should also consider, *inter alia*, the risk management measures that are recommended in:

- the opinion on the ML/FT risks affecting the Union's financial sector issued by the ESAs under Article 6(5) of Directive 2015/849, and the ESAs Risk Factor Guidelines;
- the report drawn up by the European Commission pursuant to Article 6 of Directive 2015/849;
- the report drawn up by the coordinating bodies pursuant to Article 68 of the Anti-Money Laundering Law;
- any other relevant best practices in this area (for example, guidelines issued by the sector, the FATF, the Basel Committee, etc.).

For more information on this subject, see Communication NBB\_2020\_002 (in particular point V).

### 3.3 Adjustment phase (action plan)

If, at the end of the second phase, the existing risk management measures appear to be insufficient, financial institutions should define new or additional measures to adequately manage or mitigate the risk. The action plan should be sufficiently ambitious in providing timely and appropriate solutions for the weaknesses identified (regardless of whether this involves introducing a new procedure or reviewing the automated transaction monitoring system). When establishing this action plan, it may therefore be appropriate to prioritise actions based on the impact of the identified gaps on the overall efficiency of the AML/CFT mechanisms implemented, especially if the plan comprises a large number of new measures to be introduced.

Finally, the financial institutions should ensure the overall coherence of the action plan: for instance, financial institutions will logically be required to provide for more (substantial) actions with regard to the activities or risk factors for which the residual risk was assessed as high during gap analysis phase than for the activities or risk factors for which the residual risk was assessed as low.

### 3.4 Process timetable and update of the overall risk assessment

All corrective measures necessary in light of the first global risk assessment performed following the entry into force of the Anti-Money Laundering Law should be implemented **by 1 July 2019 at the latest**. Institutions that consider themselves unable to implement certain remedial measures within that period, must submit a duly reasoned request for postponement to the NBB **by 31 May 2019 at the latest**. In such cases, the NBB may - depending on the actual circumstances and insofar as justified in view of the risk - decide to extend the remediation period until 1 January 2020 at the latest.

Additionally, Article 17 of the Anti-Money Laundering Law requires the overall risk assessment to be updated. In this context, the NBB takes this obligation to mean that financial institutions should repeat the process described above

- **whenever significant events occur, either internally or in their environment, that could significantly modify the nature and the scale of the ML/FT risks or their assessment.** These changes could for instance be the result of a decision to develop and offer new products or services, to target new categories of customers, to use new distribution channels or tools or new customer identification and identity verification techniques, to expand their activities in other countries under the freedom to provide services, etc. Examples of external events that could have considerable consequences for the risks or their assessment are significant changes in the legal and regulatory framework of the country concerned or of other countries that are important for the activities carried out, major changes in the socio-economic context, the emergence of new forms of crime or the disclosure of new ML/FT classifications and techniques, etc.
- if, after verification of the effects of the risk reduction measures (mitigation) that are already in place and/or are taken in the context of the overall risk assessment action plan, it appears that these measures are not (sufficiently) effective or efficient and, as a result, other measures seem to be necessary.

However, the nature and scale of the risks could also be changed significantly by slower and more gradual developments both within the financial institution and in its environment. As a result, the NBB considers that, even if no significant events as described above occur, each financial institution should periodically ensure that the quantitative and qualitative information on which its latest overall ML/FT risk assessment was based, has not changed in such a manner that this assessment, which is the cornerstone of its current organisation, policies, procedures and internal controls, is no longer relevant. The NBB considers that, in general, the relevance of the overall risk assessment should be reviewed **annually**. If the internal procedures provide for a lower frequency, the financial institution should be able to justify this decision in the light of the principle of proportionality, taking into account its nature and size, on the one hand, and in the light of the likely stability of the general risk level it identified earlier.

If it appears necessary to update the overall risk assessment, this should be done as soon as possible by completing the three phases described in points 3.1 to 3.3 above, in such a manner that any corrective measures needed to reduce new identified risks are implemented within a reasonable timeframe, taking into account the severity of these new risks. Depending on the circumstances, this update could be required for the entire overall risk assessment or only for those parts of it for which the risk level might have fluctuated significantly.

## 4. Communication to the NBB

Article 17 of the Anti-Money Laundering Law stipulates that the overall risk assessment must be documented, updated and made available to the NBB.

**The documents to be completed and submitted to the NBB in this context as well as the submission method are published on the page “Reporting by financial institutions”.**

The NBB expects future updates to the overall risk assessment to be mentioned and sufficiently clarified in the activity report of the AMLCO, and to be provided with updated versions of the aforementioned documents (taking into account the content of Communication NBB\_2020\_002).

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



# Organisation and internal control

Home > Financial oversight > Combating money laundering and the financing of terrori...

## Organisation and internal control in financial institutions

Governance

Risk classification

Policies, procedures, processes and internal control measures

Training and education of staff

Internal whistleblowing

## Organisation and internal control in groups

Belgian parent companies

Belgian subsidiaries and branches

Belgian central contact points of European payment institutions and electronic money institutions

## Performance of obligations by third parties

## Brexit

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



# Organisation and internal control in financial institutions

[Home](#) > [Financial oversight](#) > [Combating money laundering and the financing of terrori...](#)

**Governance**

**Risk classification**

**Policies, procedures, processes and internal control measures**

**Training and education of staff**

**Internal whistleblowing**

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



## Governance

Home > Financial oversight > Combating money laundering and the financing of terrori...

### Legal and regulatory framework

- Anti-Money Laundering Law: Articles 9 and 12
- Anti-Money Laundering Regulation of the NBB: Article 7

### Explanatory Memorandum of the Anti-Money Laundering Law

- Articles 9 and 12

### Comments and recommendations by the NBB

- Comments and recommendations

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



# Anti-Money Laundering Law of 18 September 2017 - Articles 9 and 12

## Art. 9

§ 1. Obligated entities that are legal persons shall appoint, among the members of their statutory governing body or, where appropriate, of their senior management, the person responsible, at the highest level, for supervising the implementation of and compliance with the provisions of this Law and its implementing decrees and regulations and, where appropriate, the administrative decisions made pursuant to these provisions, the European Regulation on transfers of funds and the restrictive measures referred to in Article 8, § 1, 3°.

If the obliged entity is a natural person, the functions referred to in the first subparagraph shall be performed by that person.

§ 2. Without prejudice to paragraph 3, obliged entities shall moreover appoint, within the entity, one or multiple persons charged with ensuring the implementation of the policies, procedures and internal control measures referred to in Article 8, ensuring the analysis of atypical transactions and the preparation of the relevant written reports in accordance with Articles 45 and 46, in order to, if necessary, provide the follow-up required pursuant to Article 47, as well as ensuring the transmission of the information referred to in Article 54. Moreover, these persons shall oversee the education and training of the staff and, where appropriate, of the agents and distributors, in accordance with Article 11.

If the obliged entity is a legal person, the person or persons referred to in the first subparagraph shall be appointed by its statutory governing body or its senior management.

Obligated entities shall verify in advance whether the person or persons referred to in the first subparagraph possess:

1° the professional reliability needed to perform their functions with integrity;

2° the adequate expertise, knowledge of the Belgian legal and regulatory AML/CFTP framework, availability, hierarchical level and powers within the entity that are necessary to perform these functions effectively, independently and autonomously;

3° the power to propose, on their own initiative, all necessary or useful measures, including the implementation of the means required, in order to guarantee the compliance and efficiency of the internal AML/CFTP measures, to the statutory governing body or the senior management of the obliged entity that is a legal person, or to the natural person who is an obliged entity.

§ 3. The functions referred to in paragraph 2 may be performed by the person referred to in paragraph 1 where this is justified to take into account the nature or size of the obliged entity, particularly with regard to its legal form, its management structure or its workforce.

§ 4. In the cases referred to in Article 5, § 1, 6°, d) and 7°, e), the person referred to in paragraph 2 must be established in Belgium.

## Art. 12

Where a natural person falling within any of the categories of obliged entities listed in Article 5, § 1, 23° to 25°, performs professional activities as an employee of a legal person, the obligations in this Chapter shall apply to that legal person rather than to the natural person.

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



# NBB anti-money laundering regulation of 21 November 2017 - Article 7

## Art. 7

At least once a year, the AMLCO shall establish an activity report and send it to the senior management and the statutory governing body. This report shall enable the senior management to take note of the development of any ML/FT risks to which the obliged financial institution is exposed and to ensure the adequacy of the policies, procedures and internal control measures implemented pursuant to Article 8 of the Law.

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



# Explanatory Memorandum to the Anti-Money-Laundering Law of 18 September 2017- Articles 9 and 12

## Art. 9

In accordance with the provisions of Article 46, paragraph 4 of Directive 2015/849, and to further reinforce involvement of the highest level of the hierarchy of obliged entities which are legal persons, § 1 of Article 9 of the draft Law stipulates that they must designate a member of their statutory governing body (the board of directors in the case of a public limited company or *naamloze vennootschap/société anonyme*) who has the highest level of responsibility for application of and compliance with all legal and regulatory provisions of Belgian law and the relevant European regulations on AML/CFT. Where the obliged entity has a body tasked with day-to-day management, such as a management committee, this highest-level senior manager must be chosen from its members.

This obligation was not included in the Law of 11 January 1993. This senior manager must ensure in particular that the organisational measures listed in Article 8 are sufficient and proportionate taking into account the characteristics of the obliged entity and the ML/TF risks with which they are confronted, and that these organisational measures are adopted by the body he/she is a member of and amended where necessary, in accordance with Article 8, § 4 of the draft Law.

Where the obliged entity is a natural person, the responsibilities listed in § 1 of this provision of the draft Law fall directly to this natural person. This was expressly included in the draft provision to take into account the comment from the Council of State.

This obligation to designate a senior manager as the person responsible is an addition, without thereby being a replacement, to the obligation to designate a person responsible for the enforcement of the AML/CFT policy. This obligation is now already included in Article 18 of the Law of 11 January 1993, the provisions of which are essentially taken over in § 2 of Article 9 of the draft Law. The main responsibilities of this person (also known as the Anti-Money-Laundering Compliance Officer or AMLCO) are the following:

- specific implementation of the organisational measures listed in Article 8 of the draft Law;
- analysis of atypical transactions and of cases in which the obligation of due diligence could not be fulfilled, and drawing up written reports thereon, in accordance with Articles 45 and 46 of the draft Law; and
- deciding on, where necessary, the transmission of reports of suspicions to the CTIF-CFI, in accordance with Article 47, and communicating all other information required to this latter in accordance with the draft Law.

In addition to these supervisory and operational responsibilities, the AMLCO is also responsible for educating and training members of staff and, where applicable, agents and distributors of the obliged entity, in accordance with Article 11 of the draft Law.

Subject to § 3 of Article 9 of the draft Law, the designation of an AMLCO is in principle required, irrespective of whether the obliged entity is a natural or legal person. In this latter case, the AMLCO must be designated by the statutory governing body or, where applicable, by the senior management of the obliged entity. Where there is the practice in a certain sector of an obliged entity joining, for example, an unincorporated association, each obliged entity remains responsible itself for the obligations arising from Article 8, § 1. However, there is nothing to prevent resources being pooled to rationalise the procedures enforced under the present Law.

To guarantee the effectiveness of the AMLCO function, § 2, third paragraph of draft Article 9 includes a list of the conditions the AMLCO must fulfil as the designated person in order to exercise his/her functions with integrity, independence and effectiveness. These conditions relate to the professional integrity, expertise, specific knowledge of AML/CFT, availability, hierarchical level and responsibilities of the aforementioned person within the obliged entity. Furthermore, the AMLCO must have the right to take the initiative to propose, directly to the governing body or senior management of the obliged entity or to the natural person with the capacity of obliged entity, any necessary or useful measures, and to implement the measures required, to guarantee the compliance and effectiveness of the internal measures to combat ML/TF.

This provision of the draft Law, like the preceding second paragraph, takes over and extends to all obliged entities the conditions currently listed in Article 35, §§ 1 and 2 of the Regulation of the Banking, Finance and Insurance Commission (Belgium) of 23 February 2010, approved by Royal Decree of 16 March 2010 and published in the Belgian Official Gazette of 24 March 2010 (hereinafter 'the CBFA Regulation').

Paragraph 3 of Article 9 of the draft Law provides for the possibility of adjusting the requirements under § § 1 and 2 where the characteristics of the obliged entity do not justify or allow strict compliance with these paragraphs. As a result, the tasks of the AMLCO listed in § 2 can be executed by the senior manager designated in accordance with § 1, where the obliged entities are small-scale legal persons.

Where the obliged entity is a natural person and the number of persons employed by this natural person does not allow an AMLCO to be designated from its ranks, or where the nature or scale of the activities so justify, the tasks of the AMLCO may be directly exercised by the natural person who has the capacity of obliged entity.

This is, however, without prejudice to the fact that all tasks and responsibilities described in § § 1 and 2 must in all cases be exercised by all obliged entities.

The principle laid down in Article 9 of the draft Law is a general principle. It will fall to the competent authorities to enforce this principle and apply it, where applicable via regulations as referred to in Article 86, § 1 of the draft Law, especially where it appears necessary to take into account specific practices in the sector of the obliged entities controlled by it such as, for example, in the case of the creation of unincorporated associations between these obliged entities.

Like Article 18, third paragraph of the Law of 11 January 1993, Article 9, § 4 of the draft Law stipulates, as regards payment institutions and electronic money institutions that exercise their activity on the Belgian territory by calling upon agents or distributors, that the person who exercises the function of AMLCO within the aforementioned network of agents or distributors must be established in Belgium. This provision partly transposes Article 45, paragraph 9 of Directive 2015/849.

## Art. 12

Draft Article 12 relates to the obliged entities listed in draft Article 5, § 1, 23° to 25° and transposes Article 46, point 1, third paragraph of Directive 2015/849 which provides for the following: "Where a natural person falling within any of the categories listed in point (3) of Article 2(1) performs professional activities as an employee of a legal person, the obligations in this Section shall apply to that legal person rather than to the natural person". Lawyers, bailiffs, notaries, and estate agents always have an independent status even if they exercise this activity for a legal firm which is a legal person, for a notary firm or bailiff firm, or an estate agent. It is a different matter, however, for accounting professions. They may have the title of company auditor, auditor, chartered accountant or tax consultant and exercise that profession as an employee of a company that also has the capacity of company auditor, audit firm, chartered accountant or tax consultant.

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**

# Governance: Comments and recommendations

Home > Financial oversight > Combating money laundering and the financing of terrori...

## Contents

- 1. Appointment of the senior officer responsible for AML/CFTP
- 2. Appointment of the AMLCO
- 3. Communication of the identity of the responsible persons to the NBB
- 4. Outsourcing of tasks of the AMLCO function
- 5. Application of the principle of proportionality
- 6. Other governance requirements

---

The Anti-Money Laundering Law contains specific provisions on governance. For instance, to ensure the efficiency of the AML/CFTP policy, financial institutions should at least appoint the following persons:

- on the one hand, among the members of their management committee (or their senior management), a **senior officer responsible for AML/CFTP** who is specifically tasked with ensuring the adoption of organisational measures relating to AML/CFTP (see point 1 below); and,
- on the other hand, among the members of their compliance function, a **person responsible for implementing the AML/CFTP policy (the so-called “AMLCO”)** who is tasked with the concrete steering of the AML/CFTP policy (see point 2 below).

However, the AMLCO's tasks can be outsourced in part or in full (see point 4 below). Furthermore, the NBB can accept deviating arrangements by applying the **principle of proportionality**. In accordance with Article 9, § 3, of the Anti-Money Laundering Law, it is for example possible to have the functions of senior officer responsible for AML/CFTP and of AMLCO performed by the same person and/or to outsource the AMLCO's tasks (see point 5 below).

The governance requirements relating to AML/CFTP are also expected to be integrated harmoniously into all **prudential governance rules** included in the different sectoral supervisory laws (see point 6 below).

## 1. Appointment of the senior officer responsible for AML/CFTP

The obligation to appoint a senior officer responsible for AML/CFTP arises from the transposition of Directive 2015/849 into national law and primarily aims to enhance the involvement of the highest hierarchical level of the financial institutions in ML/FT risk management.

### 1.1. Terms and conditions for the appointment of the senior officer responsible for AMLC/CFTP

#### 1.1.1. Senior officer responsible for AML/CFTP in financial institutions governed by Belgian law

##### §1. Position in the organisational chart

Article 9, § 1, of the Anti-Money Laundering Law stipulates that financial institutions should “appoint, among the members of their statutory governing body or, where appropriate, of their senior management, the person responsible, at the highest level, for supervising the implementation of and compliance with the provisions of this

Law [...]”. The comment on this provision in the explanatory memorandum of the Law specifies that “Where the obliged entity has a body tasked with senior management, such as a management committee, this senior officer must be chosen from its members”. For financial institutions falling under the NBB’s supervision, the sectoral prudential rules stipulate that a management committee or senior management should be established to ensure that there is a clear distinction, at the highest level, between business management (which is conferred upon the management committee or the senior management) and the supervision of this management (which is conferred upon the board of directors, which consists of a majority of non-executive directors). In this respect, the senior officer responsible for AML/CFTP must be appointed **among the members of the financial institution’s management committee** (the senior officer responsible for AML/CFTP therefore may not be a permanent guest of the management committee who does not have voting rights in the said committee). This person is generally the member of the management committee who is hierarchically responsible for the compliance function. If the financial institution is established in a form other than that of a public limited company, or if it is managed by a senior management because it does not have a management committee, the senior officer responsible for AML/CFTP should be a **member of this senior management**.

### *§2. Fit & proper-screening*

The senior officer responsible for AML/CFTP is expected to act with integrity and to possess general **AML/CFTP-related knowledge** so as to be able to critically review the measures taken by the AMLCO and to ensure compliance with the provisions of the Anti-Money Laundering Law.

For instance, the NBB expects financial institutions to perform fit & proper checks. Moreover, as member of the management committee (or member of the senior management), the senior officer is subjected to an expertise and integrity review (fit & proper screening). This review, which is not specifically AML/CFTP oriented, is performed by either the NBB or the European Central Bank (depending on the divisions of powers laid down in or pursuant to the SSM Regulation with regard to the supervision of credit institutions). The integrity and expertise requirements and the procedure for this screening are specified in Circular NBB\_2018\_25 (for credit institutions subject to the direct prudential supervision of the ECB, this circular should be read in conjunction with the SSM guide to fit and proper assessments). When financial institutions submit the fit & proper form “New appointment” for a candidate member of the management committee who is to perform the function of senior officer responsible for AML/CFTP, this should be explicitly mentioned, and the AML/CFTP-related knowledge of the person concerned should be specified. Where appropriate, the NBB may organise an interview. For current managers who have been appointed “senior officer responsible for AML/CFTP”, an e-mail notification sent to “supervision.ta.aml@nbb.be” suffices.

### *§3. Absence of conflicts of interest*

When appointing the senior officer responsible for AML/CFTP, financial institutions should avoid candidates who, as a result of any other responsibilities, could be affected by conflicts of interest that could jeopardise their AML/CFTP-related tasks. The NBB therefore recommends ensuring that the senior officer responsible for AML/CFTP **does not combine this task with other ML/FT risk-generating tasks** (such as the commercial function).

## **1.1.2. Senior officer responsible for AML/CFTP in branches established in Belgium by financial institutions governed by foreign law**

### *§1. Position in the organisational chart*

For branches established in Belgium by financial institutions governed by foreign law (by the law of an EEA country or of a third country), the senior officer is appointed among the branch’s managers. It should be recalled that, pursuant to prudential regulations, branches are required to have their own management and organisation structure on the Belgian territory.

### *§2. Fit & proper screening and absence of conflicts of interest*

As with a financial institution governed by Belgian law, the senior officer responsible for AML/CFTP of a branch should act with integrity and have adequate expertise in the area of AML/CFTP. When appointing such an officer, financial institutions should also avoid candidates who could be affected by conflicts of interest as a result of their other responsibilities. Since the NBB does not perform a fit & proper screening of a branch manager (as this screening is conducted by the Home Country Controller) in the context of its prudential supervision, the branch is expected to demonstrate, at the NBB’s first request, that it has taken measures to ensure that the person concerned has the expertise required and is not exposed to potential conflicts of interest.

## 1.2. Tasks

The legal obligation to appoint a senior officer responsible for AML/CFTP is meant to enhance the involvement of the highest hierarchical level of the financial institutions in the prevention of ML/FT risk. The NBB therefore expects the senior officer responsible for AML/CFTP to raise awareness, among the entire management committee or senior management, of the importance of this prevention and, in particular, to perform at least the following two tasks:

1. ensure that the AML/CFTP policies, procedures and internal control measures are adequate and proportionate, taking into account the characteristics of the financial institution and the ML/FT risks facing the financial institution. In this respect, the senior officer responsible for AML/CFTP is expected to pay particular attention (i) to the coherence between the AML/CFTP procedures and the more operational procedures for each activity, and (ii) to the coherence between the AML/CFTP policy and the policy implemented within the group; and
2. ensure that the person responsible for implementing the AML/CFTP policy (“AMLCO”) (i) has access to all the information necessary to perform his tasks, (ii) has sufficient human and technical resources and tools to be able to adequately perform the tasks assigned to him, and (iii) is well-informed of the AML/CFTP-related incidents brought to light by the internal control systems and of the shortcomings found by the national and foreign supervisory authorities while implementing the AML/CFTP provisions.

## 2. Appointment of the AMLCO

### 2.1. General principles

Article 9, § 2, of the Anti-Money Laundering Law stipulates that financial institutions should appoint one or more persons tasked with implementing and steering the AML/CFTP policy (“AMLCO”). In practice, this means that financial institutions should generally appoint **an AMLCO** who, depending on the nature or size of the financial institution and on its ML/FT risk profile, will head an “AML unit” or work alone.

Although the NBB recommends appointing a single person to perform the function of AMLCO within the compliance function (centralised model), this function can, when justified by the financial institution's organisation structures (e.g. due to an activity-based organisation), be assigned to **multiple persons**, each having their own area of competence (decentralised model). In that case, the following conditions should be met:

1. each AMLCO appointed meets the conditions set out in Article 9, § 2, paragraph 3, 2°, of the Anti-Money Laundering Law, and particularly those relating to the independence and autonomy of the AMLCO function (which specifically means that the AMLCO cannot depend hierarchically on an operational unit or function) as well as those relating to the position in the organisational chart and to fit & proper included in point 2.2 below; and
2. efficient coordination structures have been introduced to ensure the overall coherence of the AML/CFTP policy within the financial institution.

In this regard, the Bank has found that certain financial institutions have appointed AML correspondents in their commercial departments with whom the AMLCO collaborates to perform certain tasks in order to ensure that all measures to prevent ML/FTP are implemented effectively and adequately. Such an organisation could be appropriate for financial institutions with certain specific characteristics. However, the NBB stresses that the AMLCO function itself may not be split between a member of the compliance function and these “AML correspondents”, who are part of the commercial department and depend hierarchically on the person responsible for that department. Indeed, this hierarchical connection prevents these persons from complying with the conditions relating to the independence and the autonomy of the AMLCO function set out in Article 9, § 2, paragraph 3, 2°, of the Anti-Money Laundering Law, even though they are subject to dual reporting lines: on the one hand to the Compliance officer for the performance of their AML/CFTP-related tasks and on the other hand to the person responsible for the commercial department for their other tasks and functions. When such an organisation is chosen, the AMLCO should therefore remain fully responsible for the entire function, including the associated tasks for which he calls on these AML correspondents.

### 2.2. Terms and conditions for the appointment of the AMLCO

Article 9, § 2, paragraph 3, of the Anti-Money Laundering Law stipulates that the AMLCO function should be

effective, independent and autonomous, and that the person tasked with this function should have:

1. the professional integrity needed,
2. adequate expertise, including knowledge of the Belgian legal and regulatory AML/CFTP framework,
3. the availability, and
4. the hierarchical level and the powers within the institution to be able to propose, on his own initiative, all necessary or useful measures to guarantee the compliance and efficiency of the internal AML/CFTP measures to the board of directors and to the management committee

### 2.2.1. AMLCO in financial institutions governed by Belgian law

#### § 1. Position in the organisational chart

The AMLCO should be appointed within the compliance function and this choice should be made by the financial institution's management committee or, in the absence of a management committee, its senior management. The AMLCO can be either the person responsible for the compliance function ("N-1") or, in medium or large companies, an employee of the compliance function ("N-2").

Due to the territorial scope of the Anti-Money Laundering Law, the compliance with which the AMLCO is tasked with ensuring, on the one hand, and owing to the requirement set out in Article 9, § 2, paragraph 3, 2°, of the Anti-Money Laundering Law, which stipulates that the AMLCO should, in particular, possess the knowledge of the Belgian legal and regulatory framework and the availability needed to perform his functions effectively, independently and autonomously, and subject to the application of the principle of proportionality (see point 5 below), the AMLCO should be appointed among the employees of the financial institution who are **physically located** in Belgium.

However, the Bank draws attention to the fact that the conditions relating to the independence and autonomy of the AMLCO function set out in Article 9, § 2, paragraph 3, 2°, of the Anti-Money Laundering Law prevent this function from being conferred upon these AML correspondents, as they are subject to dual reporting lines: on the one hand to the Compliance officer for the performance of their AML/CFTP-related tasks and on the other hand to the person responsible for the commercial department for their other functions.

#### §2. Fit & proper-screening

- AMLCO who is responsible for the compliance function  
The terms and conditions for the appointment of the AMLCO are specified in Article 9, § 2, of the Anti-Money Laundering Law. Where the AMLCO is the person responsible for the financial institution's compliance function, he is subjected to the fit & proper screening performed by either the NBB or the ECB (depending on the divisions of powers laid down in or pursuant to the SSM Regulation with regard to the supervision of credit institutions). The integrity and expertise requirements applicable are specified in Circular NBB\_2018\_25 (for credit institutions subject to the direct prudential supervision of the ECB, this circular should be read in conjunction with the SSM guide to fit and proper assessments). For new appointments, the NBB asks financial institutions to explicitly mention in the "New appointment" form that the candidate is to perform the function of AMLCO.

Additionally, as regards credit institutions governed by Belgium law, stockbroking firms governed by Belgium law and insurance companies governed by Belgium law, it should be noted that, from 1 June 2018 onwards, the appointment of the person responsible for the compliance function will be conditional upon the successful completion of a qualifying exam conducted by the NBB/FSMA covering the area of AML/CFTP in particular. For instance, if a candidate for the function of person responsible for the compliance function is considered "fit" by the NBB on the basis of, in particular, having successfully completed the qualifying exam, the NBB deems this success to also be sufficient proof of the candidate's knowledge of the Belgian legal and regulatory AML/CFTP framework, which is required to take on the function of AMLCO

- AMLCO who is an employee of the compliance function  
For medium or large financial institutions where the compliance function comprises multiple persons, the AMLCO can be appointed among the employees of the compliance team ("N-2"). The terms and conditions for the appointment, which are specified in Article 9, § 2, of the Anti-Money Laundering Law, also apply in this case. However, the fit & proper screening by the NBB and the aforementioned qualifying exam are generally not performed as, in accordance with the prudential supervisory laws, these are only required for the appointment of the persons responsible for the independent control functions. As a result, the financial

institution concerned is expected to be able to demonstrate, at the NBB's first request, the measures it has taken to ensure compliance with Article 9, § 2, of the Anti-Money Laundering Law and, among other things, to ensure that the person concerned meets the conditions relating to integrity, expertise and knowledge of the Belgian legal and regulatory AML/CFTP framework, and to ensure that he has direct access to the board of directors and/or its subcommittees and has the right of initiative with regard to the aforementioned management bodies

### §3. Availability

The AMLCO should have **sufficient time** to perform his tasks correctly.

In large financial institutions and/or in institutions with a high ML/FT risk profile, the AMLCO is generally at the head of an AML unit comprising multiple members.

In medium-sized financial institutions and/or institutions with a standard ML/FT risk profile, the AMLCO to be appointed can work alone. In that case, the AMLCO function is a full-fledged function that cannot be combined with other functions (apart from the compliance function).

However, in small financial institutions and/or institutions with a low ML/FT risk profile, it may be disproportionate to entrust the AMLCO function to a person who performs it full-time. Please refer in this respect to point 4.5 below on the functions that can be combined by the AMLCO for reasons of proportionality.

#### **2.2.2. AMLCO in the branches established in Belgium by financial institutions governed by foreign law**

For branches established in Belgium by financial institutions governed by foreign law (by the law of another EEA country or of a third country), the Bank considers, as specified above, that taking into account the territorial scope of the Anti-Money Laundering Law and the legal requirements to have knowledge of the Belgian legal and regulatory framework and to have the availability required, and subject to the application of the principle of proportionality (see point 5 below), the AMLCOs of these branches should be appointed among the employees who are physically located in the branch concerned (and not among the employees who are physically located in the parent company).

It should also be ensured that the AMLCO to be appointed acts with integrity and has adequate expertise in the area of AML/CFTP. In this regard, the branch is expected to be able to demonstrate, at the NBB's first request, the measures it has taken to ensure compliance with Article 9, § 2, of the Anti-Money Laundering Law and, among other things, to ensure that the person concerned meets the conditions relating to integrity, expertise and knowledge of the Belgian legal and regulatory AML/CFTP framework, and to ensure that he has direct contact with the branch's managers as well as the right of initiative with regard to these managers.

### 2.3. Tasks

The AMLCO is responsible for the concrete steering of the AML/CFTP policy in the financial institution. He is charged, in particular, with the following tasks:

1. effectively implementing the organisational measures listed in Article 8 of the Law;
2. analysing atypical transactions and situations in which the due diligence obligations could not be fulfilled;
3. deciding to report suspicions to the CTIF-CFI, if necessary, in accordance with Article 47 of the Law, and providing the CTIF-CFI with all other information required pursuant to the Law. In this regard, the AMLCO makes the autonomous decision to report to the CTIF-CFI without submitting his decision to the senior officer;
4. educating and training the staff and, where applicable, the agents and distributors of the financial institution on AML/CFTP-related matters;
5. developing an annual AML/CFTP monitoring programme covering, in particular, the application of the required measures to prevent ML/FTP by the employees, agents and distributors who are in contact with customers, and implementing this programme;
6. ensuring a proper flow of AML/CFTP-related information within the financial institution and guaranteeing feedback to the management bodies (board of directors and management committee/senior management) and to the supervisory authorities. In this regard, the AMLCO should establish an activity report and send it to the management committee (or to the senior management if there is no management committee) and to the board of directors at least once a year (see point 2.4 below).

## 2.4. Organisation

### 2.4.1. Adequacy of human and technical resources

Financial institutions' management bodies (board of directors and management committee or senior management) should ensure that the AMLCO at all times has adequate human and material resources that enable him to comply effectively with the legal and regulatory AML/CFTP obligations. The resources allocated to AML/CFTP should be proportionate to the ML/FT risks.

### 2.4.2. Organisation of an "AML unit" or AMLCO working alone

As mentioned above, the AMLCO may, depending on the financial institution's nature or size and ML/FT risk profile, either lead an AML unit established within the compliance function or only perform the function of AMLCO.

#### §1. AML unit

In large financial institutions or institutions with a high ML/FT risk profile, the NBB recommends creating an AML unit within the compliance function, dedicated to ensuring compliance with the obligations set out in the Anti-Money Laundering Law. This unit, which is headed by the AMLCO, is comprised of persons acting with integrity who have expertise in the area of AML/CFTP. In this respect, the NBB recommends involving the AMLCO in the procedures relating to the recruitment and assignment of employees who will be part of the AML unit to be led by him. Where such a unit has been created, it is recommended for the AMLCO to coordinate the work relating to AML/CFTP and to play a central role for the most important decisions (e.g. reporting to the CTIF-CFI). The AMLCO may combine his task with that of person responsible for the compliance function, provided that the AML unit led by him is comprised of one or more persons assigned exclusively to the management of AML/CFTP-related aspects.

#### §2. AMLCO working alone

In smaller financial institutions and/or institutions with a low ML/FT risk profile, the AMLCO may be the only person in charge of all AML/CFTP-related tasks. In that case, the AMLCO constitutes a full-fledged function which, in principle, may not be combined with other functions. However, derogations are possible pursuant to the principle of proportionality (see point 5.5. below).

### 2.4.3. Interactions with AML correspondents who are in direct contact with customers

To properly fulfil the customer and transaction due diligence obligations, it could be necessary for the AMLCO to appoint AML correspondents within the financial institution's departments or among its external distributors who will act as intermediaries for all AML/CFTP-related questions. In this respect, the AMLCO should recruit persons with the most appropriate profile and ensure that they receive, upon recruitment and subsequently on an ongoing basis, useful training that is specifically adapted to the tasks expected of them with regard to due diligence (see also point 2.1.1, § 1 above).

## 2.5. Activity report by the AMLCO

Article 7 of the Anti-Money Laundering Regulation of the NBB requires the AMLCO to establish an activity report and send it to the management committee (or to the senior management if there is no management committee) and to the board of directors at least once a year. A copy of this report should be sent to the NBB (see the page "Reporting by financial institutions").

This report is an important document for the management bodies, as it allows them to properly perform their tasks. The objective is to periodically inform these bodies at the highest level of the obliged financial institution of the nature and intensity of the ML/FT risks to which it is exposed, and of the measures taken or recommended by the AMLCO to reduce and effectively manage these risks. Notwithstanding the great importance of AML/CFTP to prudential supervision (from the perspective of the compliance function), the objectives set out in the Anti-Money Laundering Law also aim to combat crime, which justifies AML/CFTP receiving a specific treatment and special attention. The NBB therefore asks that the annual report by the AMLCO is established separately from the annual activity report of the compliance function.

The NBB recommends that the annual report by the AMLCO contains at least the following information:

1. an explicit statement of whether or not a review of the overall risk assessment imposed by Article 16 of the Anti-Money Laundering Law was required for the reporting year as well as a justification of the decision taken;

2. the main conclusions of the update of the **overall risk assessment** required on the basis of Article 16 of the Anti-Money Laundering Law, where such an update has been performed in the past year;
3. a brief description of the **AML/CFTP organisation structure** and, where appropriate, of any significant changes made in the past year and of the underlying reasoning, distinguishing in particular between the organisation of the supervision by the persons who are in direct contact with customers or instructed with carrying out their transactions, and the organisation of the functions of the AMLCO;  
This description should include a brief description of the human and technical resources allocated to AML/CFTP by the financial institution, and the confirmation that these resources appear sufficient or, if that is not the case, an assessment of the additional resources that are deemed necessary to enable the financial institution to meet its AML/CFTP obligations;

Where the financial institution has tasked its senior officer responsible for AML/CFTP with performing the functions of AMLCO in accordance with Article 9, § 3, of the Anti-Money Laundering Law, the annual report contains the confirmation that the circumstances justifying this decision have remained unchanged or, if that is not the case, a description of the measures that the institution has taken or will take as a result of the changing circumstances;

Where the financial institution has decided to outsource all or some of the tasks of the AMLCO function to a third party or to another entity of the group, the annual report of the AMLCO mentions the checks performed with regard to the performance of the service provider as well as any significant incidents that have occurred in the past year in the context of the outsourcing, and contains an assessment of the completeness, timeliness and quality of the performance of the subcontractor and, where appropriate, a description of the measures taken or proposed to take full account of this assessment;

4. a brief description of any changes made to the risk-based approach implemented and to the policies, procedures, implementation processes and AML/CFTP-related internal control measures, as well as the reasoning behind these changes;
5. a structured overview of the work carried out by the AMLCO in the past year, including information on:
  1. the nature, number and amount of the atypical transactions detected and transmitted to the AMLCO for analysis,
  2. the nature, number and amount of the atypical transactions effectively analysed by or under the authority of the AMLCO,
  3. the nature, number and amount of the reports of suspicious transactions to the CTIF-CFI,
  4. the nature and number of the monitoring missions carried out with regard to the employees, agents and distributors who are in contact with customers,
  5. the nature and amount of the trainings provided and of the awareness-raising actions undertaken, and
  6. a description of any other measures adopted by the AMLCO;
6. an analysis of any AML/CFTP-related developments or trends and specific methods and means found with regard to, in particular, the type of customers, the type of transactions, the currencies concerned, or all other relevant information; and
7. all other useful information on the operation of the AMLCO function and the measures to prevent ML/FT.

Where appropriate, it could be useful for the annual report by the AMLCO to be based on the responses provided by the financial institution to the periodic or thematic questionnaires established by the NBB and completed by the institution in the past year. In this respect, see the page "Reporting by financial institutions".

The principle of proportionality should be applied when establishing the annual report. The level of information to be included in it may vary depending on the scale and diversity of the ML/FT risks to which the financial institution is exposed. For instance, the NBB expects the annual activity report by the AMLCO to be much more detailed in case of a financial institution carrying out diversified and large-scale activities, including high-risk activities, than in case of a financial institution that offers a more limited range of products and services associated with lower risks on a smaller scale. In any case, however, the annual report should contain sufficient information to enable the financial institution's senior management to form a view of the nature and intensity of the ML/FT risks to which it is exposed, as well as of the adequacy and efficiency of the ML/FT prevention mechanisms implemented in the institution and, where appropriate, of the improvements to be made to them.

### 3. Communication of the identity of the responsible persons to the NBB

The NBB expects to be notified without delay of any change in the identity of the senior officer responsible for AML/CFTP or of the AMLCO by e-mail to [supervision.ta.aml@nbb.be](mailto:supervision.ta.aml@nbb.be).

This notification should mention the effective date of appointment and the contact information (phone, e-mail) of the person concerned.

Additionally, with regard more specifically to the appointment of a new AMLCO, the notification of his appointment should also include the following information:

- Curriculum vitae ;
- Justification of the appointment in the light of the conditions listed in § 2 of Article 9 of the Anti-Money Laundering Law.

### 4. Outsourcing of tasks of the AMLCO function

Insofar as the financial institution remains fully responsible for the AMLCO function, it could be permitted, pursuant to the principle of proportionality and/or for reasons of efficiency, to outsource the executive tasks of the AMLCO function that are assigned to it by the Anti-Money Laundering Law and the Anti-Money Laundering Regulation of the NBB, in full or in part to a third party or to another entity belonging to the same group.

For more information on the principles and concrete arrangements such an outsourcing should comply with, see the page "Performance of obligations by third parties".

### 5. Application of the principle of proportionality

On the basis of the principle of proportionality, the governance obligations set out above may be nuanced in certain financial institutions governed by Belgian law or establishments in Belgium of financial institutions governed by foreign law (branches or agents/distributors of payment or electronic money institutions) that are small or medium sized and/or that fall within the scope *ratione personae* of the Anti-Money Laundering Law, but do not conduct activities in Belgium and/or are only exposed to a very limited extent to ML/FT risks in Belgium.

This can be illustrated by two specific and non-exhaustive examples:

- A credit institution or stockbroking firm governed by foreign law opens a branch in Belgium where the employees are tasked solely with finding potential customers in Belgium. However, the Belgian branch does not enter into business relationships with these customers, does not open accounts for these customers in Belgium, nor is it involved in providing financial services to these customers. Its task stops as soon as the interested potential customers have been directed to the financial institution's registered office in its country of origin (possibly through its website), which will establish the business relationship and carry out the transactions. Moreover, the Belgian branch in no way intervenes in the implementation of the measures taken by the foreign institution to comply with the anti-money laundering legislation applicable in its country of origin (customer due diligence measures, customer acceptance, transaction monitoring, etc.), unless, where appropriate, solely to collect information on the new Belgian customers of the foreign financial institution, in accordance with the latter's instructions, and only to submit this information to it (generally through its IT system). The business relationship is established and the AML/CFT measures are implemented directly between the foreign institution and the Belgian customers, pursuant to the national anti-money laundering legislation and regulations applicable to it in its country of establishment.
- A foreign supervisory authority notifies the NBB that a foreign payment institution will be offering financial services in Belgium through agents established there. On the basis of the notification received, the NBB should normally register the foreign payment institution on the official list of European payment institutions carrying out their activities in Belgium. Pursuant to the European Anti-Money Laundering Regulation and the

Belgian Anti-Money Laundering Law, the payment institution will fall within the scope *ratione personae* of the Belgian Anti-Money Laundering Law and will be subject to the NBB's supervision. Where appropriate, this European payment institution will be required to establish a "central contact point" in Belgium (see the page "Belgian central contact points of European payment institutions and electronic money institutions"). However, further investigation by the NBB shows that the Belgian agent of the foreign payment institution is tasked only with providing technical support to the foreign institution's Belgian customers (e.g. installing and repairing payment terminals) and that the Belgian agent therefore in no way intervenes in providing financial services to these customers nor is responsible for the correct implementation of the anti-money laundering legislation. It is also possible that the Belgian agent does intervene in collecting customer information for new Belgian customers of the foreign payment institution for the sole purpose of transmitting that information to the payment institution (generally through its IT system), but that further customer due diligence measures, the decision to accept the customer and the adoption of ongoing due diligence measures are left completely to the foreign institution's registered office.

In the cases described above, the NBB considers that the activities carried out by these foreign institutions in Belgium are not, or only to a very limited extent, exposed to any ML/FT risk, given that the financial services are exclusively or primarily provided from abroad and strongly resemble financial services offered from abroad under the freedom to provide services without a physical establishment in Belgium.

The NBB therefore considers that institutions which are subject *ratione personae* to the Belgian anti-money laundering legislation but which are small or medium sized and/or conduct activities in Belgium – through their establishment – that are not, or only to a very limited extent, exposed to specific ML/FT risks, can apply the principle of proportionality, in particular:

- by combining the functions of senior AML/CFTP officer and AMLCO;
- by outsourcing all or certain tasks of the AMLCO function;
- by simultaneously combining the functions of senior officer responsible for AML/CFTP and AMLCO and outsourcing all or part of the AMLCO's tasks;
- by submitting a request for derogation from certain reporting obligations to the NBB (for more information on the reporting obligations and the request for derogation, see the page "Reporting by financial institutions").

### 5.1. Assessment of the principle of proportionality in AML/CFTP

The NBB verifies whether the conditions for the application of the principle of proportionality in AML/CFTP are met, particularly on the basis of the following indicative criteria:

- a) the **nature of the institution**, taking into account its prudential status, its legal form, whether or not it belongs to a group, and its business model;
- b) the **size of the institution**, taking into account its balance sheet total, its turnover, the number of its full-time equivalent employees and its management structure;
- c) the **nature and complexity of its transactions** from the perspective of the ML/FT risks to which it is exposed; and
- d) **in the case of an establishment in Belgium of a financial institution governed by foreign law** (of another EEA country or of a third country), the reasons for creating the Belgian establishment and the functions and tasks assigned to it, particularly in the context of the implementation of the institution's AML/CFT policies and procedures.

In any case, a financial institution intending to make use of this possibility should be able to demonstrate to the NBB that its intended proportionate terms for the implementation of its obligations are appropriate in view of, in particular, the criteria above.

### 5.2. Combination of the functions of senior officer responsible for AML/CFTP and AMLCO

On the basis of the principle of proportionality, Article 9, § 3, of the Anti-Money Laundering Law enables financial institutions to have the function of senior officer responsible for AML/CFTP and of AMLCO performed by the same person, where justified by the nature or size of the obliged entity.

If a financial institution wishes to make use of this possibility, it is expected to compile a dossier in which (i) it demonstrates that this choice meets the proportionality criteria set out in point 5.1 above and (ii) it specifies why it wishes to apply Article 9, § 3, of the Law. This dossier should be available for submission to the NBB at its first request. Furthermore, the institution should regularly reassess whether the circumstances which justified the application of Article 9, § 3, of the Anti-Money Laundering Law still apply. If not, the financial institution should take the measures necessary for the separate appointment of a senior officer responsible for AML/CFTP in accordance with Article 9, § 1, of the Anti-Money Laundering Law, on the one hand, and of an AMLCO in accordance with Article 9, § 2, of the Anti-Money Laundering Law, on the other. In addition, the financial institution should immediately notify the NBB.

If the possibility to combine functions as laid down in Article 9, § 3, of the Anti-Money Laundering Law is used, the senior officer acting as AMLCO should be appointed among the members of the financial institution's management committee or its senior management, or among the branch's managers. A fit & proper screening should be performed and it should be ensured that the senior officer acting as AMLCO cannot be affected by conflicts of interest as a result of any other responsibilities. The rules set out in point 1.1 above regarding the senior officer responsible for AML/CFTP apply by analogy.

The senior officer acting as AMLCO should perform the tasks referred to in points 1.2 and 2.2 above.

### 5.3. Outsourcing

Pursuant to the principle of proportionality and/or for reasons of efficiency, financial institutions may be authorised to use outsourcing. Please refer to point 4 above and to the page "Performance of obligations by third parties".

### 5.4. Simultaneous use of the possibility to (i) combine the functions of senior officer responsible for AML/CFTP and AMLCO and (ii) outsource all or part of the AMLCO's tasks

Financial institutions governed by Belgian law or branches established in Belgium of a **very small size** that have a **low ML/FT risk profile** may make simultaneous use of the possibilities specified in points 5.2 and 5.3 above on the basis of the principle of proportionality.

In that case, the financial institutions concerned (governed by Belgian law or branches) should compile a dossier in which they demonstrate that the conditions set out in points 5.2. and 5.3. are met. This dossier should be available for submission to the NBB at its first request.

In that case, the senior officer acting as AMLCO (member of the management committee or of the senior management) within the financial institution or the branch should have the ultimate responsibility for all important AML/CFTP-related decisions, in addition to its task to monitor the quality of the outsourced services).

### 5.5. Combination of functions by the AMLCO

As mentioned above, in large financial institutions and/or in institutions with a high ML/FT risk profile, the AMLCO is generally at the head of an AML unit comprised of multiple members. In that case, the AMLCO function can only be combined with the function of person responsible for the compliance function.

For **medium-sized** financial institutions and/or institutions with a standard ML/FT risk profile, the AMLCO to be appointed may work alone. In that case, the AMLCO function is a full-fledged function that cannot be combined with other functions (apart from the compliance function).

However, in financial institutions governed by Belgian law or branches established in Belgium by foreign financial institutions of a **small size** and/or institutions with a low ML/FT risk profile, it may be disproportionate to entrust the AMLCO function to a person who performs it on a full-time basis. In that case, it may be appropriate to attribute this function to a person who only performs it part-time, in combination with other functions in the Belgian entity concerned or in other entities of the same group. The NBB considers that such governance rules, which are applied on the basis of the principle of proportionality, require that the following conditions, which result from the nature of the AMLCO function and from the application of Article 9, § 2, of the Anti-Money Laundering Law, be met:

1. These governance rules meet the proportionality criteria set out in point 5.1. above;
2. The other functions performed by the person concerned in the same entity or in another entity of the same group are not such as to expose them to conflicts of interest; from this viewpoint, the functions of AMLCO or

of person responsible for the compliance function in another entity of the same group may be considered compatible with the function of AMLCO of the Belgian entity;

3. The person concerned should spend sufficient time performing the AMLCO function in the Belgian entity in order to meet the availability condition set out in Article 9, § 2, paragraph 3, 2°, of the Anti-Money Laundering Law;
4. If the person concerned does not usually perform his AMLCO function in the Belgian entity, this geographic distance is without prejudice to the effective performance of this function, to the availability and to the knowledge of the Belgian legal and regulatory ML/FTP prevention framework, which are required by Article 9, § 2, paragraph 3, 2°, of the Anti-Money Laundering Law.

A financial institution wishing to apply these governance rules should compile a dossier demonstrating that all these conditions are met. This dossier should be available for submission to the NBB at its first request.

## 5.6. Senior officer responsible for AML/CFTP and AMLCO in European payment or electronic money institutions that provide payment services or distribute electronic money in Belgium solely through agents or distributors

For European payment institutions or electronic money institutions operating in Belgium through independent agents or distributors, the obligations to appoint a senior officer responsible for AML/CFTP and an AMLCO as laid down in Article 9 of the Anti-Money Laundering Law should be interpreted taking into account the specific characteristics of the presence of these financial institutions on the Belgian territory as well as the principle of proportionality.

The NBB should in any case be informed of the identity and the function of the person who, at the head office of each of these institutions and in accordance with the law applicable in his country of origin, is responsible at the highest level for ensuring that the provisions of the Anti-Money Laundering Law and the other legal and regulatory provisions referred to in Article 9, § 1, paragraph 1, of the Law are implemented and complied with in Belgium.

Moreover, where the institution is required to appoint a CCP in Belgium, it should appoint a person established in Belgium, in accordance with Article 9, §§ 2 and 4, of the Law, to perform the functions of the CCP.

For more information on the obligation to appoint a CCP, see the page “Belgian central contact points of European payment institutions and electronic money institutions”.

## 5.7. Reporting to the NBB

For the possibility of requesting a derogation from certain reporting obligations to the NBB, see the page “Reporting by financial institutions”.

# 6. Other governance requirements

The specific AML/CFTP-related governance requirements should be integrated harmoniously into all prudential governance rules applicable to the different sectors concerned.

## 6.1. AML/CFTP tasks of the board of directors

A financial institution's board of directors has the following AML/CFTP tasks:

- deciding on the overall ML/FT risk management strategy of the financial institution concerned. The board of directors should therefore have an overall view of the policy implemented and of the ML/FT risks associated with the activities performed;
- validating the institution's AML/CFTP policy (see the page “Policies, procedures, processes and internal control measures”);
- being informed of the results of the institution's overall ML/FT risk assessment and its update;
- approving the AMLCO's activity report at least once a year;
- assessing the proper functioning of the compliance function, including its AML/CFTP component, at least once a year, ensuring in particular the adequacy of the human and technical resources allocated to the AMLCO function.

## 6.2. AML/CFTP tasks of the management committee

A financial institution's management committee or, if it does not have a management committee, its senior management has the following AML/CFTP tasks:

1. implementing, at the instigation of the senior officer responsible for AML/CFTP, the organisational and operational AML/CFTP structure necessary to comply with Article 8 of the Anti-Money Laundering Law and with the AML/CFTP strategy defined by the board of directors, paying particular attention to the adequacy of the human and technical resources allocated to the AMLCO function;
2. approving the internal AML/CFTP procedures (see the page "Policies, procedures, processes and internal control measures", which stipulates that minor changes to these procedures can be validated by the senior officer responsible for AML/CFTP);
3. implementing adequate AML/CFTP-related internal control mechanisms (see the page "Policies, procedures, processes and internal control measures");
4. approving the AMLCO's annual activity report and being in regular contact with the AMLCO;
5. annually assessing the efficiency of its governance system, including the AML/CFTP policy; and
6. ensuring proper AML/CFTP reporting to both the board of directors and the NBB.

### 6.3. Adherence to compliance rules

Since the AML/CFTP policy should be integrated into the compliance function, the principles included in Circular NBB\_2012\_14 are applicable. Moreover, the prudential rule stipulating that all independent control functions should form a coherent whole, also applies, requiring a good interaction between the compliance function and the risk management function with respect to ML/FT risks (but without creating a hierarchy between these independent control functions).

Although ML/FT risk management is the subject of specific reports submitted to the NBB, the NBB expects the compliance function to also cover this aspect in the context of its reporting on compliance. However, the use of cross-references is allowed in this reporting for AML/CFTP-related aspects.

#### **Reference documents:**

- Guidelines of the European Banking Authority of 25 February 2019 (EBA/GL/2019/02) on outsourcing arrangements (for credit institutions, stockbroking firms, payment institutions and electronic money institutions);
- Circular NBB\_2018\_25 regarding suitability of directors, members of the management committee, responsible persons of independent control functions and senior managers of financial institutions;
- Circular NBB\_2012\_14 on the compliance function;
- the sectoral circulars on outsourcing:
  - for credit institutions and stockbroking firms: Circular PPB\_2004\_5 regarding sound management practices in outsourcing by credit institutions and investment firms,
  - for insurance companies: Circular NBB\_2016\_31 on the prudential expectations of the NBB as regards the governance system for the insurance and reinsurance sector,
  - for payment institutions and electronic money institutions: the aforementioned Circular PPB\_2004\_05, which is made applicable by Circulars NBB\_2015\_09 on the prudential status of electronic money institutions and NBB\_2015\_10 on the prudential status of payment institutions,
  - for settlement institutions: Circular PPB\_2007\_5 on internal control and internal audit, compliance function, prevention policy, sound management practices in outsourcing;
- The sectoral circulars on governance:
  - for credit institutions, stockbroking firms, payment institutions and electronic money institutions, settlement institutions and assimilated institutions: the governance manual,
  - for insurance companies: the aforementioned Circular NBB\_2016\_31.

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



## Risk classification

Home > Financial oversight > Combating money laundering and the financing of terrori...

### Legal and regulatory framework

- Anti-Money Laundering Regulation of the NBB: Article 4

### Comments and recommendations by the NBB

As an extension of the overall assessment of ML/FT risks, which must be performed in accordance with Article 16 of the Anti-Money Laundering Law, financial institutions are required, pursuant to Article 4 of the Anti-Money Laundering Regulation of the NBB, to define different risk categories and to apply appropriate due diligence measures specific to each category. These risk categories must specifically reflect each risk identified in the above-mentioned overall risk assessment and be based on objective risk factors that are combined in a consistent manner (cf. in particular the variables and risk factors referred to in Annexes I to III of the Law).

Based on the above, the risk classification should in theory include at least two risk categories (high and standard risk) and possibly a third one (low risk). However, it is important to note that this classification must ensure that appropriate due diligence measures are implemented in each situation. Regardless of the classification technique used, each financial institution must be able to demonstrate that its risk classification permits this objective to be attained (Art. 17, paragraph 2 of the Law). Hence it may be useful to classify situations which require identical due diligence measures in the same risk category. In that case, the number of risk categories will correspond to the number of risk situations requiring different risk mitigation measures. Thus, if several risks considered as high require different risk mitigation measures, depending on the nature of the risks concerned, it would be useful, in practice, to create the same number of corresponding risk categories. However, according to this principle, a risk classification comprising only two risk classes (high and standard risk) would only be relevant in the case of a financial institution whose overall risk assessment shows that it is essentially exposed to very homogeneous ML/FT risks which should not be considered as high, taking into account the homogeneity, from a risk viewpoint, of its activities, its customers, its distribution channels and the geographical areas concerned. In this case, although its overall risk assessment may lead it to consider that, as a general rule, all business relationships or transactions with its customers should in theory be qualified as "standard risks" and could therefore all be grouped into a single risk class and be subjected to a single set of risk reduction measures, this financial institution should also provide for a "high risks" category, which should contain business relationships or transactions that are found in the individual risk assessment to deviate from the forecast based on the overall risk assessment, so that enhanced due diligence measures are required.

From this perspective, it should be noted that, in accordance with Article 4 of the NBB Regulation, financial institutions should ensure that the risk categories they define enable them, if necessary, to classify a customer in a risk category other than that in which he should in theory be classified, if they identify, in the context of the individual risk assessment carried out in accordance with Article 19, § 2 of the Anti-Money Laundering Law, cases of high risk or cases of low risk. The definition of risk categories should also allow financial institutions to take into account the cases of enhanced due diligence referred to in Articles 37 to 41 of the Law.

While the risks specific to each institution must in the first place be reflected in the classification, based on the overall assessment performed by the institution concerned, a concrete analysis of the level of risk presented by each customer may have to lead to a shift from one risk category to another, that is different from the first category in which the risk would have been classified a priori according to the overall assessment.

Finally, each risk class must be matched by appropriate measures to manage the ML/FT risks thus identified and classified. These measures include, in particular, the customer acceptance policy and the due diligence measures (see page "Policies, procedures, processes and internal control measures").

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



# NBB anti-money laundering regulation of 21 November 2017 - Article 4

## Art. 4

Obligated financial institutions shall define different categories of risk to which they shall apply appropriate customer due diligence measures.

They shall base the definition of these risk categories on the overall risk assessment referred to in Article 16 of the Law and on objective risk criteria that are combined in a consistent manner.

Furthermore, they shall ensure that these risk categories enable them to take account of:

1° cases of high risk identified pursuant to Article 19, § 2, of the Law and, at the very least, referred to in Articles 37 to 41 of the Law;

2° if necessary, cases of low risk identified pursuant to Article 19, § 2, 2nd indent, of the Law.



# Policies, procedures, processes and internal control measures

Home > Financial oversight > Combating money laundering and the financing of terrori...

## Legal and regulatory framework

- Anti-Money Laundering Law: Articles 8, 10 and 12
- Anti-Money Laundering Regulation of the NBB:
  - Articles 8 to 18 and 22 to 24: internal procedures
  - Articles 19 to 21: performance by third parties

## Explanatory Memorandum of the Anti-Money Laundering Law

- Articles 8, 10 and 12

## Other reference documents

- ESAs Opinion dated 23 January 2018 on the use of innovative solutions by credit and financial institutions

## Comments and recommendations by the NBB

- Comments and recommendations

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



# Anti-Money Laundering Law of 18 September 2017 - Articles 8, 10 and 12

## Art. 8

§ 1. Obligated entities shall develop and implement policies, procedures and internal control measures that are efficient and commensurate with their nature and size:

1° in order to comply with the provisions of this Law, of its implementing decrees and regulations and of the implementing measures of Directive 2015/849, and in order to efficiently manage and mitigate the relevant risks identified at the level of the European Union, of Belgium and of the obliged entity itself;

2° in order to comply, where appropriate, with the provisions of the European Regulation on transfers of funds;

3° in order to comply with the mandatory provisions on financial embargoes.

§ 2. The policies, procedures and internal control measures referred to in § 1 shall include:

1° developing policies, procedures and internal control measures relating in particular to model risk management practices, customer acceptance, due diligence towards customers and transactions, reporting of suspicions, record-keeping, internal control, management of compliance with the obligations set out in this Law, in its implementing decrees and regulations and in the European Regulation on transfers of funds, as well as with the restrictive measures referred to in § 1, 3°;

2° where appropriate with regard to the nature and size of the obliged entity, and without prejudice to the obligations laid down by or pursuant to other legislative provisions:

a) an independent audit function charged with testing the policies, procedures and internal control measures referred to in 1°;

b) procedures for verifying, when recruiting and assigning staff or appointing agents or distributors, whether these persons have adequate integrity considering the risks associated with the tasks and functions to be performed;

3° educating the obliged entity's staff and, where appropriate, its agents or distributors, on ML/FT risks, and training these persons with regard to the measures implemented to reduce such risks.

§ 3. Obligated entities shall submit the policies, procedures and internal control measures implemented by them for approval to a higher ranked member of their hierarchy, pursuant to paragraph 1.

§ 4. Obligated entities shall verify the relevance and efficiency of the measures taken to comply with this article and shall, where appropriate, improve these measures.

## Art. 10

Obligated entities shall develop and implement procedures that are appropriate and commensurate with their nature and size, in order to enable their staff or their agents or distributors to report non-compliance with the obligations set out in this Book to the persons appointed pursuant to Article 9 through a specific, independent and anonymous channel.

## Art. 12

Where a natural person falling within any of the categories of obliged entities listed in Article 5, § 1, 23° to 25°, performs professional activities as an employee of a legal person, the obligations in this Chapter shall apply to that legal person rather than to the natural person.

# Explanatory Memorandum to the Anti-Money-Laundering Law of 18 September 2017 - Articles 8, 10 and 12

## Art. 8

The obligation set out in Article 16, § 1 of the Law of 11 January 1993 for the obliged entities to implement effective policies, procedures and internal control measures is taken over and detailed further in this Article of the draft Law. This Article also transposes Article 8, paragraph 3 of Directive 2015/849.

It should be noted that, in accordance with the provisions of the aforementioned Article of the Directive, § 1 expressly sets out that the policies, procedures and internal control measures to be implemented must be commensurate with the nature and scale of the entity concerned. Small-scale obliged entities that exercise relatively simple activities cannot after all be required to use mechanisms as complex as those required of large-scale obliged entities that exercise very diverse and sophisticated activities, in order to achieve the objectives laid down by this Article of the draft Law. All obliged entities must therefore establish their own internal policies, procedures and internal control measures, taking into account their specific characteristics, with which they can prove — especially to their supervisory authority — that the organisation they have set up is suitable and effective in view of the objectives laid down in the draft Law. To take into account the specific characteristics of the various categories of obliged entities, as stated above, the supervisory authorities referred to in Article 85 of the preliminary draft may, where applicable, determine the methods for implementation of this principle of proportionality, taking into account the characteristics of the sector of activity concerned, by using the regulatory powers granted to them by Article 86, § 1, or where it appears necessary, address recommendations on the subject to the obliged entities under their supervision, pursuant to § 2 of the same Article.

As regards the objectives sought, it should be noted that this draft Article considerably broadens the objectives to be achieved as compared with Article 16, § 1 of the Law of 11 January 1993.

As already set out in the Law of 11 January 1993, § 1, 1° of this Article of the draft Law specifies that the internal organisation of the obliged entities must enable them in the first place to comply with their obligations as regards prevention of ML/TF, as provided for in the draft Law or in its implementing Decrees and Regulations. This legal requirement to have an appropriate organisation relates to the entire ML/TF prevention process, all the way from customer identification, knowledge and acceptance, to the reporting of suspicious transactions to the CTIF-CFI, in accordance with draft Articles 47 et seq., which arises from the supervision of the transactions executed by the customer and from the analysis of atypical transactions, especially those that do not appear to be in line with what the obliged entity knows about the customer. Such an internal organisation should from now on enable them also to comply with the implementing measures of Directive 2015/849, including the European regulatory technical standards relating to AML/CFT. In this respect it should be noted that Directive 2015/849 set outs that the European Supervisory Authorities (hereinafter the 'ESAs') shall develop proposals for such regulatory technical standards to provide for an appropriate framework on the subject of AML/CFT for subsidiaries and branches established by European financial institutions in high-risk third countries (Article 45, paragraph 6), and develop a framework for the option offered to Member States to require, in certain circumstances, that payment institutions or electronic money institutions governed by the law of another Member State indicate a central contact point on their territory (Article 45, paragraph 10). When these are approved by the European Commission, these regulatory technical standards ensuring maximum harmonisation at an EEA-level of the provisions that apply in this matter, shall apply directly to the obliged entities concerned. The organisational measures taken by these latter must therefore also enable them to comply with these standards.

These organisational measures that the obliged entities must take under this provision of the draft Law seek not only to guarantee that the conduct of these latter is in accordance with their legal and regulatory obligations from a legal standpoint. These measures essentially seek to mitigate and effectively manage the ML/TF risks identified at a European and Belgian level as well as at the level of the obliged entity itself. It should be noted that the said objective is substantially taken over from Article 16, § 1 of the Law of 11 January 1993 (which determines that the objective consists of identifying and preventing transactions relating to ML/TF), while avoiding being interpreted as an obligation of result, which would be incompatible with a risk-based approach.

In addition to compliance with the provisions of the draft Law and the other provisions under 1°, points 2° and 3° under § 1 of this draft Article intend to ensure the overall coherence of the AML/CFT mechanisms applied by the obliged entities, by extending the objectives that their organisational measures should achieve to compliance with the EU Funds Transfer Regulation as well as the Belgian legal provisions and binding provisions on financial embargos. By including these subjects in Article 8, § 1 of the draft Law, a solution is provided to the difficulties that could arise previously, especially in the financial sector, as a result of the fact that the obligation to have an appropriate organisation to comply with the obligations regarding electronic funds transfers or targeted financial sanctions was based on the different prudential laws and legislation and not on the Law of 11 January 1993.

The term 'European Regulation on transfers of funds' is defined in Article 4, 5° of the draft Law. This term enables reference to be made successively to Regulation (EC) No 1781/2006 of the European Parliament and of the Council of 15 November 2006 on information on the payer accompanying transfers of funds, which will still be in force on the date of approval of the present Law and, from 27 June 2017, to Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006.

The term 'binding provisions on financial embargoes' is defined in Article 4, 6° of the draft Law, by reference to the nature of the obligations imposed by these regulations and the objectives they seek to achieve, i.e. combating terrorism and the financing thereof and combating the proliferation of weapons of mass destruction.

These binding provisions include, at European Union level, the EU regulations that lay down financially restrictive measures against countries, entities or individuals as part of the fight against terrorism, terrorist financing or financing of the proliferation of weapons of mass destruction. The European Union lays down these measures either to implement the decisions adopted by the Security Council pursuant to Chapter VII of the United Nations Charter, or on its own initiative by using the possibilities offered by the European Treaties. In such a case, the European Union takes restrictive measures that have not been decided upon by the Security Council or that go further than the measures decided upon by the Security Council.

At Belgian level, these relate firstly to measures that can be imposed by the Statutory Order of 6 October 1944 establishing monitoring of all possible transfers of goods and assets between Belgium and other countries, and its implementing Decrees.

Secondly, they relate to restrictive measures under the Law of 11 May 1995 on the enforcement of the resolutions adopted by the United Nations, under which the King and the Minister of Finance have the power to immediately freeze the financial assets of persons, entities and groups indicated by the decisions of the United Nations. The decisions of the United Nations Security Council are applied very strictly. There are no additional national measures taken and the targeted persons, entities and groups are only those indicated by the United Nations itself. These relate to the restrictive measures in force during the period in which the European Union has not yet executed the financial sanctions imposed.

Thirdly, they relate to enforcement of the restrictive measures imposed by the Council of the European Union as provided for in the Law of 13 May 2003 on the enforcement of the restrictive measures taken by the Council of the European Union against States, some persons and entities.

Finally, they relate to the restrictive measures imposed by the Royal Decree of 28 December 2006 on specific restrictive measures directed against certain persons and entities with a view to combating the financing of terrorism.

Article 3 stipulates that: "The assets and economic resources of the persons and entities that commit or attempt to commit, facilitate or collaborate with terrorist offences, not referred to in Common Position 2001/931/CFSP, in Regulation (EC) No 2580/2001 or in Regulation (EC) No 881/2002, and included in the list in annex, drawn up by the National Security Council based on the evaluations of the Coordination Unit for Threat Analysis, after consultation

with the competent judicial authority and approved by the Council of Ministers, shall be frozen. Wherever necessary, the National Security Council will add new names of persons or entities to the list in accordance with the same procedure”.

The list referred to here is the national list of persons and entities whose assets in Belgium are frozen. The administrative freezing of the assets referred to in Article 3 of the aforementioned Royal Decree is a preventive measure against terrorism and the financing thereof.

This general definition of financial embargoes enables account to be taken of the frequency with which new European regulations and Belgian legislation and regulations on the subject are approved.

The updated list of the European regulations and Belgian legislation and regulations concerned, as well as a consolidated version of the national list, can be found on the following website:

<https://finance.belgium.be/en/treasury/financial-sanctions>.

Paragraph 2 of the same Article, which transposes Article 8, paragraph 4 of Directive 2015/849, specifies what must be understood by “policies, procedures and internal control measures referred to in § 1”, recalling that these policies, procedures and internal control measures under this first paragraph must be commensurate with the nature and scale of the entity referred to.

In the first place, it refers to the development of risk management models in the area of ML/TF. Principally it is a question of determining the method for making an inventory of — and measuring — the risks concerned and determining the risk variables used therein.

The obliged entities must also establish a ‘customer acceptance policy’. The aim of this is essentially to divide customers into several risk classes based on the aforementioned risk management model, and to establish, for each of these, appropriate procedures and methods for entering into business relationships with or executing transactions for these customers. These methods must mitigate the risk that the obliged entity involuntarily become involved in ML/TF transactions. Where appropriate, this customer acceptance policy may determine the situations in which the obliged entity does not deem itself able to sufficiently mitigate the risk and in which it consequently refuses, based on a case-by-case analysis and justification, to enter into business relationships or execute transactions with or for the person concerned.

For the rest, the internal procedures of the obliged entity must describe in detail how it works in practice to comply with all of its obligations regarding AML/CFT (especially its due diligence obligations relating to customers and transactions, the obligation to report suspicions as referred to in Book II, Title 4, Chapter 2 of this draft Law, and the obligation to keep documents and evidence). They must also encompass the application of the provisions on embargoes and freezing of assets and, where applicable, the obligations regarding electronic funds transfers. These procedures must be complied with by the members of staff of the obliged entity and by all persons who act in its name and on its behalf.

Finally, the obliged entities must establish internal control measures to enable them to ensure effective compliance with the aforementioned internal procedures.

If justified by the nature and scale of the obliged entity, and without prejudice to the application of other legislation (especially the Banking Law and the Law on the supervision of insurance companies), the aforementioned measures must be complemented with the establishment of an independent audit function to ensure the effective enforcement and the effectiveness of the aforementioned policies, procedures and internal control measures.

In view of the nature of ML/TF prevention, the effective application of the organisational measures described above could be undermined if the persons tasked with them in their capacity of member of staff, agent or distributor do not exhibit appropriate integrity for the risks associated with the tasks and functions to be exercised. The draft Law therefore requires, where appropriate pursuant to the nature and scale of the obliged entity, that these latter apply procedures for the verification of these integrity requirements at the time of recruiting persons, and of their designation for tasks or functions within which they could be exposed to the risk of ML/TF.

Furthermore, the obliged entity’s effective and efficient enforcement of the organisational framework regarding ML/TF assumes that these same persons have a good understanding of the ML/TF risks with which they may be confronted and that they have good knowledge of the measures taken by the obliged entity to be able to face these

risks. Just as in Article 17, first paragraph of the Law of 11 January 1993, Article 8, § 2, 3° of the draft Law therefore imposes on the obliged entities the obligation to educate and train the persons concerned. The terms of this obligation are set out in detail in Article 11 of the draft Law.

In accordance with Article 8, paragraph 5 of Directive 2015/849, draft Article 8, § 3 lays down that the organisational measures described hereinabove must be approved by a higher ranked member of their hierarchy of the obliged entity to guarantee that the senior management of the latter supports these measures and uses its authority to enforce compliance therewith. Where the obliged entity consists only of one natural person, it obviously refers to that person.

Finally, § 4 of the draft Article lays down that the obliged entities must verify the relevance and efficiency of the aforementioned organisational measures to prevent ML/TF and that they must, where appropriate, improve these. Such adjustments may be necessary, for example, to take into account the evolution of the context in which the obliged entity exercises its activities, or the evolution of the entity itself, or the nature and scale of its activities, etc. Even in the absence of such changes, the obliged entities must regularly assess the effectiveness of the measures they take in order to identify and remedy any potential shortcomings.

## Art. 10

Article 10 of the draft Law transposes Article 61, paragraph 3 of Directive 2015/849 and imposes on obliged entities the obligation to provide for internal mechanisms commensurate with their nature and scale and which enable their staff and, where applicable, their agents and distributors, to report breaches of obligations regarding AML/CFT which they may have identified, to the senior manager responsible and to the AMLCO. These internal reports must be able to be anonymous and sent to their addressees through a specific and independent channel, which entails that they must be able to be sent directly to them rather than going through the hierarchy. It should be noted that, in the same way as for the application of draft Articles 8 and 9, the principle of proportionality and consequently the comments provided above on this subject, also apply to internal procedures for reporting breaches.

## Art. 12

Draft Article 12 relates to the obliged entities listed in draft Article 5, § 1, 23° to 25° and transposes Article 46, point 1, third paragraph of Directive 2015/849 which provides for the following: "Where a natural person falling within any of the categories listed in point (3) of Article 2(1) performs professional activities as an employee of a legal person, the obligations in this Section shall apply to that legal person rather than to the natural person". Lawyers, bailiffs, notaries, and estate agents always have an independent status even if they exercise this activity for a legal firm which is a legal person, for a notary firm or bailiff firm, or an estate agent. It is a different matter, however, for accounting professions. They may have the title of company auditor, auditor, chartered accountant or tax consultant and exercise that profession as an employee of a company that also has the capacity of company auditor, audit firm, chartered accountant or tax consultant.



# NBB anti-money laundering regulation of 21 November 2017 - Articles 8 to 24

## Art. 8

§ 1. Obligated financial institutions shall adopt and implement a customer acceptance policy that is appropriate to the activities they carry out, enabling them to subject the entry into business relationships with customers or the conclusion of occasional transactions on behalf of customers to a prior examination of any ML/FT risks associated with the customer's profile and with the nature of the business relationship or the occasional transaction requested, as well as to take measures seeking to reduce the risks identified.

§ 2. The customer acceptance policy shall notably enable obliged financial institutions to extend full support to the prevention of ML/FT through appropriate examination of the characteristics of their customers, the products, services or transactions that they offer, the countries or geographical areas concerned and the distribution channels that they use.

In their customer acceptance policy, obliged financial institutions shall split customers into the different risk categories referred to in Article 4.

§ 3. The customer acceptance policy shall also make it possible to implement binding provisions on financial embargoes.

## Art. 9

The customer acceptance policy of obliged financial institutions shall submit to an appropriate examination and to a decision at an appropriate management level, acceptance of customers who are likely to present a particular risk, notably those:

1° who are identified as presenting a high risk pursuant to Article 19, § 2, of the Law and, at the very least, those referred to in Articles 37 to 41 of the Law;

2° who request opening of numbered accounts or conclusion of numbered contracts referred to in Article 11.

If necessary, it shall take account of the fact that it has not been possible to gather relevant information about the customer's address or, where required, the date and place of birth of one of the beneficial owners of the customer, to determine whether the measures referred to in the first paragraph should be applied to the customer in question.

## Art. 10

Obligated financial institutions shall identify and verify the identity of customers in accordance with Articles 26 to 32 of the Law when there are reasons to doubt that the person wishing to carry out a transaction under a business relationship entered into previously is actually the customer identified for this business relationship or his/her authorised and identified representative.

## Art. 11

The opening of numbered accounts for customers or the conclusion of numbered contracts shall be subject to the condition that the internal procedures set by the obliged financial institution pursuant to Article 8 of the Law stipulate:

1° the conditions under which these accounts may be opened or these contracts concluded;

2° the terms of operation;

3° that these conditions and terms should be without prejudice to the obligations arising from the provisions laid down in Article 8, § 1, of the Law and in this Regulation.

## Art. 12

The internal procedures defined by the obliged financial institution pursuant to Article 8 of the Law shall also provide for:

1° precise rules concerning supporting documents or reliable and independent sources of information accepted by the obliged financial institution for the purposes of verification of identity pursuant to Article 27, § 1, of the Law, depending on the characteristics of the persons in question, the individual risk assessment made pursuant to Article 19, § 2, of the Law, and the risk classification carried out pursuant to Article 4 of this Regulation.

For the purposes of verification of identity, a specific identification technology may be accepted as a supporting document or reliable and independent source of information within the meaning of the above-mentioned Article 27, § 1, of the Law, if an analysis of the reliability of this technology so justifies;

2° if the individual risk assessment conducted in accordance with Article 19, § 2, 1st indent, of the Law, shows that the risk associated with the customer and the business relationship or the occasional transaction is low:

information which, pursuant to Article 26, § 3, of the Law, must not be collected by the obliged financial institution;

information which, pursuant to Article 27, § 3, of the Law, must not be verified;

3° if the individual risk assessment conducted in accordance with Article 19, § 2, 1st indent, of the Law, shows that the risk associated with the customer and the business relationship or the occasional transaction is high:

information which, pursuant to Article 26, § 4, of the Law, is considered by the obliged financial institution as enabling an indisputable distinction of the person concerned from anyone else, as well as any additional information to be collected if necessary;

the measures to be taken by the obliged financial institution paying particular attention to ensure that the documents or sources of information used to verify this information enable it, pursuant to Article 27, § 4, of the Law, to acquire a high degree of certainty as to its knowledge of the person concerned;

4° the measures to be taken by the obliged financial institution when it identifies the agent(s) of a customer, pursuant to Article 22 of the Law, the representative(s) of a customer, and verifies their identity, to ascertain the powers of representation of the person(s) concerned;

5° the measures to be taken by the obliged financial institution to understand, pursuant to Article 23, § 1, 2nd indent, of the Law, the ownership and control structure of the customer or of the agent who is a company, a legal person, a foundation, a fiducie, a trust or a similar legal arrangement;

6° the measures to be taken by the obliged financial institution to identify and verify the identity of the beneficial owners of its customers, agents of its customers or beneficiaries of life insurance contracts, in addition to consultation of the registers referred to in Article 29 of the Law, if necessary.

## Art. 13

Without prejudice to the identification and verification of the identity of customers who are professional counterparties, as well as their beneficial owners, in accordance with Articles 21, 23 and 26 of the Law and this Regulation, and provided that the obliged financial institutions which establish a relationship with these counterparties or carry out transactions with them shall ensure that they themselves and their transactions do not present high ML/FT risks, obliged financial institutions may extend identification of customers' employees who they have mandated to conclude transactions on their behalf to cover the last name, first name, date and place of birth and the rank or functions of these employees in the customer chart, with the exception of their address.

The internal procedures of obliged financial institutions that make use of the option provided for in the first paragraph shall list exhaustively the categories of professional counterparties, as well as the categories of business relationships or transactions, to which these specific terms for the identification and verification of the identity of customers' agents may be applied.

## Art. 14

Obliged financial institutions which make use of the derogation provided for in Article 31 of the Law and verify the identity of persons referred to in Articles 21 to 24 of the Law in the course of the business relationship shall determine, in their internal procedures, appropriate measures guaranteeing that the conditions set out in the above-mentioned Article 31 are met.

## Art. 15

If obliged financial institutions cannot fulfil their obligations to identify and verify the identity of a customer, or the customer's agents or beneficial owners within the time limits referred to in Articles 30 and 31 of the Law, or their obligations to keep these identification data up to date in accordance with the Law, they may apply restrictive measures as an alternative to ending the already established business relationship, as required pursuant to Article 33, § 1, 1st indent, of the Law, if it consists of:

1° a life insurance contract, unilateral termination of which is contrary to other mandatory legal or regulatory provisions or public policy provisions. In this case, the obliged financial institution may refuse payment of any supplementary premium by the policyholder, without prejudice to the consequences that the legal or regulatory provisions attach to non-payment of a premium;

2° a loan contract, unilateral termination of which would expose the obliged financial institution to a severe and disproportionate negative impact. In this case, the obliged financial institution shall refuse any increase in the amount lent and shall terminate the business relationship as soon as possible.

In the cases referred to in the 1st indent, obliged financial institutions shall apply, with regard to the business relationship, customer due diligence measures proportional to the level of re-assessed risk, in accordance with Article 19, § 2, of the Law, taking account of the fact that this business relationship has not been terminated. Moreover, obliged financial institutions shall refuse to enter into any other business relationship with the customer concerned and to carry out any occasional transaction on behalf of this customer.

## Art. 16

Obliged financial institutions shall set out in writing for their staff who are in direct contact with customers or instructed with carrying out their transactions:

1° the appropriate criteria enabling them to detect atypical transactions;

2° the procedure required to subject these transactions to a specific analysis under the responsibility of the AMLCO, in accordance with Article 45, § 1, of the Law, so as to determine whether these transactions may be suspected of being associated with money laundering or terrorist financing.

## Art. 17

Obligated financial institutions shall set up a monitoring system for detecting any atypical transactions which might not have been detected by their staff who are in direct contact with customers or instructed with carrying out their transactions.

This monitoring system must:

- 1° cover all customers' accounts and contracts and all their transactions;
- 2° be based on precise and relevant criteria fixed by each obliged financial institution taking particular account of the characteristics of its customers, the products, services or transactions that it offers, the countries or geographical areas concerned and the distribution channels that they use, and be sufficiently discriminating to make it possible to detect atypical transactions effectively;
- 3° allow these transactions to be detected rapidly;
- 4° be automated, unless the obliged financial institution can demonstrate that the nature, number and volume of transactions to be monitored do not require it;
- 5° be subject to an initial validation procedure and a regular re-examination of its relevance with a view to adapting it, if necessary, in accordance with the development of the customer base targeted by the obliged financial institution, the products, services or transactions that it offers, the countries or geographical areas concerned and the distribution channels that they use.

The criteria referred to in paragraph 2, 2nd indent, shall notably take into account the specific ML/FT risk associated with transactions carried out by customers whose acceptance has been subjected to stricter rules under the customer acceptance policy referred to in Title 3.

## Art. 18

Pursuant to Article 9, §§ 1 and 2, of the Law, obliged financial institutions shall adopt appropriate procedures, for carrying out as soon as possible, depending on the circumstances, an analysis of the atypical transactions in order to determine, pursuant to Article 45 of the Law, whether the CTIF-CFI should be notified of the suspicions in accordance with Article 47 of the Law.

## Art. 19

Obligated financial institutions which make use of agents or sub-contractors to enter into or maintain business relationships with customers or carry out occasional transactions on behalf of them shall set out in writing to these intermediaries the identification and verification procedures to be implemented, in compliance with the Law and this Regulation. They shall ensure that these procedures are respected.

## Art. 20

Obligated financial institutions shall state in writing to their agents and sub-contractors who are in direct contact with customers:

- 1° appropriate criteria enabling them to detect atypical transactions;
- 2° the procedure required for carrying out a specific analysis of these transactions under the responsibility of the AMLCO, in accordance with Article 45, § 1, of the Law, in order to determine whether these transactions may be suspected of being linked to money laundering or terrorist financing.

## Art. 21

The intervention of a third-party business introducer pursuant to Article 42 of the Law shall be subject to the condition that the internal procedures of the obliged financial institution stipulate:

1° that the obliged financial institution shall verify beforehand and keep the documents on which it has based its verification that the third-party business introducer meets, where appropriate, the conditions laid down in Article 43, § 1, 3°, and § 2, 2nd indent, of the Law;

2° that the third-party business introducer undertakes, in writing, beforehand to:

immediately provide the obliged financial institution with the information concerning the identity of the customers that will be introduced and, where appropriate, of their agents and beneficial owners, concerning the customer's characteristics and the purpose and intended nature of the business relationship, that is necessary for fulfilling the due diligence requirements conferred upon them in accordance with Article 42 of the Law;

provide the obliged financial institution, without delay and at first request, with a copy of the supporting documents or of the reliable sources of information he/she used to verify the identity of customers and, where appropriate, of their agents and beneficial owners.

## Art. 22

When an obliged financial institution wishes to report suspicions pursuant to Article 47 of the Law, it shall carry out an individual re-assessment of ML/FT risks, in accordance with Article 19, § 2, of the Law, taking account of the specific fact that a suspicion has been raised about the customer concerned. It shall decide, on the basis of this re-assessment and the customer acceptance policy referred to in Title 3, whether to maintain the business relationship subject to the implementation of due diligence measures adapted to such re-assessed risks, or whether to terminate it.

## Art. 23

Obliged financial institutions shall set up monitoring systems to monitor compliance with:

1° the provisions of the European Regulation on transfers of funds;

2° binding provisions concerning financial embargoes.

These monitoring systems must:

1° cover all customers' accounts and contracts and all their transactions;

2° allow rapid detection of any infringements of the provisions referred to in the first paragraph or detection in real time whenever these provisions require it;

3° be automated, unless the obliged financial institution can demonstrate that the nature, number and volume of transactions to be monitored do not require it;

4° be subject to an initial validation procedure and a regular review.

## Art. 24

Obligated financial institutions shall record in writing, on paper or electronically, the measures that they have effectively implemented for the application of the due diligence requirements referred to in Book II, Title 3, of the Law, of those concerning analysis of atypical transactions and reporting of suspicions referred to in Book II, Title 4, of the Law, of the provisions of the European Regulation on transfers of funds and binding provisions concerning financial embargoes. They shall keep this justification for the period of time determined by Article 60 of the Law.

# Policies, procedures, processes and internal control measures: Comments and recommendations

Home > Financial oversight > Combating money laundering and the financing of terrori...

## Contents

- 1. Links between the overall risk assessment and the organisation
- 2. AML/CFTP organisation
- 3. Internal control measures relating to AML/CFTP (including expectations with regard to the internal audit function)
- 4. Application of the principle of proportionality
- 5. Other prudential organisational rules to be complied with

Financial institutions should set up an efficient AML/CFTP organisation that is commensurate with their nature and size. Fulfilling this obligation is essential to ensure compliance with substantive AML/CFTP obligations such as the obligation to exercise due diligence regarding transactions and business relationships, to analyse atypical transactions and report suspicions of ML/FT, as well as the obligations related to transfers of funds, embargoes and asset freezing, etc. For this purpose, the Anti-Money Laundering Law reinforces coherence between the substantive AML/CFTP provisions and the AML/CFTP organisation (see the Explanatory Memorandum of the Anti-Money Laundering Law for more information on this subject).

This organisation should include adequate measures for performing an **overall ML/FT risk assessment de BC/FT**, but also use the results of this assessment as a basis for properly addressing the risks mapped (see point 1 below). It should comprise a set of **internal policies, procedures and processes** (see point 2) as well as an **internal control system** (see point 3).

However, in accordance with the principle of **proportionality**, the NBB could accept a simplified organisational structure (see point 4). Additionally, the AML/CFTP organisation is expected to be integrated harmoniously into the **overall organisation of the financial institution** (see point 5).

## 1. Links between the overall risk assessment and the organisation

The setting up of an adequate AML/CFTP organisation including all elements detailed below is closely linked to the overall risk assessment.

On the one hand, in order to perform an appropriate overall risk assessment within a financial institution, the objectives of this assessment should be clearly specified beforehand (internal policy aspect), the assessment should be performed in a sufficiently precise procedural framework and it should be subject to adequate internal controls to ensure the relevance and objectivity of its results in terms of mapping ML/FT risks and measuring their intensity.

On the other hand, the NBB expects financial institutions to base their AML/CFTP organisation, policies, procedures and internal control system as specified below on the results of their overall ML/FT risk assessment, which the entire AML/CFTP policy should address adequately and proportionately. Moreover, since these risks can evolve over time and their nature and size can be influenced by significant events, the overall risk assessment procedure should be

updated periodically. When such an update reveals significant changes in the nature and/or intensity of previously mapped risks, the financial institution is required to examine whether its organisation, policies, procedures, processes and internal control system should be modified to adapt them to the changes found.

As a result, the NBB believes that financial institutions should consider it a top priority to set up an adequate and controlled organisational and procedural framework for the overall risk assessment, as this overall risk assessment is the essential basis for all other measures implemented in accordance with the legal and regulatory AML/CFTP requirements.

For further information on the content, preparation methodology and updating of the overall risk assessment, see the page "Overall risk assessment".

## 2. AML/CFTP organisation

As regards their AML/CFTP organisation, financial institutions should define and implement (i) policies, (ii) internal procedures and (iii) implementation processes.

### 2.1. AML/CFTP policy

Article 8 of the Anti-Money Laundering Law requires financial institutions to develop and implement efficient and proportionate AML/CFTP policies first and foremost. These policies should establish the basic principles which should be complied with in the context of the financial institution's activities and specified in detail in the internal procedures in order to be implemented effectively.

The NBB therefore expects each financial institution, by adopting its AML/CFTP policy in accordance with Article 8 of the Anti-Money Laundering Law, to clearly specify its self-imposed AML/CFTP objectives and the guidelines to be complied with when establishing internal procedures and processes (see below) in order to achieve these objectives. The AML/CFTP policy should cover the **two aspects** detailed below in particular:

1. **ML/FT risk management**; and
2. **Customer acceptance**.

The NBB expects from financial institutions that this policy is:

- formalised in a written document;
- validated by their board of directors;
- in accordance with the regulations in effect and with the changes made to them;
- proportionate and adapted to the nature and extent of their activities;
- distributed to all concerned staff (for example through a publication on the Intranet); and
- updated regularly (particularly following a change in the overall risk assessment).

This policy should also form a coherent whole with and be included completely or in summarised form in the **integrity policy** which is to be validated by the financial institution's board of directors in accordance with the sectoral laws for prudential supervision. However, if the AML/CFTP policy is included completely in the institution's integrity policy, the NBB asks that the former be easily identifiable within the latter. This policy should also form a coherent whole with and be included completely or in summarised form in the integrity policy which is to be validated by the financial institution's board of directors in accordance with the sectoral laws for prudential supervision. However, if the AML/CFTP policy is included completely in the institution's integrity policy, the NBB asks that the former be easily identifiable within the latter.

#### 2.1.1. ML/FT risk management

The NBB expects financial institutions' AML/CFTP policy to contain a section dedicated to ML/FT risk management which should cover three domains:

1. the basic principles of the ML/FT risk-based approach chosen;
2. the maximum ML/FT risk tolerance; and
3. the guidelines to be followed when defining the ML/FT risk management procedures and measures and internal control measures.

The **first part** of the policy should establish the basis of the risk-based approach applied by the financial institution in accordance with Article 7 of the Anti-Money Laundering Law. This first part of the ML/FT risk management policy, which is obligatory for all managers, staff members, agents and representatives of the financial institution, should aim to raise the awareness of all these persons about the necessity of recognising the existence of the risks to which the financial institution is exposed, of measuring these risks in an objective and impartial manner and of implementing management and reduction measures that are proportionate and adapted to their size and nature. For this purpose, this first part of the ML/FT risk management policy should, in order to establish an adequate overall risk assessment procedure (see below), contain a general description of the risk variables to be taken into account and the basic principles to be followed in terms of risk factor mapping and analysis.

The **second part** should specify maximum risk tolerance limits for each activity segment subject to ML/FT risk. This ML/FT risk strategy should be integrated in a coherent and harmonious manner (i) into the general risk appetite policy which is to be validated by the board of directors pursuant to the sectoral supervisory laws and, (ii) where appropriate, into the specific policy or policies on operational and reputational risk. Account should also be taken of the primary objective of the Anti-Money Laundering, i.e. reducing ML/FT risk within individual financial institutions as much as possible and requiring them to respond appropriately when this risk materialises, in order to prevent it from spreading throughout the financial sector and society in general.

The **third part** of the policy should contain a general description of (i) the manner in which the institution intends to manage each ML/FT risk mapped in the overall risk assessment, (ii) the link between the ML/FT risk management measures implemented within the financial institution and the maximum ML/FT risk tolerance policy, and (iii) the guiding principles for defining the internal control measures to be implemented to ensure the efficiency of the ML/FT risk management measures. This third part should include the reference framework to be used as a basis for establishing the internal risk-based procedures to be applied for identifying and verifying the identity of persons involved in business relationships or occasional transactions. In this regard, see the page “Object of the identification and identity verification” in particular.

This section of the AML/CFTP policy, which is dedicated to ML/FT risk management, should be integrated harmoniously with financial institutions’ existing risk management policies.

### 2.1.2. Customer acceptance

The customer acceptance policy is an extension of and forms a coherent whole with the ML/FT risk management policy. In terms of principles, it primarily aims to determine the conditions regarding the reduction of ML/FT risk which the financial institution imposes on itself for entering into a business relationship with its customers or to become involved in performing occasional transactions for its customers. This customer acceptance policy should enable institutions to adequately take into account the overall risk assessment and the diversity of the risks mapped in terms of nature and intensity. This diversity should also be reflected in the risk classification. The customer acceptance policy should thus enable institutions to define appropriate procedures and arrangements for entering into a business relationship with or performing transactions for these customers. It is important to note that the customer acceptance policy is essentially intended to serve as a framework for the decision-making process as regards the establishment of a business relationship or the execution of the occasional transaction and the nature and intensity of the due diligence measures to be implemented. However, these decisions may not result automatically from the customer acceptance policy, but require an individual risk assessment carried out in accordance with Article 19 of the Anti-Money Laundering Law that allows the possible specificities of each individual case to be taken adequately into account.

In concrete terms, the financial institution should specify the following in its customer acceptance policy, depending on the characteristics of the products and services offered by it and on the customers targeted by it:

1. the general criteria for assigning new customers to different risk categories;
2. the principles for the differentiated allocation of the power to decide to enter into the business relationship or perform the transaction desired by the customer to persons with an adequate hierarchical level for each risk category. In this regard, particular attention should be paid to the customers (i) who are considered to be posing a high risk pursuant to Article 19, § 2, of the Anti-Money Laundering-Law, (ii) who are referred to in Articles 37 to 41 of the Law, (iii) who request the opening of numbered accounts or the conclusion of numbered contracts, and (iv) for whom no relevant information regarding their address or, where appropriate, the date and place of birth of their beneficial owner(s) could be collected; and
3. the basic principles to be followed by the procedures implementing the mandatory provisions on financial embargoes that are applicable at the start of the relationship.

## 2.2. Internal procedures

On the basis of their AML/CFTP policy (see above), financial institutions are required to draft AML/CFTP procedures for their staff and agents.

The NBB particularly recommends developing procedures on at least the following subjects:

1. **overall risk assessment** (see the page on this subject);
2. **customer and transaction due diligence measures** (see the page on this subject);
3. **analysis of atypical transactions and reporting of suspicions to the CTIF-CFI** (see the page on this subject);
4. the measures required for compliance with the obligations related to **financial embargoes and asset freezing** and, where appropriate, with the European Regulation on **transfers of funds** (see the pages on these subjects);
5. **retention and protection of data and documents** (see the page on this subject); and
6. **internal whistleblowing** (see the page on this subject).

The NBB expects financial institutions' AML/CFTP procedures to be

- formalised in writing;
- validated by their management committee (or their senior management if there is no such committee) or, in case of minor changes, by the senior officer responsible for AML/CFTP;
- in accordance with the regulations in effect and with the changes made to them;
- proportionate and adapted to the nature and extent of their activities;
- comprehensive, detailed and operational (where appropriate, specific procedures should be established for each activity);
- distributed to all concerned staff; and
- updated regularly (particularly following a change in the overall risk assessment).

### 2.2.1. Overall risk assessment procedure

Given the crucial role played by the overall risk assessment in the AML/CFTP system to be developed by financial institutions, the NBB believes they should consider it a top priority to each develop a robust procedural framework ensuring a high level of relevance and objectivity for the results of the assessment (also see Chapter 1. above).

This internal procedure should at least include:

- a list of the relevant risk variables and factors taken into account and of the sources of quantitative and/or qualitative information for each of these factors used;
- the methodology for analysing risk factors, including any weightings;
- the procedure for the validation and adoption of the results of the overall risk assessment by the institution's management committee or senior management;
- the procedure for informing the board of directors about the approved results of the overall risk analysis;
- the arrangements for updating the overall risk assessment, including during its periodic review or following significant events.

The overall risk assessment procedure should take particular account of high-risk cases for which the Anti-Money Laundering Law requires enhanced due diligence (see the page "Special cases of enhanced due diligence").

### 2.2.2. Procedures relating to customer and transaction due diligence measures

Generally, internal procedures relating to customer and transaction due diligence measures should be a direct extension of the risk classification. Indeed, it should be recalled that financial institutions should be able to demonstrate for each of their risk categories that their internal procedures relating to due diligence measures are appropriate for mitigating the risks classified in this way, taking into account their nature and intensity.

Moreover, if the activities performed are diverse, it could also be appropriate for the financial institution, for risks of the same level and the same nature, to establish distinct due diligence procedures for each of its activities, to adequately take into account their specificities, notably in terms of their organisation within the financial institution. In such a case, however, the financial institution should ensure the overall coherence of its diverse due diligence procedures.

The internal procedures relating to customer and transaction due diligence measures should cover at least the elements listed below.

Attention should also be paid to the necessity for financial institutions to establish their internal procedures referred to here in compliance with the specific provisions of the Anti-Money Laundering Law regarding the retention and protection of data (see the page “Retention and protection of data and documents”) and with all other legislations and regulations applicable, such as those listed on the page “Due diligence requirements and compliance with other legislations”. As regards the latter aspect, financial institutions can nevertheless deem it preferable to establish specific internal procedures (see section 2.2.5. below).

## **A. Procedure for identifying and verifying the identity of customers, agents and beneficial owners**

### *A.1. Exhaustive listing of the persons to be identified*

To ensure that the legal identification and identity verification obligations are met for all persons involved in a business relationship or occasional transaction, the procedure for identifying and verifying the identity of these persons should specify the measures required to determine whether, in addition to the customer, there is a need to identify one or more of his agents and, where appropriate, one or more beneficial owners in accordance with legal provisions. For further information on this subject, see the page “Persons to be identified”.

### *A.2. Arrangements for identification and identity verification*

This procedure should specify the measures required to identify these persons and verify their identity.

In this regard, particular attention should be paid to the fact that the previous anti-money laundering regulations specified in a uniform manner for each category of customers (natural persons, legal persons, legal arrangements) which data should be collected to meet the identification obligation, while Article 26, § 2, of the new Anti-Money Laundering Law establishes the rules applicable in standard-risk situations, and § 3 of the same Article allows these requirements to be relaxed in low-risk situations (in compliance with the objective defined in § 1 of that Article) and § 4 requires them to be strengthened in high-risk situations.

As regards the obligation to verify the identity of the persons concerned, neither Article 27 of the Anti-Money Laundering Law nor the Anti-Money Laundering Regulation of the NBB contains a precise, uniform and prescriptive list of the supporting documents to be used. Article 27, § 1, of the Law requires the identification data collected to be checked against one or more supporting documents or reliable sources of information through which this data can be confirmed. § 2 of the same Article requires financial institutions to verify all identification data collected in standard-risk situations; § 3 allows them to reduce the amount of identification data to be collected in low-risk situations while § 4 requires them to not only verify all identification data collected in accordance with Article 26, §§ 2 and 4 of the Law, but also ensure with increased attention that the supporting documents used for the verification provide a high degree of certainty regarding the identity of the person concerned.

**The introduction of the risk-based approach in the context of the obligations to identify and verify the identity of the persons concerned therefore requires financial institutions to give a detailed description in their internal procedures of the concrete measures to be taken to fulfil these obligations and to do so in a manner that is consistent with the result of their overall risk assessment and with their risk classification.**

To this end, it could be useful for the part of the procedure for due diligence measures relating to the “Identification and verification of the identity of customers, agents and beneficial owners” to include a **correlation table of the supporting documents accepted for each risk class, as well as a list** of the circumstances in which certain supporting documents need not be submitted.

Additionally, the NBB expects this procedure to contain detailed information on the concrete arrangements for consulting the National Register and the register of beneficial owners (the “UBO register” created pursuant to Article 73 et seq. of the Anti-Money Laundering Law), as well as the additional identification and identity verification measures to be adopted in accordance with Article 29 of the Anti-Money Laundering Law when consulting the UBO register.

For further details, see the page “Object of the identification and identity verification” in particular.

**As regards the identification obligation**, the procedure should recall the data legally required to be collected in standard-risk situations (Article 26, § 2, of the Anti-Money Laundering Law) and specify the measures to be taken when the address of the person to be identified cannot be determined.

Moreover, the internal procedure should specify the additional identification data to be collected in high-risk situations (see Article 12, 3°, of the Anti-Money Laundering Regulation of the NBB).

If the financial institution decides to make use of the possibility to relax the obligation to identify persons involved in low-risk occasional transactions or business relationships, its internal procedure should also specify which identification data needs not be collected.

**As regards the obligation to verify the identity of the persons involved**, Article 12, 1°, of the Anti-Money Laundering Regulation of the NBB stipulates that the procedure should contain precise rules on the supporting documents or reliable and independent sources of information that are accepted by the financial institution for identity verification. It should be noted that, if the internal procedure authorises the use of new technologies as supporting documents or independent sources of information, this authorisation should be based on an objective and documented analysis of the reliability of this technology guaranteeing that its level of reliability is appropriate in view of the level and nature of the ML/FT risks associated with the business relationships or the occasional transactions in the context of which these technologies are used.

For the development of this internal procedure, the NBB advises financial institutions to take particular account of the comments and recommendations mentioned on the page “Object of the identification and identity verification”.

In this regard, the internal procedure should list the supporting documents that can be accepted in standard-risk situations and the enhanced identity verification measures for persons involved in high-risk business relationships or occasional transactions. If the financial institution decides to make use of the possibility to relax the obligation to verify the identity of persons involved in low-risk occasional transactions or business relationships, its internal procedure should also specify which identification data needs not be verified.

#### *A.3. Specific measures for identifying and verifying the identity of agents*

For agents, identification and identity verification rules identical to those imposed with regard to customers (see A.2. above) should apply and the internal procedure should provide for special rules to ascertain their powers of representation in accordance with Article 12, 4°, of the Anti-Money Laundering Regulation of the NBB.

#### *A.4. Measures to gain insight into the ownership and control structure of the customer or agent that is a society, a legal person, a foundation, a fiducie, a trust or a similar legal arrangement*

In accordance with Article 12, 5°, of the Anti-Money Laundering Regulation of the NBB, the procedure should contain specific rules for gaining insight into the ownership and control structure of the customer or agent that is a society, a legal person, a foundation, a fiducie, a trust or a similar legal arrangement.

#### *A.5. Specific measures for identifying and verifying the identity of beneficial owners*

In accordance with Article 12, 6°, of the Anti-Money Laundering Regulation of the NBB, the internal procedure should provide for precise rules regarding the measures to be taken to identify and verify the identity of the beneficial owners (i) of customers, (ii) of the agents of customers or (iii) of the beneficiaries of life insurance contracts. This procedure should also specify the measures to be taken if a beneficial owner’s date and place of birth or address cannot be determined.

If the internal procedure provides for the use of the central register of beneficial owners referred to in Article 73 of the Anti-Money Laundering Law or of the equivalent registers held in other countries of the EEA or in third countries, it should also specify which additional measures, proportionate in view of the identified risk level, are required in accordance with Article 29 of the Anti-Money Laundering Law.

#### *A.6. Delayed identification and verification of the identity of the persons concerned*

If the financial institution decides to make use of the possibility provided for in Article 31 of the Anti-Money Laundering Law to delay the verification of the identity of persons involved in a business relationship in compliance with the conditions laid down in that Article, the internal procedure should contain a precise and limitative list of the circumstances in which this possibility can be used, as well as of the measures needed to perform the verification as soon as possible after first contact with the customer.

*A.7. Inability to fulfil the obligations to identify and verify the identity of persons involved in a business relationship or an occasional transaction*

Considering that it is prohibited to enter into a business relationship or perform an occasional transaction exceeding the thresholds defined by the Law when the persons involved cannot be identified and/or have their identity verified in accordance with the legal provisions (Article 33 of the Anti-Money Laundering Law) and given the legal obligation to conduct a special investigation in such situations to determine whether a suspicion should be reported to the CTIF-CFI, the internal procedure should specify the measures to be taken by staff members or independent agents in contact with customers to take note of such situations and report them to the AMLCO for the purposes of the investigation required by Article 46 of the Anti-Money Laundering Law.

**B. Customer acceptance procedure**

*B.1. Collection of relevant information on the characteristics of the customer and on the purpose and nature of the business relationship or the occasional transaction*

The internal procedure should list the relevant information to be obtained, depending on the risk classification, to identify the customer's characteristics and the purpose and nature of the business relationship or the occasional transaction.

For further information, see the page "Identification of the customer's characteristics and of the purpose and nature of the business relationship or the occasional transaction".

*B.2. Individual risk assessment*

The internal procedure should define the methodology followed to perform the individual assessment of the risks associated with the business relationship or occasional transaction concerned, in accordance with Article 19 of the Anti-Money Laundering Law.

In this regard, the internal procedure should establish the arrangements for the analysis of all information collected on the customer and the intended business relationship or occasional transaction in order to determine for each specific case which risk class defined following the overall risk analysis is appropriate to ensure that the most relevant due diligence measures are applied to the business relationship or the occasional transaction, taking into account its characteristics or special features.

For further information, see the page "Individual risk assessment".

*B.3. Customer acceptance*

Based on the individual risk analysis, the customer acceptance procedure should organise, in compliance with the customer acceptance policy, the decision-making process of the financial institution for entering into a business relationship with the customer or performing the intended occasional transaction.

In particular, the procedure should determine, depending on the ML/FT risk established on the basis of the individual risk assessment, the hierarchical level of the persons who - alone or together - are authorised to decide to enter into a relationship or perform a transaction. Where appropriate, it should also determine the AMLCO's involvement in this decision-making process and the verifications required prior to the decision.

When deciding to accept a customer, the customer's special requests should be taken into account. For instance, if the customer's request involves opening a numbered account or concluding a numbered contract, the customer acceptance procedure should specify, in accordance with Article 11 of the Anti-Money Laundering Regulation of the NBB, the conditions under which this account can be opened or this contract concluded as well as the terms of operation. However, these conditions and terms are without prejudice to the legal and regulatory ongoing due diligence obligations. For further information, see the page "Anonymous or numbered accounts and contracts".

**C. Procedure for ongoing due diligence with regard to the business relationship and the transactions**

*C.1. Update of the identification and verification of the identity of customers, agents and beneficial owners and information on the characteristics of the customer and on the purpose and nature of the business relationship*

The internal procedure should specify the circumstances in which the identification and verification of the identity of persons involved in a business relationship (customer, agents and beneficial owners) and/or the collection of information on the characteristics of the customer and/or on the purpose and nature of the business relationship should be repeated in accordance with Article 35, § 1, 2°, of the Anti-Money Laundering Law in order to update the data held by the financial institution. It should also determine, according to the risk, the time limit within which this update and a new individual risk assessment should be performed. For further details, see the page "Ongoing due diligence and detection of atypical transactions".

*C.2. Existing customers*

The NBB also draws attention to the fact that the provisions of the Anti-Money Laundering Law and Regulation of the NBB not only apply to the business relationships or the occasional transactions which financial institutions conclude with new customers, but also - without a transitional period - to the ongoing business relationships entered into with customers before the entry into force of these new legal and regulatory provisions.

The NBB therefore expects financial institutions to reassess the business relationships they entered into before the entry into force of the Anti-Money Laundering Law and Regulation of the NBB based on the criteria defined in their customer acceptance policy, prioritising business relationships considered a high risk before this reassessment.

For this purpose and following the reassessment, financial institutions are expected to:

1. specify in their internal procedures which method is used to assign an appropriate risk class to each business relationship with existing customers in accordance with their risk classification, based on the information available at that moment on the customer and the business relationship;
2. update the information held on business relationships with existing customers when previously fulfilled due diligence requirements are insufficient, taking into account the new risk class assigned to the business relationship.

Based on this reassessment, financial institutions can, where appropriate, take one of the measures provided for in Article 15 of the Anti-Money Laundering Regulation of the NBB.

*C.3. Due diligence with regard to business relationships and transactions*

In accordance with Article 35, § 1, 1°, of the Anti-Money Laundering Law, the internal procedure should define the measures to be taken by persons who are in direct contact with customers or instructed with carrying out their transactions in order to comply with the obligation to exercise ongoing due diligence and to detect atypical transactions. These measures should take into account the level and nature of the risks associated with the business relationship or the occasional transaction concerned as shown by the individual risk assessment and, in particular, the cases in which enhanced due diligence is required by the Anti-Money Laundering Law. For further information, see the page "Ongoing due diligence and detection of atypical transactions".

This procedure should include:

- a list of the criteria enabling persons who are in direct contact with customers or instructed with carrying out their transactions to detect atypical transactions (see Article 16, 1°, of the Anti-Money Laundering Regulation of the NBB);
- the procedure required to subject these transactions to a specific analysis under the responsibility of the AMLCO in accordance with Article 45, § 1, of the Law in order to determine whether these transactions can be suspected of being linked to money laundering or terrorist financing (see Article 16, 2°, of the Anti-Money Laundering Regulation of the NBB);
- the initial procedure for validating the monitoring system referred to in Article 17 of the Anti-Money Laundering Regulation of the NBB and the procedure for periodically reviewing the relevance of this system in order to adapt it if necessary;
- where appropriate, the procedure for monitoring transactions when it is decided to use a non-automated monitoring system.

**2.2.3. Procedure for analysing atypical transactions, reporting suspicions to the CTIF-CFI and processing requests for information addressed by the CTIF-CFI to the financial institution**

The procedure for analysing atypical transactions and reporting suspicions to the CTIF-CFI should cover at least the following:

1) it should contain a detailed description of the process for the analysis to be performed by or under the authority of the AMLCO:

- a) of the internal reports relating to situations in which the obligations to identify and verify the identity of the persons involved cannot be fulfilled (see the procedures in A.7. above);
- b) of the internal reports relating to detected atypical transactions which staff members, agents or distributors are required to submit to the AMLCO in accordance with the procedure for due diligence with regard to business relationships and transactions (see the procedure in C.2. above);
- c) of the alerts generated by the monitoring system for business relationships and occasional transactions that is referred to in Article 17 of the Anti-Money Laundering Regulation of the NBB;

to determine whether there is a suspicion of ML/FT within the time limit required by the Law;

2) it should contain a detailed description of the process by which the AMLCO processes requests for information addressed by the CTIF-CFI to the financial institution, so he can answer them within the time limit required;

3) if these processes imply the involvement of staff members who are not part of the compliance function, of agents or distributors of the financial institution, the procedure should clearly specify the specific responsibility of these persons in this context and their obligation to cooperate fully and without delay on the analysis of the transactions concerned or on the collection and transmission of the information required;

4) it should explicitly state that the AMLCO, in accordance with the provisions of the Anti-Money Laundering Law, is competent – in principle but not exclusively – to decide whether there is a suspicion of ML/FT and, as a result, holds the autonomous power to report a suspicion to the CTIF-CFI and answer the latter's requests for additional information;

5) it should explicitly state that the financial institution's managers, staff members, agents or distributors are legally prohibited, subject to the exceptions provided for in the Anti-Money Laundering Law, from informing the customer or third parties that information is, will be or has been transmitted to the CTIF-CFI, or that transactions of the customer are or have been considered atypical and are or have been analysed for that reason;

6) it should outline and specify, in the specific context of the financial institution, which measures are taken to ensure the protection of reporting entities in accordance with Article 57 of the Anti-Money Laundering Law.

For further information, see the pages "Analysis of atypical transactions", "Reporting of suspicions", "Prohibition of disclosure" and "Protection of reporting entities".

#### **2.2.4. Procedure for monitoring transfers of funds and financial embargoes and implementing asset freezing measures**

The procedure(s) for monitoring transactions in view of the obligations relating to transfers of funds, financial embargoes and asset freezing should cover at least the following:

1) as regards the **rules on financial embargoes and asset freezing**:

1. they should organise the process for the analysis, initial validation and periodic review of the transaction monitoring system implemented, in accordance with Article 23 of the Anti-Money Laundering Regulation of the NBB;
2. they should specify the terms for the regular update of the lists of persons subject to measures relating to financial embargoes and asset freezing that are used by the transaction monitoring system implemented;
3. they should provide for a precise and detailed organisation of the process whereby alerts generated by the transaction monitoring system are analysed as soon as possible under the responsibility of the AMLCO to verify their relevance;
4. if alerts are proven to be relevant, the procedures should provide for a precise and detailed organisation:
  1. of the process for the immediate freezing of the assets concerned;
  2. of the procedure for notifying asset freezing to the competent service of the FPS Finance; and
  3. of the investigation of the transaction concerned and, where appropriate, of the business relationship in the context of which the transaction took place, to be carried out under the responsibility of the AMLCO to determine whether they also raise suspicions of ML/FT (see section 2.2.3. above).

For further information, see the page “Financial embargoes and asset freezing”.

2) as regards the **rules on transfers of funds**:

1. the internal procedures should organise the process for the analysis, initial validation and periodic review of the transaction monitoring system implemented, in accordance with Article 23 of the Anti-Money Laundering Regulation of the NBB;
2. they should organise the analysis and decision-making process with regard to the measures to be taken in accordance with Articles 7 and 8, § 1, of the European Regulation on transfers of funds if the financial institution operates as payment service provider of the beneficiary, and with Articles 11 and 12, § 1, if the financial institution operates as intermediary payment service provider when the transaction monitoring system implemented by it detects the receipt of a transfer of funds not accompanied by the full information required on the payer and the payee;
3. they should organise the process for detecting payment service providers of payers or intermediary payment service providers of received transfers of funds who repeatedly fail to provide the information required on the payer or the payee, as well as the decision-making process for the measures to be taken in such cases in accordance with Articles 8, § 2, and 12, § 2, of the European Regulation on transfers of funds;
4. they should organise the process for the investigation by the AMLCO of transfers of funds received without the information required in accordance with Articles 9 and 13 of the European Regulation on transfers of funds, to determine whether there are suspicions of ML/FT (see section 2.2.3. above);

For further information, see the page “Transfers of funds”.

### **2.2.5. Procedure for the retention and protection of data and documents**

If the aspects on the retention and protection of data and documents are not incorporated in the internal procedures listed above, the financial institution should establish a specific procedure for this matter. In any case, these internal procedures should at least cover the items mentioned on the page “Retention and protection of data and documents”.

The NBB notes in this regard that the copy of the supporting documents which the financial institution has used to identify the identity of the customer or his agent can be stored on an electronic device that can also be used for retention purposes. The same retention obligations apply to documents which the institution has used to verify the identity of beneficial owners or, failing that, to the justification for why this verification was not reasonably possible.

Additionally, the procedure for the retention and protection of data and documents should list the information and documents to be retained, the retention period and the time when the retention period starts. This procedure should ensure the confidentiality of the documents (storage, persons with access to them, etc.) and, in this regard, take into account the recommendations on the processing of personal data issued by the Commission for the Protection of Privacy.

In its procedures, the financial institution should describe the terms for accessing this data, even if it uses an external service provider to archive this data. The NBB urges financial institutions to implement mechanisms for accessing customer records that are adapted to their organisation and enable the stakeholders competent with regard to AML/CFTP to obtain them as soon as possible, particularly in order to answer requests for additional information from the CTIF-CFI.

### **2.2.6. Internal whistleblowing procedure**

In accordance with Article 10 of the Anti-Money Laundering Law, the financial institution should establish an internal whistleblowing procedure to enable its staff or agents or distributors to report non-compliance with the obligations set out in the Anti-Money Laundering Law to the senior officer responsible for AML/CFTP and the AMLCO. For further information, see the page “Internal whistleblowing”.

## **2.3. Implementation process**

To be efficient, the AML/CFTP organisation should be supported by a set of IT tools and implementation/control processes.

### **2.3.1. At the level of the persons who are in direct contact with customers or instructed with carrying out their transactions**

The financial institution should establish a database of customers, agents and beneficial owners that enables concrete compliance with the customer due diligence obligations. This database should contain all information provided for in the procedure for the identification of customers, agents and beneficial owners and should be consistent with the customer acceptance procedure.

In accordance with Article 16 of the Anti-Money Laundering Regulation of the NBB, the AMLCO should submit written rules to the persons who are in direct contact with customers or instructed with carrying out their transactions, including (i) the appropriate criteria that enable them to detect atypical transactions and (ii) the procedure required to submit the transactions to the AMLCO so he can perform a specific analysis and determine whether these transactions can be suspected to be linked to ML/FTP. In this context, a communication channel should be opened between the staff concerned and the AMLCO, enabling the former to submit internal reports on suspicious transactions and non-identifiable persons to the latter.

### **2.3.2. At the level of the AMLCO**

In accordance with the Anti-Money Laundering Regulation of the NBB and taking into account the institution's characteristics, the AMLCO should at least have the following IT processes and systems:

- permanent electronic access to the database of customers, agents and beneficial owners;
- a monitoring system enabling the detection of atypical transactions which, as the case may be, might not have been detected by the persons who are in direct contact with customers or instructed with carrying out their transactions (Article 17 of the Anti-Money Laundering Regulation of the NBB). For further information on this system, see the page "Analysis of atypical transactions";
- a monitoring system guaranteeing compliance (i) with the provisions of the European Regulation on transfers of funds and (ii) with the binding provisions on financial embargoes. For further information on this system, see the page "Financial embargoes and asset freezing";
- an IT process enabling rapid asset freezing;
- an electronic data storage and archiving system (or a paper-based system for very small financial institutions) which can be used for registering the measures implemented to fulfil the due diligence obligations and the obligations to analyse atypical transactions, report suspicions, comply with the provisions of the European Regulation on transfers of funds and with the binding provisions on financial embargoes;
- if certain tasks of the AMLCO are outsourced, a process to follow up on these tasks and on the quality of the service provider's performance.

## **3. Internal control measures relating to AML/CFTP (including expectations with regard to the internal audit function)**

Pursuant to the Anti-Money Laundering Law, financial institutions should implement an internal control system to monitor compliance with AML/CFT procedures. This internal control system should be proportionate to the nature and extent of the financial institution's activities. This system, which may take multiple forms, should also be adapted to the risk classification established by the financial institution.

The internal control system should cover all activities that could potentially expose the financial institution to ML/FT risks and should apply to the entire AML/CFTP system. It should contain the following:

- the checks relating to the activities of the operational (commercial, management) services and departments;
- the checks relating to the activities of the AMLCO (including his role as entity reporting to the CTIF-CFI) and, where appropriate, those of his team; and
- the AML/CFTP checks relating to third-party business introducers or subcontractors (agents).

As such, financial institutions are expected to periodically and permanently monitor all persons active in the field of AML/CFTP within the institution.

The periodic checks can take place on various occasions and, in that regard, take the following forms:

1. annual assessment of the financial institution's governance or internal control system by its management committee;

2. annual assessment of the proper functioning of the financial institution's compliance function by its board of directors;
3. monitoring missions carried out by the compliance function, for example with regard to the checks conducted by the operational services or to the use of outsourcing;
4. audit missions relating to the AML/CFTP system carried out by internal audit; etc.

For the first two types of checks, the NBB urges financial institutions to ensure that the report submitted to it by the management committee and the board of directors specifically targets the management of the AML/CFTP system and enables the identification of weaknesses in this area and the adoption of corrective measures.

As regards the monitoring missions carried out by the compliance function, the NBB expects the monitoring plans of financial institutions' compliance functions to cover all AML/CFTP obligations.

As regards the AML/CFTP missions of the internal audit function, the NBB expects from financial institutions that their audit planning takes into account the results of the overall AML/CFTP risk assessment. For instance, the NBB considers it standard practice to have all aspects of the AML/CFTP process audited approximately every three years for institutions that have a standard or high ML/FT risk profile based on their overall risk assessment, and approximately every five years for institutions that have a low risk profile. This standard should be interpreted as being without prejudice to any important events that would require such an audit before the end of the usual periodic time limit (for example in case of a legislative change).

In general, the NBB highlights the fact that this website's pages related to operational AML/CFTP obligations (for example Ongoing due diligence and detection of atypical transactions, Analysis of atypical transactions, Reporting of suspicions, etc.) also contain certain recommendations of the NBB on internal control and internal audit. See the web pages on these topics for further information.

## 4. Application of the principle of proportionality

The Anti-Money Laundering Law and its explanatory memorandum clearly state that the AML/CFTP organisation to be implemented should be proportionate to the nature and size of the entity concerned.

In practice, this principle of proportionality should primarily be reflected in the level of sophistication of the internal procedures to be adopted and may justify the merging of multiple internal procedures into a single procedure.

It could also be reflected in the possibility to forgo, under the conditions set out in the Regulation of the NBB, the use of IT tools for transaction monitoring, in favour of more manual and less sophisticated systems. See in this regard the page "Ongoing due diligence and detection of atypical transactions".

Although the AML/CFTP organisation requirements apply in all cases, their intensity may vary depending on the scale of the underlying ML/FT risk. As a result, the NBB expects large financial institutions with diversified activities to have more sophisticated and detailed procedures than small financial institutions that are involved in less complex activities and are only exposed to a low ML/FT risk, which can have much more succinct and simple internal procedures.

## 5. Other prudential organisational rules to be complied with

The specific AML/CFT related governance requirements should be integrated harmoniously into all prudential governance rules applicable to the different sectors concerned. For instance, the sectoral prudential rules on organisational structure, task allocation, management of conflicts of interest, consistency of policies and internal procedures, information reporting and internal control should be complied with in the context of ML/FT risk management.

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**





# Training and education of staff

Home > Financial oversight > Combating money laundering and the financing of terrori...

## Legal and regulatory framework

- Anti-Money Laundering Law: Articles 11 and 12

## Explanatory Memorandum of the Anti-Money Laundering Law

- Articles 11 and 12

## Comments and recommendations by the NBB

The effectiveness of the AML/CFTP policy of financial institutions depends largely on the ability of their staff and representatives to contribute to its implementation. This ability depends on their technical knowledge and their awareness of the critical need to prevent ML/FT transactions, both of which are the responsibility of the AMLCO (see “Governance” page).

### 1. Education

The AMLCO should educate the staff of his financial institution about the ML/FT risks to which it is exposed, taking into account the broader national and international environment in which it operates, and about the reasons why it is necessary to reduce these ML/FT risks. The education thus consists in disseminating general AML/CFTP information **to all staff members**. This information can take various forms: company letters, intranet, meetings, etc. Through this process, staff are and remain informed of the risks, including ML/FT methods, trends and typologies, as well as of the risk-based approach implemented by the financial institution to reduce and manage these risks.

### 2. Training

In addition to the general education, the AMLCO should ensure that a (theoretical and practical) AML/CFTP training is provided to guarantee that the persons concerned by the AML/CFTP risks are effectively able to implement the AML/CFTP measures in effect in the financial institution. The NBB recommends that, as far as possible, this training be provided by the AMLCO or members of its team, where appropriate, in association with the department in charge of staff training. Nevertheless, if this task is outsourced to a third party, the AMLCO should ensure (i) that the subcontractor has the required AML/CFTP knowledge to guarantee the quality of the training to be provided, (ii) that the management conditions of the outsourcing are set and respected, and (iii) that the content of this training is adapted to the specific features of the financial institution concerned and that the field experience of the institution's AMLCO is properly reflected in the training (see below).

As regards the **ratione personae scope**, the training should cover all staff (irrespective of their status) of the financial institution who are concerned by the ML/FT risks, as well as its independent agents (not brokers) and, if the financial institution is an electronic money institution, its distributors.

The **training procedures** must be adapted to the financial institution's organisation and take account of its nature and size, as well as of its ML/FT risk profile.

The **subject of the training** to be provided must be proportionate to the ML/FT risks to which the persons to whom it is provided, may be exposed. A distinction can be made in this respect between:

- *persons working in the compliance function* under the responsibility of the AMLCO: training should be thorough and cover all AML/CFTP aspects, thus enabling the financial institution to comply with all its AML/CFTP obligations;
- *persons in contact with customers or instructed with carrying out their transactions (employees, agents and distributors)*: training should enable them to detect atypical transactions effectively and to alert the AMLCO as soon as possible in accordance with internal procedures;
- *persons responsible for developing procedures or software or other tools applicable to activities that are sensitive to ML/FT risk*: this training must enable them to adequately integrate the AML/CFTP issue.

The training program may include several sessions which, in accordance with the Anti-Money Laundering Law, are defined taking into account the tasks performed by the persons concerned and their exposure to ML/FT risks. In general however, the NBB recommends that all training sessions cover the following aspects:

1. all Belgian legal and regulatory AML/CFTP obligations applicable to financial institutions (overall risk assessment and risk classification, individual risk assessment, due diligence requirements, detection and analysis of atypical transactions, reporting of suspicions, embargoes, freezing of assets, electronic transfers of funds, etc);
2. the internal organisation, i.e. the risk-based approach and the policies, procedures, implementation processes of the institution and the existence of an internal reporting procedure ("internal whistleblowing");
3. the experience acquired within the institution and, in particular the cases of atypical transactions identified previously;
4. recent developments with regard to the ML/FT phenomenon in practice (typologies, risk factors, etc.);
5. the existence within the NBB of a reporting procedure ("external whistleblowing": see Article 11, § 1, paragraph 3 of the Anti-Money Laundering Law).

The NBB also reminds financial institutions that training should be updated in the light of any changes in legislative and regulatory provisions and, more generally, of any changes affecting the AML/CFTP organisation.

As regards the **frequency of training**, it should be provided both when new staff are recruited (short-term training after entry into service), and on an ongoing basis whenever updating is necessary, in particular as a result of changes in the identified risks or in the organisation of the financial institution.

The NBB also recommends setting up a **system for monitoring training and verifying the good understanding** of the substance by the staff concerned. To this end, the staff concerned can be asked to take a test after the training. The financial institution should also be able to demonstrate to the NBB the trainings taken by the staff involved in the ML/FT risks, as well as by the agents and the distributors.

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



# Anti-Money Laundering Law of 18 September 2017 - Articles 11 and 12

## Art. 11

§ 1. Obligated entities shall take measures commensurate with their risks, nature and size in order to familiarise the members of their staff whose functions require this as well as their agents or distributors with the provisions of this Law and its implementing decrees and regulations, including the applicable data protection requirements and, where appropriate, the obligations referred to in Article 8, § 1, 2° and 3°.

They shall ensure that the persons referred to in the first subparagraph know and understand the policies, procedures and internal control measures in force within the obliged entity in accordance with Article 8, § 1. They shall also ensure that these persons possess the required knowledge of the methods and criteria to be applied in order to identify possible ML/FT related transactions, of the course of action to be taken in such a chase, and of the manner in which the obligations referred to in Article 8, § 1, 2° and 3°, should be fulfilled.

Additionally, they shall ascertain that the persons referred to in the first subparagraph are aware of the internal reporting procedures referred to in Article 10, and of the procedures for reporting to the supervisory authorities referred to in Article 90.

§ 2. The measures referred to in paragraph 1 shall include the participation of the persons referred to in the first paragraph in special ongoing training programmes. They can be determined taking into account the functions performed by these persons within the obliged entity, as well as the ML/FT risks to which they might be exposed by performing these functions.

## Art. 12

Where a natural person falling within any of the categories of obliged entities listed in Article 5, § 1, 23° to 25°, performs professional activities as an employee of a legal person, the obligations in this Chapter shall apply to that legal person rather than to the natural person.



# Explanatory Memorandum to the Anti-Money-Laundering Law of 18 September 2017 - Articles 11 and 12

## Art. 11

Article 11 of the draft Law transposes Article 46, paragraph 1 of Directive 2015/849 and takes over the current provisions of Article 17, first paragraph, of the Law of 11 January 1993 as well as further developing them. This Article is pursuant to Article 8, § 2, 3° of the present draft and supplements it. Whilst this latter Article provides for the obligation of informing the persons concerned about ML/TF risks and training them on the measures implemented to reduce such risks, draft Article 11 covers only the second aspect. It should also be noted that draft Article 9, § 2, first paragraph gives the AMLCO the responsibility of ensuring the education and training of the persons involved.

Based on this, § 1 of draft Article 11 describes what the training of the persons concerned should involve in practice, i.e. essentially:

- the general legal framework that applies in the area of AML/CFT, and
- the policies, procedures and internal control measures in force within the obliged entity, in line with the general legal framework.

The second paragraph specifies that the obliged entities should not content themselves with offering a purely theoretical training course but must ensure that the persons concerned are genuinely able to apply the measures in force and, in particular, to identify suspicious transactions and in such cases to proceed in a proper and appropriate way.

Finally, the third paragraph states that the obliged entities must ascertain that the persons concerned are aware of the internal reporting procedures referred to in Article 10 and of the procedures for reporting to the supervisory authorities as referred to in Article 90 of the draft Law. This knowledge is after all indispensable for these procedures to be effective.

Paragraph 2 of draft Article 11 states that it does not suffice to offer a one-off training course to those concerned, for example when they join the company, but rather that the obliged entities must offer ongoing training. The objective of this is to ensure that account is taken of the changeable nature of ML/TF risks and of the legal, regulatory and procedural framework of AML/CFT. In contrast, § 2 allows the intensity and thoroughness of the training given as well as the frequency of updates to courses to be determined based on the functions and responsibilities of the persons concerned, to take into account their potentially different levels of exposure to ML/TF risks by virtue of the tasks and responsibilities they undertake.

## Art. 12

Draft Article 12 relates to the obliged entities listed in draft Article 5, § 1, 23° to 25° and transposes Article 46, point 1, third paragraph of Directive 2015/849 which provides for the following: "Where a natural person falling within any of the categories listed in point (3) of Article 2(1) performs professional activities as an employee of a legal person, the obligations in this Section shall apply to that legal person rather than to the natural person". Lawyers, bailiffs, notaries, and estate agents always have independent status even if they exercise this activity for a legal firm which is a legal person, for a notary firm or bailiff firm, or an estate agent. It is a different matter, however, for accounting

professions. They may have the title of company auditor, auditor, chartered accountant or tax consultant and exercise that profession as an employee of a company that also has the capacity of company auditor, audit firm, chartered accountant or tax consultant.



# Internal whistleblowing

Home > Financial oversight > Combating money laundering and the financing of terrori...

## Legal and regulatory framework

- Anti-Money Laundering Law: Articles 10, 12 and 36

## Explanatory Memorandum of the Anti-Money Laundering Law

- Articles 10, 12 and 36

## Comments and recommendations by the NBB

In accordance with Article 10 of the Anti-Money Laundering Law, financial institutions should define and set up an internal whistleblowing system allowing their staff, agents and, in the case of electronic money institutions, their distributors to inform the AMLCO and the senior AML/CFTP officer of breaches of the Anti-Money Laundering Law through a specific, independent and anonymous channel.

In practice, the NBB expects financial institutions to implement the following two measures:

- on the one hand, define and implement a clear **procedure** to be followed by their staff and agents or distributors that precisely indicates (i) what the internal AML/CFTP alerts can relate to, (ii) what are the different steps of the procedure and (iii) what protection is offered to persons making use of this internal whistleblowing system; and
- on the other hand, put in place a **secure reporting system** to anonymously (without resorting to the normal hierarchical channels) report breaches of AML/CFTP obligations to the AMLCO and the senior AML/CFTP officer.

This internal AML/CFTP whistleblowing system may, if necessary, be integrated into the internal "Compliance" whistleblowing system which might already have been set up pursuant to the sectoral prudential supervision laws for infringements of the financial institution's standards and code of conduct, provided that (i) the recipients of AML/CFTP alerts are the AMLCO and the senior AML/CFTP officer (besides, where applicable, the head of the Compliance function if the latter is not the AMLCO) and (ii) the communication channels effectively ensure the anonymity of the whistleblowers.

Furthermore, in accordance with Article 11, paragraph 3 of the Anti-Money Laundering Law, the AMLCO should, as part of his education and training programme, ensure that the staff members of the financial institution concerned, its agents and distributors are aware of this internal AML/CFTP whistleblowing system.

Finally, as stipulated in the Anti-Money Laundering Law, the principle of proportionality is applicable. This principle will be reflected in the level of sophistication of the procedure to be adopted and the reporting system to be put in place, as described above. The latter may be less sophisticated in financial institutions that are smaller in size or have a lower ML/FT risk profile.

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



# Anti-Money Laundering Law of 18 September 2017- Articles 10, 12 and 36

## Art. 10

Obligated entities shall develop and implement procedures that are appropriate and commensurate with their nature and size, in order to enable their staff or their agents or distributors to report non-compliance with the obligations set out in this Book to the persons appointed pursuant to Article 9 through a specific, independent and anonymous channel.

## Art. 12

Where a natural person falling within any of the categories of obliged entities listed in Article 5, § 1, 23° to 25°, performs professional activities as an employee of a legal person, the obligations in this Chapter shall apply to that legal person rather than to the natural person.

## Art. 36

Each obliged entity shall ensure that its staff, agents and distributors who internally report a transaction they consider atypical within the meaning of Article 35, § 1, 1°, or who report that the entity is unable to fulfil the due diligence requirements referred to in Articles 33, § 1, 34, § 3 and 35, § 2, are protected from being exposed to threats or hostile action, and in particular from adverse or discriminatory employment actions.



# Explanatory Memorandum to the Anti-Money-Laundering Law of 18 September 2017 - Articles 10, 12 and 36

## Art. 10

Article 10 of the draft Law transposes Article 61, paragraph 3 of Directive 2015/849 and imposes on obliged entities the obligation to provide for internal mechanisms commensurate with their nature and scale and which enable their staff and, where applicable, their agents and distributors, to report breaches of obligations regarding AML/CFT which they may have identified, to the senior manager responsible and to the AMLCO. These internal reports must be able to be anonymous and sent to their addressees through a specific and independent channel, which entails that they must be able to be sent directly to them rather than going through the hierarchy. It should be noted that, in the same way as for the application of draft Articles 8 and 9, the principle of proportionality and consequently the comments provided above on this subject, also apply to internal procedures for reporting breaches.

## Art. 12

Draft Article 12 relates to the obliged entities listed in draft Article 5, § 1, 23° to 25° and transposes Article 46, point 1, third paragraph of Directive 2015/849 which provides for the following: "Where a natural person falling within any of the categories listed in point (3) of Article 2(1) performs professional activities as an employee of a legal person, the obligations in this Section shall apply to that legal person rather than to the natural person". Lawyers, bailiffs, notaries, and estate agents always have an independent status even if they exercise this activity for a legal firm which is a legal person, for a notary firm or bailiff firm, or an estate agent. It is a different matter, however, for accounting professions. They may have the title of company auditor, auditor, chartered accountant or tax consultant and exercise that profession as an employee of a company that also has the capacity of company auditor, audit firm, chartered accountant or tax consultant.

## Art. 36

The mechanisms for detecting and analysing suspicious transactions and cases in which the obliged entity is not able to fulfil its due diligence obligations rest in the first place on the attention and critical thinking of persons whom, within the obliged entity, are in first-line contact with the customers and their transactions. In order for these mechanisms to be effective, these persons must not experience any fear of being penalised within the obliged entity because they have reported such a transaction or such a situation to the AMLCO. They must also be protected from any threat or any hostile action external to the obliged entity and especially from those that could come from the customer concerned or the persons associated therewith. Draft Article 36 states that obliged entities must take reasonable measures to ensure the protection of their members of staff, agents or distributors who find themselves in this situation from threats or hostile action, including internal adverse or discriminatory employment actions.



# Organisation and internal control in groups

[Home](#) > [Financial oversight](#) > [Combating money laundering and the financing of terrori...](#)

**Belgian parent companies**

**Belgian subsidiaries and branches**

**Belgian central contact points of European payment institutions and electronic money institutions**

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



# Belgian parent companies

Home > Financial oversight > Combating money laundering and the financing of terrori...

## Legal and regulatory framework

- Anti-Money Laundering Law: Articles 13 and 14
- Anti-Money Laundering Regulation of the NBB: Articles 6 and 25
- Commission Delegated Regulation (EU) 2019/758 of 31 January 2019 on the minimum action and the type of additional measures credit and financial institutions must take to mitigate ML/FT risk in certain third countries

## Explanatory Memorandum of the Anti-Money Laundering Law

- Articles 13 and 14

## Other reference documents

- FATF Guidance dated 4 November 2017 on Private Sector Information Sharing

## Comments and recommendations by the NBB

- Comments and recommendations

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



# Anti-Money Laundering Law of 18 September 2017 - Articles 13 and 14

## Art. 13

§ 1. Obligated entities that are part of a group shall implement group-wide AML/CFT policies and procedures, including in particular data protection policies and policies and procedures for sharing information within the group for AML/CFT purposes.

Obligated entities established in another Member State or in a third country shall ascertain that these policies and procedures are implemented efficiently within their establishments in that other Member State or third country.

§ 2. Obligated entities established in another Member State shall ensure that their establishments comply with the national provisions of that Member State transposing Directive 2015/849.

§ 3. Obligated entities established in a third country shall ensure that their establishments in that third country comply with the national provisions of that country which provide for minimum AML/CFT requirements that are at least as strict as those provided for in this Law.

Obligated entities established in a third country whose minimum AML/CFT requirements are less strict than those provided for in this Law shall ensure that their establishments implement the obligations set out in this Law, including those regarding data protection, to the extent that the third country's law so allows.

If a third country's law does not permit the implementation of the policies and procedures required pursuant to paragraph 1, obligated entities shall ensure that their establishment in that third country applies additional measures to those provided for locally in order to effectively handle the ML/FT risk, and shall inform their supervisory authority competent in accordance with Article 85.

## Art. 14

Obligated entities may not open a branch or representative office in a country or territory designated by the King pursuant to Article 54.

They may neither directly or indirectly acquire or create a subsidiary operating as an obligated entity that is domiciled, registered or established in the aforementioned country or territory.

# Explanatory Memorandum to the Anti-Money-Laundering Law of 18 September 2017 - Articles 13 and 14

## Art. 13

Article 13 of the draft Law adopts the provisions of Article 16, § 2 of the Law of 11 January 1993 and supplements them to take into account Article 45, paragraphs 1 to 3 and 5, first sentence of the Directive, which is transposed by this Article.

Paragraph 1, first indent of this draft Article expresses the general principle that all companies and branches that form part of one same group must comply with the policies and procedures for AML/CFT established at a group level.

The main aim of this provision is to ensure coherence within a group in the organisation of the different group entities (in particular from the point of view of the tasks of the different AMLCOs), in the customer acceptance policy used, in the form in which the ongoing due diligence is conducted, in the level of internal control, and in the policy for recruiting and training staff on the subject of ML/TF, etc. As with the Directive which it transposes, this provision specifies that this group-wide policy must also include data protection policies, and policies and procedures for sharing information within the group for AML/CFT purposes.

Nevertheless, this obligation should be combined with the principle of territorial application of the anti-money-laundering legislation. This means that the policy of a foreign group to which a Belgian obliged entity belongs may not pose an obstacle to this Belgian obliged entity's application of the provisions of the present draft Law. Likewise, the group-wide policy established by a Belgian parent undertaking must enable the entities established in other Member States to comply with the AML/CFT provisions that apply in those Member States, even if they are stricter than the provisions of the Directive.

The second paragraph of the same § of this draft Article specifies that the Belgian entities that are the parent undertakings of a group must make sure that all subsidiaries and branches of the group established in other Member States or third countries follow the group-wide policy.

In cases where these subsidiaries and branches are established in another Member State, the local legislation on AML/CFT, taking into account the principle of territoriality specified above, may ipso facto be deemed as the level equal to that of the Belgian legislation on AML/CFT, given that this local legislation must arise from the transposition of Directive 2015/849. Nevertheless, the Belgian parent undertaking must ensure that its subsidiary or branch complies with the legislation on AML/CFT of that other Member State (Belgian legislation does not after all apply to this branch or subsidiary).

Pursuant to § 3, first subparagraph, of draft Article 13, the principle under § 2 applies where the subsidiary concerned or the branch concerned is established in a third country where the legislation on AML/CFT lays down obligations at least as strict as those provided for under Belgian legislation. However, this equivalence may not be derived from the fact that the national legislation of that third country arises from the transposition of Directive 2015/849. To be able to apply § 3, first subparagraph of this draft Article, the Belgian obliged entity concerned must therefore conduct a comparative analysis of the legislation of the third country concerned and the Belgian legislation to ascertain whether the condition of equivalence is met. If this analysis reveals that the obligations laid down by the legislation of that country are stricter than those provided for by Belgian legislation, the Belgian parent undertaking must ensure that its branch or subsidiary in that country complies with these stricter obligations.

If, however, the comparative analysis referred to above reveals that the obligations laid down by the national legislation of the third country concerned (or some of these obligations) are less strict than those provided for by Belgian legislation, the parent undertaking must ensure that its subsidiary or branch applies these latter obligations.

Where, in the case described in the previous paragraph, the local legislation does not allow application of the obligations laid down by the Belgian legislation, the parent undertaking must impose additional measures on its branch or subsidiary to effectively handle the ML/TF risk arising therefrom. This could, for example, involve restrictions on activities, exclusion of certain categories of client, etc. Furthermore, the parent undertaking must inform its supervisory authority in Belgium of such measures.

## Art. 14

Article 14 of the draft Law takes over the provision of Article 19 of the Law of 11 January 1993 and extends it to all obliged entities: where the King, aside from the measures that may be taken at an EEA level (in particular, via the approval of European regulations), makes use of Article 54 of the present Law to respond to the FATF's call for its members to take counter-measures against an uncooperative country or territory, the designation by the King of that country or territory automatically leads to obliged entities being prohibited from opening branches or representative offices in that country or on that territory or setting up or acquiring, directly or indirectly, a subsidiary in that country or on that territory.



# NBB anti-money laundering regulation of 21 November 2017 - Articles 6 and 25

## Art. 6

§ 1. Obligated financial institutions established in another Member State or in a third country, or which have subsidiaries that are obliged financial institutions in Belgium, shall take appropriate measures to ensure that their branches and subsidiaries carry out, each for its own account, an overall assessment of the ML/FT risks to which they are exposed in their country of establishment, and that they report back with this overall risk assessment.

§ 2. The obliged financial institutions referred to in Article 5, § 1, 6°, a) to c), and 7°, a) to d), of the Law, shall also ensure that an overall assessment be made of ML/FT risks associated with the activities that they carry out in another Member State or third country through one or several persons who are established and represent them there.

## Art. 25

Obligated financial institutions that are established in another Member State or in a third country, or which have subsidiaries established in Belgium which are obliged financial institutions, shall define their ML/FT policies and procedures group-wide in accordance with Article 13 of the Law on the basis of an assessment of the risks to which the group is exposed, taking account of the risks identified pursuant to Article 6 by each of the subsidiaries and branches that are part of this group. If necessary, they shall also take account of any activities that they carry out in another Member State or in a third country through one or more persons who are established there and who represent them.



# Belgian parent companies: Comments and recommendations

Home > Financial oversight > Combating money laundering and the financing of terrori...

## Contents

- 1. AML/CFTP governance at group level
- 2. Policies, procedures, processes and internal control measures at group level
- 3. Application of local legislation by branches and subsidiaries established abroad

---

This page concerns the parent entities governed by Belgian law which are at the head of a group as defined in Article 4, 22°, of the Anti-Money Laundering Law (see the page “Definitions”).

Although the AML/CFTP legislation and regulations are territorially applicable, the legal and reputational risk incurred by financial institutions that are part of a group and do not have an adequate AML/CFT policy is an overall risk that could affect the whole group, even in circumstances where the incident that creates the risk is located in a single entity of the group.

Thus, the parent entity governed by Belgian law which is at the head of a group must coordinate the AML/CFTP policies of the group's operating entities, in order to ensure that the application of the different AML/CFTP legislations to which they are subject is carried out in a harmonious manner and to achieve an equal level of effectiveness of ML/FT prevention in all these entities. This involves developing AML/CFTP governance at group level and ensuring that a set of appropriate policies, procedures, implementation processes and internal control measures are adopted (see points 1 and 2 below). Where a group has branches or subsidiaries abroad, the parent entity should also ensure that each of the group's entities concerned complies fully with the locally applicable AML/CFTP legislation and regulations, on the one hand, and that the resulting level of requirements is at least equivalent to that required by Belgian legislation and regulations, on the other hand (see point 3 below).

Where the parent entity governed by Belgian law is itself a subsidiary of a parent company governed by Belgian law or by the law of another EEA country or a third country, the NBB considers that this parent entity governed by Belgian law fulfils its obligations defined in Article 13 of the Anti-Money Laundering Law and Articles 6 and 25 of the Anti-Money Laundering Regulation of the NBB by ensuring that the group policy defined by its own parent company and applicable to it:

1. complies with Article 26 of the Anti-Money Laundering Regulation of the NBB (see in this respect the page “Belgian subsidiaries and branches”),
2. enables it to comply with the legal and regulatory obligations that apply to it as a parent entity governed by Belgian law, as well as with the recommendations set out below, and
3. also applies to its own branches and subsidiaries.

If necessary, it should take appropriate additional measures to ensure that these conditions are met.

## 1. AML/CFTP governance at group level

In order to be able to coordinate the AML/CFTP policies at group level, the parent entity must implement an AML/CFTP governance system at group level that is proportionate to its size and ML/FT risk profile.

## 1.1. Role of the board of directors and the management committee of the parent entity of the group

The board of directors and the management committee of the parent entity of the group should implement a system for coordinating the management of ML/FT risks at group level.

Specifically, the parent entity's board of directors must notably (i) decide on the group's general ML/FT risk management strategy, (ii) validate the group's AML/CFTP policy and (iii) define a maximum ML/FT risk tolerance level for the group.

As for the management committee, it must in particular (i) designate a "Group AMLCO" and set up the organisational and operational coordination structure at group level, (ii) validate the group's internal AML/CFTP procedures and ensure that these are consistent with the group's structure and with the size and characteristics of the financial institutions belonging to it, (iii) set up appropriate internal AML/CFTP control mechanisms at group level and (iv) regularly evaluate the effectiveness of the AML/CFTP policy at group level.

## 1.2. "Group AMLCO"

The NBB recommends designating a "Group AMLCO" within the parent entity. The Group AMLCO's tasks are the following:

1. coordinate and supervise the drafting, in accordance with the principles defined at group level, and the effective implementation by each entity of the group of internal procedures for the overall assessment of the ML/FT risks to which it is exposed;
2. organise the centralisation of the results of risk assessments carried out at local level in order to have a good knowledge and understanding of the nature, intensity and location of the ML/FT risks to which the group as a whole is exposed. In this respect, the parent entity of the group should take into account, in its ML/FT risk management system at group level, both the individual risks of the various entities of the group and their possible interrelations that could have a significant impact on group-wide risks. In this respect, particular attention should be paid to the risks to which the group's branches or subsidiaries established in non-equivalent third countries or third countries presenting a high ML/FT risk are exposed (see below);
3. taking into account the knowledge of the ML/FT risks to which the group is exposed, coordinate the definition of the AML/CFTP policies and procedures of the different entities of the group with a view to ensuring consistency and a high level of effectiveness of prevention measures throughout the group. In this respect, the Group AMLCO should ensure that local policies and procedures not only guarantee compliance with the AML/CFTP legislations and regulations applicable to each entity of the group individually, but also aim, more broadly, to identify, control and reduce local ML/FT risks in a manner consistent with the principles applicable in this respect throughout the group;
4. coordinate the activities of the various local AMLCOs in the group's operational entities in order to ensure that they work consistently.

This coordination at group level should not affect the legal capacity of subsidiaries and branches to meet their legal and regulatory obligations applicable at local level and the capacity of the management bodies of these entities to manage their local AML/CFTP policy.

## 1.3. Intra-group outsourcing

The local rules on outsourcing must be respected when AMLCO functions of local entities are outsourced in their entirety to the group AMLCO located in the parent company. Without prejudice to these rules, the parent entity of the group should (i) also establish an inventory of cases of intra-group AML/CFTP outsourcing, in order to determine which function relates to which legal entity and (ii) ensure that intra-group outsourcing does not compromise the compliance of each subsidiary with its AML/CFTP obligations. See in this respect item 3 of the "Governance" page.

# 2. Policies, procedures, processes and internal control measures at group level

In order to be able to coordinate the group's AML/CFTP policies, the parent entity should define and implement a set of (i) policies, (ii) internal procedures, (iii) implementation processes and (iv) internal control measures. These policies, procedures, processes and internal control measures must be proportionate to the size and the AML/CFTP risk profile of the group.

## 2.1. Risk assessment at group level

It is recommended that the AML/CFTP organisation of the group provides appropriate measures to centralise the results of the overall risk assessments of the different entities of the group at parent entity level. This centralisation must enable the parent entity to know and understand the nature, intensity and location of the ML/FT risks to which the group as a whole is exposed, also taking into account possible interrelations between the ML/FT risks to which different entities of the group are exposed and which may have an impact on the group, in order to adequately respond to the BC/FT risks to which the group is exposed.

## 2.2. AML/CFTP policy of the group

The group-wide AML/CFTP policy includes the fundamental principles to be followed within the group to ensure proper coordination of the measures taken to prevent the ML/FT risk to which the group is exposed. This policy should cover two aspects:

1. ML/FT risk assessment at group level, and
2. customer acceptance.

### 2.2.1. ML/FT risk assessment at group level

One of the key points for effective and relevant management of ML/FT risks within the group is the implementation of consistent AML/CFTP standards throughout the group. It is therefore important that each group develops a general policy for the management of the group's ML/FT risks which provides a framework for the specific ML/FT risk management policies applicable in each entity of the group. The latter must implement the standards applicable throughout the group at the level of the entity concerned and ensure their effectiveness, even when local specificities or specificities related to the activities carried out also need to be taken into consideration.

The ML/FT risk management policy at group level should include at least:

1. The main principles of the risk-based approach to be implemented throughout the group. These main principles should cover at least (i) uniform rules for the elaboration of global risk assessments in the operational entities and (ii) standard risk criteria on which the risk-based approach developed at local entity level is based;
2. The maximum level of ML/FT risk tolerance for the group;
3. Guidelines to be followed in managing the AML/CFTP policies at local level. These guidelines include in particular:
  - criteria to ensure an equivalent level of customer and transactions due diligence and diligence with regard to the analysis of atypical transactions. These standards should concern at least:
    - the essential rules of the system for monitoring business relationships and transactions, and
    - the procedural rules for the analysis and the follow-up to be given, on the basis of that analysis, to the atypical operations detected;
  - the main principles to be followed in the organisation of the AML/CFTP policy to be implemented throughout the group. Such measures include in particular:
    - the implementation of an adequate organisation, taking into account in particular the principle of separation of functions,
    - the implementation of procedures laid down in accordance with the essential principles defined at group level,
    - information exchange and feedback to local entity management bodies, and
    - the effective inclusion of the control of AML/CFTP aspects in the scope of the internal audit.

### 2.2.2. Customer acceptance within the group

The risk-based approach applied by each entity of the group to identify customers, verify their identity, know customers characteristics, know the purpose and nature of business relationships, and to accept customers must be defined in accordance with the legal and regulatory provisions applicable to the entity concerned and taking into account the specific features of the activities it carries on.

Nevertheless, the rules for the risk-based approach implemented by the various entities should be coordinated at group level in order to guarantee consistency throughout the group and to ensure that each entity of the group imposes on itself the required level of rigour in collecting and verifying the information required for consistent application of the customer acceptance policy.

Thus, the parent entity of the group is expected to define a group policy for customer acceptance in order to guarantee a consistent assessment of the risks that customers may represent, regardless of the group entity with which they wish to enter into a relationship.

This customer acceptance policy of the group should contain:

1. general risk criteria for classifying customers by risk category; and
2. procedural rules relating to the examination of applications and the decision to enter into a relationship with customers, depending on the level of risk that these customers are likely to present.

### 2.3. Internal procedures of the group

Based on its group AML/CFTP policy, the parent company of a group must ensure that each entity of the group has established and effectively implements all required internal AML/CFTP procedures.

In addition, in accordance with Article 13 of the Anti-Money Laundering Law, at least two internal group procedures must be developed: (i) a procedure for sharing information within the group and (ii) a data protection procedure.

#### 2.3.1. Internal information sharing procedure of the group

The exchange of information between the group entities is essential for the full effect of the group's AML/CFTP policy.

In view of the specific nature of this information, the NBB expects financial institutions to allow only the AMLCO or members of its team to transmit and/or have access to the exchanged customer information.

The NBB considers that exchange of information within the group seems particularly desirable with a view to:

- consistently implementing the ML/FT risk assessment obligations in the different entities of the group;
- implementing the group's customer acceptance policy (in particular with a view to identifying customers who enter into business relationships or carry out transactions through various entities of the group);
- consistently exercising due diligence towards customers, business relationships and transactions, taking into account, in particular, all business relationships and transactions entered into by the same customer with various entities of the group;
- analysing detected atypical transactions in order to meet the legal obligations to report suspicions, and to ensure an appropriate follow-up of these reports within the group (cf. Art. 56, § 2, 1° and 2° of the Anti-Money Laundering Law).

Examples of information that may be exchanged within a group include in particular:

- identification data of customers and, where applicable, agents and beneficial owners;
- information relating to the purpose and nature of the business relationship;
- information necessary to know the customer;
- any other relevant information on the customer and its transactions which may be necessary for the assessment of the ML/FT risks presented by the customer.

It is recalled that the notion of group is defined in Belgium in Article 4, 22° of the Anti-Money Laundering Law. This notion covers in particular all branches and subsidiaries, irrespective of whether the power is exercised by holding a majority of the voting rights or by other means listed in Article 22.1.b. to d. of Directive 2013/34/EU.

#### 2.3.2. Internal data protection procedure of the group

Since the exchange of information within the group described above will generally involve the transmission, between the entities of the group, of personal data concerning the customers, the framework for this exchange must be defined in compliance with the legal provisions on the protection of personal data that are applicable. It is therefore important to ensure that these information flows comply with Regulation 2016/679 of 27 April 2016 on the protection of personal data ("GDPR"). Account should be taken of the conditions under which, in accordance with the said

Regulation, the transmission of information to subsidiaries and branches located in EEA countries, as well as the additional conditions to which the said Regulation subjects the transmission of information to entities located in third countries.

## 2.4. Implementation process at group level

To effectively coordinate the AML/CFTP policies applicable at local level, the group AMLCO must have at its disposal an IT tool to effectively implement information sharing on the AML/CFTP aspects within the group.

## 2.5. Internal control measures within the group

The group's parent entity must ensure that internal control measures are adopted to ensure that the AML/CFTP policies that are implemented within the group's various operating entities are applied harmoniously and consistently. These mechanisms inter alia involve the regular performance of internal AML/CFTP audits by the internal audit function of the group.

Furthermore, if the group includes subsidiaries or branches abroad (EEA or third countries), the parent entity must ensure, if necessary through on-site controls conducted by its internal audit function, that these subsidiaries and branches actually have the required administrative organisation and internal control, not only to comply with local AML/CFTP legislation, but also with the various above-mentioned standards defined at group level.

# 3. Application of local legislation by branches and subsidiaries established abroad

The provisions of the Law and the Anti-Money Laundering Regulation of the NBB have a territorial scope. They therefore do not apply to branches and subsidiaries of a Belgian parent entity that are established abroad. However, pursuant to the same principle of territoriality, these branches and subsidiaries are subject to the legal and regulatory AML/CFTP provisions of their country of establishment.

In this respect, a distinction can be made depending on whether the subsidiary or branch is located in an EEA country or in a third country.

## 3.1. Branches and subsidiaries established in another EEA country

Where subsidiaries or branches are established in another EEA country, Article 13, § 2 of the Anti-Money Laundering Law provides that such subsidiaries and branches are required to ensure compliance with the national provisions of that other country transposing Directive 2015/849. However, with a view to the sound management of ML/FT risks, the Belgian parent entity of a group must also ensure that these subsidiaries and branches also comply with the group's AML/CFTP policies.

## 3.2. Branches and subsidiaries established in a third country

Where subsidiaries or branches are established in third countries, Article 13, § 3 of the Anti-Money Laundering Law makes a distinction according to whether or not the third country is considered equivalent:

- In case of a third country imposing minimum AML/CFTP obligations at least as strict as those provided for in the Anti-Money Laundering Law, the Belgian parent entity must ensure that its subsidiaries and branches established in that third country comply with the national AML/CFTP provisions of that third country.. The Belgian parent company must also ensure that these subsidiaries and branches comply with the group's AML/CFTP policies.
- In case of a third country imposing minimum AML/CFT obligations which are less strict than those provided for in the Anti-Money Laundering Law, the Belgian parent company must ensure that its subsidiaries and branches concerned apply the obligations set out in the Belgian Anti-Money Laundering Law (including data protection obligations, as far as the law of the third country allows). In concrete terms, this means that branches and subsidiaries of Belgian groups must apply measures complementary to those provided for locally to deal effectively with ML/FT risks. In addition, the Belgian parent company must also ensure that these branches and subsidiaries fully comply with the group-wide policies and procedures. If local legislation precludes the application of these stricter regulations, the parent company must take appropriate measures,

in accordance with the provisions of Commission Delegated Regulation (EU) 2019/758 of 31 January 2019 on the one hand, and inform the NBB, on the other.

Where a financial institution carries out transactions or maintains business relations with natural or legal persons or with legal arrangements, such as trusts or fiducies, which are established in a high-risk third country, Article 38, paragraph 1, of the Anti-Money Laundering Law requires it to implement enhanced due diligence measures (see the page "High-risk third countries"). Where a Belgian parent entity has established a branch or subsidiary in such a country, it must in principle require that subsidiary or branch, pursuant to Article 13, § 3, paragraph 2, of the Anti-Money Laundering Law, to implement such enhanced due diligence measures with regard to all its own local customers. Nevertheless, Article 38(2) of the Anti-Money Laundering Law provides that financial institutions may "*based on an individual risk assessment, authorise [these branches and subsidiaries] to not automatically apply enhanced customer due diligence measures, provided that they ensure that the branches and subsidiaries concerned fully comply with the group-wide policies and procedures*".

The NBB considers that the correct application of the above-mentioned legal obligations implies that the Belgian parent entity which plans to establish a branch or subsidiary in a third country carries out or has carried out a detailed and reliable legal analysis of the legal and regulatory framework in the field of AML/CFTP and other related matters (in particular the protection of personal data and privacy) which is in force in the host country, in order to determine whether this legal framework can be considered equivalent or, if not, to identify the local law provisions that are less stringent than those laid down under Belgian law and to determine which additional obligations should be imposed by the parent entity on its subsidiary or branch established in the third country concerned. Moreover, as the locally applicable legal framework is likely to evolve over time, the NBB considers that parent entities must have appropriate "regulatory due diligence" mechanisms in order to be rapidly informed of any relevant legislative or regulatory changes in third countries in which subsidiaries or branches of the group are established. It is their responsibility to update their above-mentioned legal analyses on this basis in order, if necessary, to rapidly adopt appropriate measures with regard to their subsidiaries and branches concerned if these legal or regulatory changes require so. The NBB expects the Belgian parent entities to be able to provide it, on first request, with a copy of their updated legal analyses concerning each of the third countries in which subsidiaries and branches of the group are established, and to demonstrate to it that the additional measures imposed on them are appropriate to achieve a level of requirements equivalent to that provided for by Belgian legislation.

If a Belgian parent entity wishes to make use of the option provided for in Article 38, paragraph 2, of the Anti-Money Laundering Law, referred to above, the NBB recommends:

- supplementing the above-mentioned legal analysis of the local legal and regulatory framework with a carefully documented written risk assessment in order to specifically identify the risks to which the local entity and the group are exposed, in relation to customers established in the country concerned, as a result of weaknesses and gaps in local AML/CFTP legislation;
- being able to demonstrate that the application of existing group-wide policies and procedures in force, adapted where necessary to include specific measures, does substantially reduce the identified risks;
- ensuring that the local entity's compliance with these policies and procedures is subjected to special monitoring, paying particular attention, where appropriate, to compliance with the measures specifically set out in these policies and procedures in order to reduce the identified risks.

Finally, in accordance with Article 14 of the Anti-Money Laundering Law, it is recalled that financial institutions may never open a branch or representative office in countries designated by the King pursuant to Article 54 of the Law.

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



# Belgian subsidiaries and branches

Home > Financial oversight > Combating money laundering and the financing of terrori...

## Legal and regulatory framework

- Anti-Money Laundering Law: Art. 13, § 1
- Anti-Money Laundering Regulation of the NBB: Art. 26

## Explanatory Memorandum of the Anti-Money Laundering Law

- Art. 13, § 1

## Comments and recommendations by the NBB

This page pertains to subsidiaries governed by Belgian law or branches established in Belgium that are part of a group of which the parent company is a financial institution governed by foreign law (of another EEA country or a third country). In such a case, as the Belgian AML/CFTP legislation and regulations have a territorial scope, it should be ensured that the coordination in the area of AML/CFTP that exists at group level is without prejudice to the legal capacity of subsidiaries governed by Belgian law and of branches established in Belgium to fulfil their legal and regulatory AML/CFTP obligations in Belgium.

For this purpose, the Belgian entity (a subsidiary governed by Belgian Law or a branch established in Belgium) should analyse the compliance of the group policies and procedures with the legal and regulatory AML/CFTP provisions applicable in Belgium (see point 1) and ensure that its parent company, if necessary, takes certain measures guaranteeing its permanent ability to comply with these provisions (see point 2). If all or some of the tasks of the Belgian entity's AMLCO are outsourced to the parent company or to another entity of the group, particular attention should also be paid to the recommendations by the NBB in this area (see point 3).

### 1. Analysis of compliance of group AML/CFTP policies and procedures with the legal and regulatory AML/CFTP provisions applicable in Belgium

In accordance with Article 26 of the Anti-Money Laundering Regulation of the NBB, the NBB expects the AMLCOs of Belgian subsidiaries or branches that are part of a foreign group to assess, before implementing the ML/FT risk prevention policies and procedures defined at group level, whether these comply with the provisions referred to in Article 8 of the Anti-Money Laundering Law and with the provisions of the Anti-Money Laundering Regulation of the NBB. This compliance analysis should be retained within the Belgian entity and should be available for submission to the NBB at its first request.

If the ML/FT risk prevention policies and procedures defined at group level could potentially impede the proper implementation of the aforementioned provisions by the Belgian entity, the Belgian entity's AMLCO should ask its parent company for an exemption from the policy and procedures defined at group level in order to remedy the

incompatibility found. Where it is not possible to bring the measures imposed by the group into compliance with the aforementioned provisions by applying this exemption procedure, the AMLCO should inform the NBB to enable the latter to examine the consequences of this situation and determine the measures to be taken to remedy it, where appropriate in the context of its collaboration with the competent supervisory authority of the country of origin.

## 2. Governance mechanisms within the group

In terms of governance, the group's organisation and management should not run counter to the legal and regulatory AML/CFTP provisions to which the subsidiaries governed by Belgian law and the branches established in Belgium are subject.

For instance, it should be ensured that appropriate internal mechanisms within the group allow the autonomy of the Belgian entity's management bodies in relation to AML/CFTP to be maintained. These mechanisms should be based in particular on:

1. an adequate allocation of tasks between the AMLCO of the group and the Belgian AMLCO;
2. a governance system at the level of the parent company that is respectful of the autonomy of the Belgian entity in relation to AML/CFTP, and particularly of the fact that the Belgian entity's AML/CFTP policy is effectively managed by the Belgian financial institution's management bodies (board of directors and management committee or senior management);
3. a system for the mutual exchange of information within the group which enables both the AMLCO of the group and the AMLCO of the Belgian entity to receive useful information; and
4. a system for managing conflicts of interest within the group that covers the aspects related to AML/CFTP.

The management bodies (board of directors and management committee or senior management) of the subsidiary governed by Belgian law or of the branch established in Belgium should ensure that these mechanisms are implemented at the level of the parent company. Additionally, they should ensure that the parent company takes full account of the need to provide the Belgian entity's AMLCO or, where appropriate, the AML unit with adequate human and technical resources to enable it to comply effectively with the Belgian legal and regulatory AML/CFTP obligations. Particular attention should also be paid to the resources of the Belgian entity's internal audit function, as it must ensure that the AML/CFTP policy implemented within the Belgian entity is in full compliance with the legal and regulatory AML/CFTP provisions applicable in Belgium.

## 3. Outsourcing of tasks of the Belgian entity's AMLCO within the group

The recommendations above also apply if all or some of the tasks of the Belgian entity's AMLCO are outsourced to the foreign parent company or to another entity of the same group.

As regards the compliance analysis of group policies and procedures referred to in point 1:

- in case of partial outsourcing, the analysis should be performed by the Belgian entity's AMLCO with regard to all his tasks and should be completed by an impact analysis of this outsourcing which demonstrates that it does not impair compliance with the legal and regulatory AML/CFTP provisions applicable in Belgium;
- if all tasks of the Belgian entity's AMLCO are outsourced to the parent company or to another entity of the same group, the aforementioned compliance and impact analyses of the outsourcing should be performed, as the case may be, by the AMLCO or by the senior officer acting as AMLCO, where appropriate assisted by the liaison on the Belgian entity's payroll. This analysis should be retained within the Belgian entity and should be available for submission to the NBB at its first request.

Moreover, the group's internal governance mechanisms included in point 2 above are fully applicable. The Belgian entity should also take particular care to ensure that these governance rules are properly complied with at the level of the parent company.

For further information on outsourcing, see also the pages "Governance" and "Performance of obligations by third parties".

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**





# Anti-Money Laundering Law of 18 September 2017 - Article 13 § 1

## Art. 13

§ 1. Obligated entities that are part of a group shall implement group-wide AML/CFT policies and procedures, including in particular data protection policies and policies and procedures for sharing information within the group for AML/CFT purposes.

Obligated entities established in another Member State or in a third country shall ascertain that these policies and procedures are implemented efficiently within their establishments in that other Member State or third country.



# Explanatory Memorandum to the Anti-Money-Laundering Law of 18 September 2017 - Article 13 § 1

## Art. 13 §1

Article 13 of the draft Law adopts the provisions of Article 16, § 2 of the Law of 11 January 1993 and supplements them to take into account Article 45, paragraphs 1 to 3 and 5, first sentence of the Directive, which is transposed by this Article.

§ 1 of this draft Article begins by expressing the general principle that all companies and branches that form part of the same group must comply with the policies and procedures for AML/CFT established at group level.

The main aim of this provision is to ensure coherence within a group in the organisation of the different group entities (in particular from the point of view of the tasks of the different AMLCOs), in the customer acceptance policy used, in the form in which the ongoing due diligence is conducted, in the degree of internal control, and in the policy for recruiting and training staff on the subject of ML/TF, etc. Just like the Directive it transposes, this provision specifies that this group-wide policy must also include data protection policies, and policies and procedures for sharing information within the group for AML/CFT purposes.

Nevertheless, this obligation should be combined with the principle of territorial application of anti-money-laundering legislation. This means that the policy of a foreign group to which a Belgian obliged entity belongs may not cause an obstacle to this Belgian obliged entity's application of the provisions of the present draft Law. Likewise, the group-wide policy established by a Belgian parent undertaking must enable the entities established in other Member States to comply with the AML/CFT provisions that apply in those Member States, even if they are stricter than the provisions of the Directive.

The second indent of § 1 specifies that the Belgian entities that are the parent undertakings of a group must make sure that all subsidiaries and branches of the group established in other Member States or third countries follow the group-wide policy.



# NBB anti-money laundering regulation of 21 November 2017 - Article 26

## Art. 26

Obligated financial institutions that are part of a group whose parent company is an obliged financial institution governed by the law of another Member State or a third country shall assess, under the responsibility of the AMLCO, before implementing them, whether the ML/FT policies and procedures defined group-wide comply with the provisions mentioned in Article 8 of the Law and with those set out in this Regulation. Otherwise, they shall ask their parent company for an exemption from the policy and procedures defined at group level in order to guarantee compliance with the above-mentioned legislative and regulatory provisions. Where it is not possible for the measures imposed by the group to comply with the said provisions by applying this exemption procedure, they shall inform the Bank.



# Belgian central contact points of European payment institutions and electronic money institutions

Home > Financial oversight > Combating money laundering and the financing of terrori...

## Legal and regulatory framework

- RTS on CCP to strengthen fight against financial crime
- Anti-Money Laundering Law: Article 15
- Anti-Money Laundering Regulation of the NBB: Article 27

## Explanatory Memorandum of the Anti-Money Laundering Law

- Article 15

## Other reference documents

- EBA Opinion dated 24 April 2019 on the nature of passport notifications regarding agents and distributors under Directive 2015/2366 (PSD2), Directive 2009/110/EC (EMD2) and Directive 2015/849 (AMLD)

## Comments and recommendations by the NBB

- Comments and recommendations

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



# Anti-Money Laundering Law of 18 September 2017 - Article 15

## Art. 15

The obliged entities referred to in Article 5, § 1, 6°, d), and 7°, e), shall, under the conditions set by the National Bank of Belgium through a regulation adopted in accordance with the implementing measures of Directive 2015/849 referred to in Article 45(10) of the said Directive, appoint a central contact point situated in Belgium that is charged with ensuring, on behalf of the appointing obliged entity, compliance with the provisions of this Law and its implementing decrees and regulations, as well as facilitating the National Bank of Belgium's performance of its supervisory tasks, particularly by providing this authority with all documents and information requested by it.

The regulation referred to in the first paragraph shall specify in particular the functions to be performed by the appointed central contact points.



# NBB anti-money laundering regulation of 21 November 2017 - Article 27

## Art. 27

§ 1. Pursuant to Article 15 of the Law, the obliged financial institutions referred to in Article 5, § 1, 6°, d), and 7°, e), of the Law, shall appoint a central contact point situated in Belgium when at least one of the following criteria is met:

1° the number of the obliged financial institution's establishments situated in Belgium is equal to or exceeds 10;

2° the cumulative amount of the electronic money distributed and redeemed in Belgium or the cumulative value of the payment transactions executed in Belgium by the obliged financial institution's establishments situated in Belgium is expected to exceed three million euros per financial year or has exceeded three million euros in the previous financial year;

3° the information necessary to assess whether or not the criterion referred to in 1° or 2° is met, is not made available to the Bank upon request and in a timely manner;

Without prejudice to the first paragraph, obliged financial institutions referred to in it shall appoint a central contact point situated in Belgium:

1° when the obliged financial institution's establishments situated in Belgium execute transactions there that may imply the use of cash or anonymous electronic money;

2° when the Bank decides and publishes on its website that the exercise in Belgium of a specific activity so requires on the basis that this activity is identified as presenting a high level of ML/FT risks by the European Commission in the risk assessment referred to in Article 6 of Directive 2015/849, by the coordinating bodies in the national risk assessment referred to in Article 68 of the Law, or by the Bank itself on the basis of a documented risk analysis;

3° when the Bank requires an obliged financial institution to do so, providing it deems it appropriate on the basis of a documented analysis with regard to the high level of ML/FT risks to which this obliged financial institution is exposed through the exercise in Belgium of a specific activity;

§ 2. Apart from the functions provided for by the regulatory technical standards referred to in Article 45(11), of Directive 2015/849 with a view to ensuring compliance with AML/CFT rules and facilitating supervision by competent authorities, the central contact point appointed in accordance with paragraph 1 shall perform the following additional functions:

1° detect atypical transactions or, at the very least, ensure that the criteria used for detecting atypical transactions comply with the provisions of the European Regulation on transfers of funds, of the Law and of this Regulation, and are appropriate for the activities carried out in Belgium by the obliged financial institution;

2° decide whether suspicions should be reported pursuant to Article 47 of the Law and, where appropriate, the content of any such report;

3° reply, in accordance with Article 48 of the Law, to any request for information from the CTIF-CFI concerning the activities carried out by the obliged financial institution's establishments situated in Belgium.

# Explanatory Memorandum to the Anti-Money-Laundering Law of 18 September 2017 - Article 15

## Art. 15

Article 15 of the draft Law must be read in combination with Article 5, § 1, 6°, d) and 7°, e) and with Article 9, § 4. This Article pertains to cases of obliged entities that are payment institutions or electronic money institutions governed by the law of another Member State and established on Belgian territory exclusively via agents or distributors established in Belgium representing these obliged entities. In such cases, Member States are authorised to require, by virtue of Article 45, paragraph 9 of Directive 2015/849, these institutions to appoint a “central contact point” in their territory that is charged with ensuring, on behalf of the appointing institution, compliance with the AML/CFT rules and with facilitating supervision by the competent authorities.

Pursuant to Article 45, paragraph 10 of the Directive, the European Commission will be required to adopt the regulatory technical standards proposed by the ESAs concerning the criteria for determining the circumstances in which the appointment of a central contact point is appropriate, and what the functions of the central contact points should be. As a reminder, regulatory technical standards are legislative texts that aim for maximum harmonisation and are directly applicable in the Member States.

Taking this context into account, Article 15 of the draft Law maintains, albeit more expressly, the option that Belgium already used under the Law of 11 January 1993 to require in these cases that the obliged entities designate a central contact point in Belgium. It has transpired that such a designation ensures quicker and more efficient reporting to the CTIF-CFI of suspicions with regard to, inter alia, money transfers in which cash or anonymous electronic money is handled, and facilitates supervision, both by the obliged entity itself and by the competent supervisory authority (the NBB: see below), of the activity of a potentially very high number of agents or distributors in Belgium.

In view of the fact that a significant part of the rules that apply to these central contact points will already be laid down through directly applicable regulatory technical standards, it is not necessary for this draft Law to provide for a more detailed organisation of these rules. However, insofar as it would appear necessary to supplement, at national level, the rules already established at European level, the NBB is empowered, pursuant to Article 15 of the draft Law, to determine the conditions that these central contact points will have to meet, and the functions they will need to perform by way of a regulation in accordance with the aforementioned regulatory technical standards.



# Belgian central contact points of European payment institutions and electronic money institutions: Comments and recommendations

Home > Financial oversight > Combating money laundering and the financing of terrori...

## Contents

- 1. Background
- 2. Appointment of a CCP in Belgium
- 3. Functions of the CCP in Belgium

## 1. Background

Firstly, it should be noted that, in accordance with the provisions of Directive 2015/849, the provisions of the Anti-Money Laundering Law and of the Anti-Money Laundering Regulation of the NBB have a territorial scope. As a result, they apply in particular to financial institutions that are governed by the law of another EEA country or of a third country and that are established on Belgian territory to offer financial services or products there, regardless of the form of the institution. The fact whether or not the institution exclusively takes the form of one or more independent agents or independent distributors operating under representation contracts concluded with the financial institution, without the latter establishing any other form of organisation (branch) on Belgian territory, in no way alters the fact that this financial institution, **within the limits of the activities it carries out in Belgium** through its agents or distributors, (i) is subject to all obligations set out in Book II of the Anti-Money Laundering Law and to the provisions of the Anti-Money Laundering Regulation of the NBB – including the obligations regarding appropriate organisation –, (ii) is required to notify CTIF-CFI of any suspicious transactions carried out in Belgium, (iii) is subject to the obligations regarding financial embargoes and asset freezes applicable in Belgium, including those resulting from the Belgian list of persons subject to targeted financial sanctions, (iv) falls under the supervisory and sanction powers of the NBB, (v) etc. (for further details on this subject, see the EBA Opinion dated 24 April 2019).

To facilitate the effective implementation of the above principles, Article 15 of the Anti-Money Laundering Law requires payment institutions and electronic money institutions that are governed by the law of another EEA country and provide payment services or distribute electronic money in Belgium “through one or more persons established in Belgium who represent the institution for that purpose” to appoint, “under the conditions set by the National Bank of Belgium through a regulation adopted in accordance with the implementing measures of Directive 2015/849 referred to in Article 45(10) of the said Directive”, **a central contact point** (hereinafter referred to as “CCP”) **situated on Belgian territory**.

**The obliged entities subject to this obligation** are, specifically, the payment institutions and electronic money institutions that are governed by the Law of another EEA country (hereinafter referred to as “European payment or electronic money institutions”) and respectively provide payment services or distribute electronic money in Belgium **solely through agents or distributors**. On behalf of the institution that appointed it and in the same way as the AMLCO appointed pursuant to Article 9, § 2, of the Anti-Money Laundering Law would do if the European payment institution or electronic money institution concerned operated in Belgium through a branch (see point 2 of the “Governance” page), this CCP should ensure compliance with the legal and regulatory AML/CFTP provisions applicable in Belgium and facilitate the NBB’s performance of its supervisory tasks, particularly by providing it with all documents and information requested by it.

The implementing measures of the Directive referred to in its Article 45(10) and mentioned in Article 15 of the Anti-Money Laundering Law, are the **regulatory technical standards of the European Commission** (“RTS”), which determine:

- the cases in which EEA countries in whose territory payment institutions or electronic money institutions governed by another EEA country provide payment services or distribute electronic money through agents or distributors (hereinafter referred to as the “host country”) may require a CCP to be appointed on their territory (see Article 3 of the RTS);
- the minimum functions to be performed by the CCP if its appointment is required (see Articles 4 and 5 of the RTS), as well as certain functions that the host country of the CCP could require it to perform additionally (see Article 6 of the RTS).

The ESAs present these regulatory technical standards to the European Commission for adoption. Once adopted, these legal acts are directly applicable in EEA countries. The rules adopted at the European level are supplemented at the national level by the provisions of **Article 27 of the Anti-Money Laundering Regulation of the NBB** which, in accordance with the aforementioned technical standards, establish:

- the cases in which the European payment or electronic money institutions providing payment services or distributing electronic money **in Belgium** through agents or distributors should appoint a CCP on Belgian territory (see Article 27, § 1, of the Anti-Money Laundering Regulation of the NBB);
- the functions which this CCP is required to perform **in addition to the minimum functions provided for in the RTS** (see Article 27, § 2, of the Anti-Money Laundering Regulation of the NBB).

As such, Belgium exercises the options provided for in the RTS, allowing EEA countries to require (i) that a CCP be appointed on their territory, and (ii) that this CCP perform functions in addition to those laid down in these RTS.

**In other words**, European payment or electronic money institutions offering payment services or distributing electronic money in Belgium solely through agents or distributors should refer to:

- Article 27, § 1, of the Anti-Money Laundering Regulation of the NBB, adopted pursuant to Article 3 of the RTS, to determine the cases in which they should appoint a CCP situated in Belgium;
- Articles 4 and 5 of the RTS, read in conjunction with Article 27, § 2, of the Anti-Money Laundering Regulation of the NBB, to know which functions should be performed by this CCP.

## 2. Appointment of a CCP in Belgium

European payment or electronic money institutions operating in Belgium through agents or distributors should appoint a CCP situated in Belgium **if any of the following criteria are met** (see Article 27, § 1, first paragraph, of the Anti-Money Laundering Regulation of the NBB, adopted pursuant to Article 3, paragraph 1 of the RTS):

1. the European institution concerned provides payment services or distributes electronic money in Belgium **through at least ten agents or distributors**;
2. this institution effects payment transactions or distributes or redeems electronic money in Belgium **the cumulative amount of which (i) is expected to exceed three million euros at the end of the financial year or (ii) has exceeded three million euros in the previous financial year**;
3. the information necessary to assess whether the previous two criteria are met **is not made available to the Bank in a timely manner**;

Moreover, **in any case**, even if the previous criteria are not met, a CCP situated in Belgium should also be appointed in the following cases:

1. when the agents or distributors of the European institution concerned that are situated in Belgium effect **transactions there that may involve the use of cash or anonymous electronic money** (see Article 27, § 1, second paragraph, 1°, of the Anti-Money Laundering Regulation of the NBB, adopted pursuant to Article 3, paragraph 2 of the RTS).

Transactions that “*may involve the use of cash or anonymous electronic money*” not only refer to cases where funds are received from customers in these forms by the payment or electronic money institution, but also to cases where transfers of funds received in any form by the payment institution can be delivered in these forms to the beneficiaries in Belgium, or where non-anonymous electronic money can be redeemed in cash or converted to anonymous electronic money on Belgian territory.

The particularly risky nature, in terms of ML/FT, of transactions that may involve cash or anonymous electronic money, which justifies the requirement to appoint a CCP on Belgian territory when such transactions are effected there, (i) even if the payment or electronic money institution concerned only operates there through a single agent or distributor, and (ii) regardless of the value of the transactions effected, as the quantitative criteria referred to in Article 27, § 1, first paragraph, of the Anti-Money Laundering Regulation of the NBB do not apply in those cases – is apparent:

- from the ratio legis of the provisions of the European Regulation on transfers of funds (Articles 5 to 7), which impose enhanced customer identification measures for transfers of funds involving cash or anonymous electronic money;
- from the ratio legis of Book III of the Anti-Money Laundering Law, which limits the use of cash;
- from the Supranational Risk Assessment Report published by the European Commission on 26 June 2017, in accordance with Article 6 of the Directive (see pages 10, 15 and 19 in particular);
- from the ESA guidelines of 4 January 2018 on risk factors (see pages 45, 46, 51 and 52 in particular).

Furthermore, the use of transactions involving cash is mentioned by CTIF-CFI in a very large number of money laundering or terrorist financing typologies, which it publishes in its successive annual reports, thereby confirming the high ML/FT risk associated with this type of transactions.

2. **when the NBB decides and publishes on its website that the performance of a specific activity in Belgium so requires**, on the grounds that this activity is considered as presenting high ML/FT risks, either by the European Commission in the supranational risk assessment conducted pursuant to Article 6 of the Directive, by the coordinating bodies in the national risk assessment referred to in Article 68 of the Anti-Money Laundering Law, or by the NBB itself based on a documented analysis (see Article 27, § 1, second paragraph, 3°, of the Anti-Money Laundering Regulation of the NBB, adopted pursuant to Article 3, paragraph 2 of the RTS);

If payment or electronic money institutions perform other activities than those referred to in point a) above, that would be identified in the future as presenting a particularly high ML/FT risk, and if they only perform these activities on Belgian territory through one or more agents or distributors, the NBB could require them to appoint a CCP situated in Belgium.

3. **when the NBB requires a European payment or electronic money institution to do so**, on the grounds that it deems this appropriate, based on a documented analysis, in light of the high ML/FT risks to which this institution is exposed by performing a specific activity in Belgium (see Article 27, § 1, second paragraph, 3°, of the Anti-Money Laundering Regulation of the NBB, adopted pursuant to Article 3, paragraph 3 of the RTS).

In that case, the Bank will decide on an individual basis, with due regard to the specific situation of the payment or electronic money institution concerned. This could be the case, in particular, when the NBB finds that a European payment or electronic money institution that has not established a CCP in Belgium grossly fails to comply with the Belgian anti-money laundering legislation and regulations in the context of the activities it carries out through its Belgian agents and distributors, and that this institution does not seem to be able to remedy these serious shortcomings from its registered office, as a result of which the ML/FT risks associated with the activities carried out in Belgium should be considered high if they are not subject to adequate reduction and management measures.

## 3. Functions of the CCP in Belgium

### 3.1 General principles

The overall objective of appointing a CCP is to ensure the presence, in the country on the territory of which a payment or electronic money institution governed by another EEA country offers payment services or distributes electronic money solely through agents or distributors, of a person or entity responsible for ensuring the proper implementation of the AML/CFTP provisions in place on that territory.

The positioning of a person or entity assuming such a central function on the – in this case Belgian – territory aims, on the one hand, to better guarantee the quality and speed of the reporting of suspicions to CTIF-CFI (especially with regard to transactions that are particularly exposed to ML/FT risk, i.e. transfers of funds involving the handling of cash or anonymous electronic money) and, on the other hand, to facilitate the monitoring, both by the European payment or electronic money institution itself and by the NBB, of the activities of a potentially very large number of agents or distributors in Belgium.

It should be stressed that it is the European payment or electronic money institution, not the CCP itself, which remains subject to the Anti-Money Laundering Law and which is **responsible** for the proper performance of its legal and regulatory AML/CFTP obligations. Unlike the European payment or electronic money institution concerned, which is responsible for the actions of its agents or distributors and of the CCP it appointed in Belgium, the CCP therefore cannot be subject to the administrative measures referred to in Articles 93 and 94 of the Anti-Money Laundering Law or to the administrative sanctions referred to in Articles 132 to 135 of the Law.

It should also be noted that, in accordance with Article 95 of the Anti-Money Laundering Law, when the NBB finds that a European payment or electronic money institution has committed in Belgium a serious breach of the AML/CFTP provisions applicable – namely the provisions of Book II of the Anti-Money Laundering Law, the Anti-Money Laundering Regulation of the NBB, the RTS, the European Regulation on transfers of funds or the due diligence requirements imposed by the binding provisions on financial embargoes – it may, as part of the administrative measures it is authorised to impose, prohibit the European payment or electronic money institution concerned from providing services in Belgium through one or more agents or distributors in Belgium designated by the Bank.

## 3.2 Functions of the CCP

Pursuant to Articles 4 and 5 of the RTS, **the functions to be performed by the CCP** appointed in Belgium are as follows:

1. **ensuring compliance with the AML/CFTP rules.** To that end, the CCP should:
  - facilitate the development and implementation of the policies, procedures and internal control measures referred to in Article 8 of the Anti-Money Laundering Law by keeping the European payment or electronic money institution that appointed it informed of the legal and regulatory AML/CFTP requirements applicable on Belgian territory;
  - monitor, on behalf of the European payment or electronic money institution that appointed it, the effective compliance by the agents and distributors through which the payment or electronic money institution offers services in Belgium (i) with the legal and regulatory AML/CFTP requirements applicable on Belgian territory and (ii) with the policies, procedures and internal control measures adopted by the said institution pursuant to Article 8 of the anti-Money Laundering Law;
  - inform the head office of the European payment or electronic money institution that appointed it of any potential violation or non-compliance found with the agents and distributors of this institution in Belgium, including any information that could affect the ability of these agents and distributors to comply with the policies, procedures and internal control measures, or that could influence the risk assessment of the institution in another manner;
  - ensure, on behalf of the European payment or electronic money institution that appointed it, that corrective measures are taken when the agents and distributors of this institution in Belgium do not comply or run the risk of not complying anymore with the legal and regulatory AML/CFTP requirements applicable on Belgian territory;
  - ensure, on behalf of the European payment or electronic money institution that appointed it, that the institution's agents and distributors in Belgium and their staff meet the training requirements referred to in Article 11 of the Anti-Money Laundering Law (see the "Training and educating staff" page); and
  - represent the European payment or electronic money institution that appointed it in its contacts with the competent Belgian AML/CFTP authorities, particularly with CTIF-CFI and FPS Finance (for notifications of asset freezing).
2. **facilitating the NBB's monitoring of compliance with AML/CFTP rules.** For this purpose, the CCP should, on behalf of the European payment or electronic money institution that appointed it:

- represent the said payment or electronic money institution in its contacts with the NBB;
- be able to access information held by the agents and distributors of the institution concerned that are situated in Belgium;
- answer any request from the NBB regarding the activities of this institution's agents and distributors situated in Belgium and provide the NBB with any relevant information held by that institution or by its agents and distributors situated in Belgium. Regular reporting may be required at the request of the NBB;
- facilitate the on-site inspections conducted by the NBB at premises of the agents and distributors of the payment or electronic money institution concerned that are situated in Belgium.

Aside from the aforementioned functions, the CCP appointed in Belgium should perform the following **additional functions** (see Article 27, § 2, of the Anti-Money Laundering Regulation of the NBB):

1. detect atypical transactions or, at the very least, ensure that the criteria used to detect atypical transactions are (i) in compliance with the provisions of the European Regulation on transfers of funds, of the Anti-Money Laundering Law and Regulation of the NBB, and (ii) adequate for the activities performed in Belgium by the European payment or electronic money institution concerned;
2. decide whether a reporting of suspicions is necessary pursuant to Article 47 of the Anti-Money Laundering Law and, where appropriate, decide on the content of such a reporting;
3. answer, in accordance with Article 48 of the Law, any request for information from CTIF-CFI on the activities performed by the agents or distributors of the European payment or electronic money institution concerned that are situated in Belgium.

### 3.3 Location, form and implementation arrangements

Regarding **the location** of the CCP, the Anti-Money Laundering Law provides that, whenever a CCP is required, it should be situated on Belgian territory (see Article 15 of the Law) and that, in such cases, the natural person appointed pursuant to Article 9, § 2, of the Law who is responsible for performing the functions of CCP, should also be established in Belgium (see Article 9, § 4, of the Anti-Money Laundering Law).

Conversely, neither the Belgian legal framework nor the European RTS lay down rules regarding **the form** to be taken by the CCP. However, this form should be adequate to enable the CCP to effectively perform all the functions listed above for the entire network of agents or distributors established in Belgium.

The NBB therefore considers it the responsibility of the European payment or electronic money institution to determine the form of its CCP, taking into account the principle of proportionality. As such, the NBB expects the institution, in particular, to be able to demonstrate to it (i) that the human and technical resources located in Belgium to enable the CCP to fully perform its functions for the entire network of agents or distributors established in Belgium, are adequate, particularly considering the extent of the network, the number and volume of the transactions carried out in Belgium, the level and characteristics of the ML/FT risks associated with the activities performed in Belgium, etc., and (ii) that the form of the CCP is appropriate for pooling and managing these resources adequately and consistently.

Taking into account the above, the CCP could thus take the form, for example, (i) of one or more staff members in Belgium who report hierarchically to the compliance department or the AMLCO of the European payment or electronic money institution, (ii) of one or more of the agents or distributors established in Belgium (or of the only agent or distributor established in Belgium) who perform(s) the functions falling under the responsibility of the CCP in addition to its/their operational functions when carrying out transactions or establishing business relationships with customers, or (iii) of an independent expert specifically charged with performing these functions by the institution through an agency agreement, etc.

In any case, the NBB expects the payment or electronic money institution to be able to demonstrate that the person responsible for performing the functions of the CCP in Belgium, as referred to in Article 9, § 4, of the Anti-Money Laundering Law, possesses the required qualities listed in Article 9, § 2, of the Law. As such, this person should possess:

- the professional reliability needed to perform his/her functions with integrity;
- the adequate expertise, knowledge of the Belgian legal and regulatory AML/CFTP framework, availability, hierarchical level and/or powers, both within the payment or electronic money institution and with regard to its agents or distributors established in Belgium, that are necessary to perform its functions effectively, independently and autonomously;

- the power to propose to the payment or electronic money institution, on his/her own initiative, all necessary or useful measures, including the implementation of the means required, to guarantee the compliance and efficiency of the internal AML/CFTP measures.

The conditions set out in 2° and 3° above are assessed on a case-by-case basis, taking into account the principle of proportionality and, therefore, the characteristics of the relevant network of agents or distributors established in Belgium and of the activities performed.

Moreover, for reasons of efficiency, it is acceptable to **outsource** the executive tasks falling under the responsibility of the CCP appointed in Belgium in full or in part to another entity belonging to the same group. These tasks include quality control of the performance of the agents or distributors, ongoing supervision aimed at detecting atypical transactions, analysis of these transactions in accordance with the internal procedures, particularly the collection of any additional information, and the development of an opinion based on this analysis regarding the (non-)suspect nature of the transaction under consideration. However, it should be noted that outsourcing cannot infringe on the responsibility of the CCP to fully perform its functions. For example, if the analysis of atypical transactions is outsourced to another entity of the group, the CCP should retain the power to decide, on the basis of this analysis, whether or not to submit a suspicious transaction report to CTIF-CFI. Likewise, when tasks related to the supervision of the activities of agents or distributors are outsourced to another entity of the group, the CCP should retain the right to decide on the actions to be taken with regard to agents for which shortcomings have been identified. Moreover, the CCP should ensure that the arrangements for performing the outsourced functions are adequate, and it should retain the ability to adapt them if necessary. Generally speaking, if the organisation of the CCP is outsourced in such a manner, the comments and recommendations formulated in point 3 of the "Governance" page should be taken into account. For more information on the outsourcing aspect, reference is also made to the "Performance of obligations by third parties" page.

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



# Performance of obligations by third parties

Home > Financial oversight > Combating money laundering and the financing of terrori...

## Legal and regulatory framework

- Anti-Money Laundering Law: Articles 42 to 44
- Anti-Money Laundering Regulation of the NBB: Articles 19 to 21

## Explanatory Memorandum of the Anti-Money Laundering Law

- Articles 42 to 44

## Other reference documents

- BCBS Guidelines dated June 2017 on Sound management of risks related to money laundering and financing of terrorism (see Annex 1)

## Comments and recommendations by the NBB

- Comments and recommendations

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



# Anti-Money Laundering Law of 18 September 2017 - Articles 42 to 44

## Art. 42

Without prejudice to the use of agents or subcontractors that act on their instructions and operate under their control and responsibility, obliged entities may rely on third party business introducers to fulfil the due diligence requirements laid down in Articles 26 to 32, 34 and 35, § 1, 2°. In that case, the ultimate responsibility for ensuring compliance with these obligations shall remain with the obliged entities concerned.

## Art. 43

§ 1. For the purposes of this Chapter, a “third party business introducer” shall be defined as:

1° an obliged entity as referred to in Article 5;

2° an obliged entity within the meaning of Article 2 of Directive 2015/849 that is governed by the law of another Member State;

3° an obliged entity within the meaning of Article 2 of Directive 2015/849 that is governed by the law of a third country and:

a) that must fulfil legal or regulatory customer due diligence requirements and record-keeping obligations that are consistent with those laid down in Directive 2015/849; and

b) whose compliance with these legal or regulatory obligations is monitored in accordance with the requirements laid down in Chapter VI, Section 2, of Directive 2015/849.

§ 2. Obligated entities may not rely on third party business introducers established in high-risk third countries.

By way of derogation from the first subparagraph, obliged entities may rely on their branches and majority-owned subsidiaries or on other entities of their group that are established in a high-risk third country, if the following conditions are met:

1° the obliged entity relies on information provided solely by a third party business introducer that is part of the same group;

2° the group applies AML/CFT policies and procedures, customer due diligence measures and rules on record-keeping in accordance with this Law, with Directive 2015/849 or with equivalent rules provided for by the law of a third country, and efficiently verifies whether the third party business introducer complies effectively with these policies and procedures, measures and rules;

3° the effective implementation of the obligations referred to in 2° is supervised at group level by the supervisory authority competent pursuant to Article 85 or by the supervisory authority of the Member State or third country where the parent company of the group is established.

## Art. 44

§ 1. Obligated entities that rely on a third party business introducer shall demand that the latter immediately submit the information on the identity of the customer and, where appropriate, of his agents and beneficial owners, as well as on the customer's characteristics and on the purpose and intended nature of the business relationship, that is necessary for the fulfilment of the due diligence requirements that have been conferred upon the third party business introducer in accordance with Article 42.

They shall also take appropriate measures in order to enable the third party business introducer to, immediately and at first request send them a copy of the supporting documents or of the reliable sources of information it used to verify the identity of the customer and, where appropriate, of his agents and beneficial owners.

Under the conditions set out in Articles 42 and 43, obliged entities may accept the results of due diligence requirements fulfilled by a third party business introducer situated in a Member State or in a third country, even if the data or supporting documents that were used as a basis for the identification or identity verification differ from the data required by this Law or its implementing measures.

§ 2. The obliged entities referred to in Article 5 that act as third party business introducers shall immediately provide the bodies or persons to which the customer has been introduced with the information concerning the identity of the customer and, where appropriate, of his agents and beneficial owners, concerning the customer's characteristics and the purpose and intended nature of the business relationship, that is necessary for fulfilling the due diligence requirements conferred upon them in accordance with Article 42.

They shall also, without delay and at first request, submit a copy of the supporting documents or of the reliable sources of information they used to verify the identity of the customer and, where appropriate, of his agents and beneficial owners.



# NBB anti-money laundering regulation of 21 November 2017 - Articles 19 to 21

## Art. 19

Obligated financial institutions which make use of agents or sub-contractors to enter into or maintain business relationships with customers or carry out occasional transactions on behalf of them shall set out in writing to these intermediaries the identification and verification procedures to be implemented, in compliance with the Law and this Regulation. They shall ensure that these procedures are respected.

## Art. 20

Obligated financial institutions shall state in writing to their agents and sub-contractors who are in direct contact with customers:

1° appropriate criteria enabling them to detect atypical transactions;

2° the procedure required for carrying out a specific analysis of these transactions under the responsibility of the AMLCO, in accordance with Article 45, § 1, of the Law, in order to determine whether these transactions may be suspected of being linked to money laundering or terrorist financing.

## Art. 21

The intervention of a third-party business introducer pursuant to Article 42 of the Law shall be subject to the condition that the internal procedures of the obliged financial institution stipulate:

1° that the obliged financial institution shall verify beforehand and keep the documents on which it has based its verification that the third-party business introducer meets, where appropriate, the conditions laid down in Article 43, § 1, 3°, and § 2, 2nd indent, of the Law;

2° that the third-party business introducer undertakes, in writing, beforehand to:

a) immediately provide the obliged financial institution with the information concerning the identity of the customers that will be introduced and, where appropriate, of their agents and beneficial owners, concerning the customer's characteristics and the purpose and intended nature of the business relationship, that is necessary for fulfilling the due diligence requirements conferred upon them in accordance with Article 42 of the Law;

b) provide the obliged financial institution, without delay and at first request, with a copy of the supporting documents or of the reliable sources of information he/she used to verify the identity of customers and, where appropriate, of their agents and beneficial owners.



# Explanatory Memorandum to the Anti-Money-Laundering Law of 18 September 2017 - Articles 42 to 44

## Art. 42

Draft Article 42 authorises obliged entities to rely on third party business introducers to fulfil the following general due diligence obligations:

- identification and identity verification obligations (Articles 26 to 32);
- the obligation to identify the customer's characteristics and the purpose and nature of the business relationship (Article 34);
- the obligation to update information (which constitutes the second aspect of the obligation of ongoing due diligence - cf. Article 35, § 1, 2°) even if not expressly provided for by the Directive.

As regards the observation by the Council of State according to which the obligation to update the aforementioned information may not be entrusted to third parties to the extent that it comes under ongoing due diligence, whilst Articles 25 of the Directive authorises Member States to allow obliged entities to rely on third parties as regards the fulfilment only of the due diligence obligations referred to in Article 13, § 1, first paragraph, a), b), and c) but not d) (this last point being dedicated to the ongoing due diligence obligation), it should be pointed out that a case of relying on third parties which is frequently identified is that of an obliged entity which has the capacity of a life insurer that relies on the services of an insurance intermediary; however, in this case, the intermediary generally intervenes when entering into the business relationship with the customer but also for the entire lifetime of the contract meaning that in practice, it is that person who effectively proceeds with updating the customer's information. It seems that in this case preventing the intermediary concerned from transmitting the updated customer information to the life insurer during the business relationship (a case not expressly authorised by the Directive) does not make any sense; the fact that Article 25 of the Directive does not refer to the obligation of ongoing due diligence referred to in Article 13, § 1, first paragraph, d) seems to come from a conceptual and unintentional error on the part of the EU law-makers, which must be corrected in the draft provision.

In accordance with Article 29 of the Directive, the provisions relating to relying on third party business introducers apply without prejudice to the possibility for obliged entities to rely on authorised agents or sub-contractors acting on their instructions and operating under their control and responsibility. By contrast, a person who executes the said obligations as regards customers of the obliged entity independently thereto, on the entity's instructions and under its control and responsibility without acting by virtue of a mandate or sub-contracting agreement should be considered a third party business introducer.

If an obliged entity relies on a third party business introducer, the ultimate responsibility for ensuring compliance with these obligations shall remain with the obliged entities concerned.

## Art. 43

Draft Article 43, which transposes Article 26 of the Directive, determines which persons obliged entities may call on as third party business introducers.

§ 1 specifies that, within the meaning of the draft Law, authorised third party business introducers are:

1° obliged entities as referred to in Article 5;

2° obliged entities within the meaning of Article 2 of Directive 2015/849 that are governed by the law of another Member State;

3° obliged entities within the meaning of Article 2 of Directive 2015/849 that are governed by the law of a third country and:

- that must fulfil legal or regulatory customer due diligence requirements and record-keeping obligations that are consistent with those laid down in Directive 2015/849; and
- whose compliance with these legal or regulatory obligations is monitored in accordance with the requirements laid down in Chapter VI, Section 2, of Directive 2015/849.

The notion of “third party business introducer” is therefore broadened compared to that of Article 10 of the Law of 11 January 1993 in terms of the fact that all obliged entities may from now on act as a third party business introducer and not only the entities listed in the Law. However, because the draft Law, taking into account the evolution of the European system, no longer provides for the establishment of a list of equivalent third countries by the King, it is up to each obliged entity that wishes to rely on a third party business introducer governed by the law of a third country to determine if the legal and regulatory provisions and the checks to which the third party is subject meet the conditions of equivalence described above.

§ 2 of this draft provision excludes obliged entities being able to rely on third party business introducers established in high-risk third countries.

As a reminder, a high-risk third country is defined in Article 4, 9° as a third country (i.e. outside the European Union):

- with AML/CFT regimes identified by the European Commission (in accordance with Article 9 of Directive 2015/849) as having strategic deficiencies that pose significant threats to the financial system of the European Union; or
- that presents a geographical risk identified as high by the FATF, the Ministerial Committee tasked with coordinating the fight against the laundering of money of illicit origin and the National Security Council or the obliged entity itself.

In accordance with that authorised under Article 26, the second paragraph of § 2 of Directive 2015/849, however, provides for an exemption to the exclusion referred to in the first paragraph. It authorises obliged entities to rely on their branches and majority-owned subsidiaries, or on other entities of their group even if they are established in a high-risk third country if the conditions listed are met. It should be noted that all the branches and subsidiaries, whether direct or indirect, are considered eligible if they are all covered by the group-wide policy.

Three conditions are provided for by the second paragraph of § 2:

1° firstly, the obliged entity must rely on information provided solely by a third party business introducer that is part of the same group; in other words, the third party business introducer must have obtained and verified the information himself/herself and may not have received it from another third party;

2° the group must apply AML/CFT policies and procedures, customer due diligence measures and rules on record-keeping in accordance with this Law (if the parent company is Belgian), or with the law of a Member State in accordance with Directive 2015/849 (if the parent company is governed by the law of another Member State) or with equivalent rules provided for by the law of a third country (if the parent company is governed by the law of a third country), and must efficiently verify whether the third party business introducer complies effectively with these policies and procedures, measures and rules;

3° the effective implementation of the obligations referred to in 2° must be supervised at group level by the supervisory authority competent pursuant to Article 85 or by the supervisory authority of the Member State or third country where the parent company of the group is established.

## Art. 44

Article 44, § 1 transposes Article 27 of the Directive and takes over Article 10, § 1, second paragraph of the Law of 11 January 1993. It provides that obliged entities that rely on a third party business introducer must demand that the latter immediately submit the information on the identity of the customer and, where appropriate, of his/her agents and beneficial owners, as well as on the customer's characteristics and on the purpose and intended nature of the business relationship, that arise from the duty of due diligence executed by the third party business introducer in accordance with Article 42.

The obliged entities that rely on a third party business introducer must also take appropriate measures in order to enable the third party business introducer to, immediately and at first request send them a copy of the supporting documents or of the reliable sources of information it used to verify the identity of the customer and, where appropriate, of his/her agents and beneficial owners.

The obliged entities may accept the results of due diligence requirements fulfilled by a third party business introducer situated in a country in the EEA or in a third country, even if the data or supporting documents that were used as a basis for the identification or identity verification differ from the data required by this Law or its implementing measures.

Conversely, draft Article 44, § 2 requires subjected entities that act as third party business introducers to immediately transmit the information concerned and provide on request, without delay, copies of the supporting documents used.

# Performance of obligations by third parties: Comments and recommendations by the NBB

Home > Financial oversight > Combating money laundering and the financing of terrori...

## Contents

- 1. Outsourcing of tasks of the AMLCO function
- 2. Performance of due diligence obligations by third parties

## 1. Outsourcing of tasks of the AMLCO function

Insofar as the financial institution remains fully responsible for the AMLCO function, it could be permitted, pursuant to the principle of proportionality and/or for reasons of efficiency, to outsource the executive tasks of the AMLCO function that are assigned to it by the Anti-Money Laundering Law and the Anti-Money Laundering Regulation of the NBB, in full or in part to a third party or to another entity belonging to the same group.

### 1.1. General principles

As a reminder, a financial institution outsources (or subcontracts) a function when it concludes an agreement in any form with a service provider, on the basis of which the latter carries out a process or task that otherwise would be carried out by the financial institution itself. Outsourcing differs from consulting in that a consultant only provides an opinion to his client financial institution without carrying out the process or task concerned himself.

The use of outsourcing by a financial institution to fulfil its legal and regulatory AML/CFTP obligations should in no way lessen the responsibility of the institution concerned to have an appropriate and efficient organisation and to fulfil its legal and regulatory obligations in this regard, nor transfer this responsibility to the service provider.

Consequently, given the nature of the function of senior officer responsible for AML/CFTP of a financial institution governed by Belgian law or of a branch established in Belgium, as referred to in Article 9, § 1, of the Anti-Money Laundering Law, the NBB considers that neither this function nor the tasks of this function should be outsourced to either a third party or to another entity belonging to the same group, where applicable. Indeed, all financial institutions governed by Belgian law and all branches established in Belgium should appoint an internal “senior officer responsible for AML/CFTP” or, pursuant to the principle of proportionality, a “senior officer acting as AMLCO” (see point 5 of the page “Governance”).

In this regard, the NBB stresses in particular that the power to take strategic decisions in relation to AML/CFTP should not be outsourced and should be exercised, depending on the nature of the decision and without prejudice to the application of the group policy (see “Organisation and internal control in groups”), by the management committee or senior management of the financial institution, its senior officer responsible for AML/CFTP, its head of the Compliance function (as hierarchical head of the AMLCO, when the latter is an “N-2” member of the Compliance function), its AMLCO or, as the case may be, its senior officer acting as AMLCO (where, for reasons of proportionality, use is made of the possibility to combine functions as provided for in Article 9, § 3, of the Anti-Money Laundering Law).

This relates in particular to decisions concerning:

- the validation of the overall risk assessment,
- the internal AML/CFTP organisation,

- the AML/CFTP policy of the financial institution,
- the adoption of internal AML/CFTP procedures,
- the individual risk assessment, the entry into the business relationship and the assignment of the risk profile,
- the establishment of criteria to detect atypical transactions,
- the reporting of suspicious transactions to CTIF-CFI,
- the notifications of assets freezes to the FPS Finance,
- etc.

Conversely, insofar as the financial institution remains fully responsible for the AMLCO function as mentioned above, it could be permitted, pursuant to the principle of proportionality and/or for reasons of efficiency, to outsource the executive tasks of the AMLCO function that are assigned to it by the Anti-Money Laundering Law and the Anti-Money Laundering Regulation of the NBB, under the conditions described below, in full or in part to a third party or to another entity belonging to the same group. This can include ongoing supervision aimed at detecting atypical transactions, analysis of these transactions in accordance with the internal procedures, the collection of any additional information and the development of an opinion based on this analysis regarding the (non-)suspicious nature of the transaction under consideration.

For small financial institutions or institutions with an inherently low exposure to ML/FT risk, outsourcing could be justified in particular by the application of the principle of proportionality (see point 5 of the page "Governance"). Outsourcing may also be justified, for financial institutions belonging to a group, on the grounds of optimisation of the management of the resources needed to perform this function in the various entities of the group (e.g. centralisation of certain IT tools in the parent company).

However, the NBB draws attention to the fact that outsourcing within a group, by a subsidiary to its registered office or to another subsidiary of the group to which it belongs (intragroup outsourcing), is subject to the same requirements as outsourcing to an external service provider. Financial institutions making use of intragroup outsourcing should in particular take the measures necessary to identify and manage any conflicts of interest that could arise from such an outsourcing agreement.

Similarly, given the territorial scope of the AML/CFTP legislation and regulations (for more information on the scope, see the page "Scope"), the transfer of tasks of the AMLCO function by a branch of a financial institution governed by the law of another EEA country or of a third country to its registered office or to another branch of the legal entity to which it belongs, should be considered outsourcing and therefore meet the prudential requirements in this regard.

Consequently, in the aforementioned cases of outsourcing and when the financial institution is a credit institution, investment firm, payment institution or electronic money institution, the Guidelines of the European Banking Authority of 25 February 2019 and Circular NBB\_2019\_19 of 19 July 2019 on outsourcing apply.

The NBB considers that the same principles also apply to the outsourcing of tasks of the AMLCO by life insurance companies.

As regards payment institutions and electronic money institutions that carry out activities in Belgium through agents or distributors established there, all principles and recommendations included in this Chapter apply *mutatis mutandis* to the outsourcing of tasks of the "central contact point" (see the page "Belgian central contact points of European payment institutions and electronic money institutions").

The NBB also points out that, since the tasks of the AMLCO fall under the internal control functions of the financial institutions, these tasks should be considered "critical or important functions" within the meaning of paragraph 24(b) of the aforementioned Guidelines of the European Banking Authority, unless the financial institution has been able to demonstrate beforehand that a failure in the performance of the outsourced tasks will not impair the efficiency of the internal control performed by the AMLCO.

Attention is also drawn to the fact that, with regard to critical or important functions (see above), the outsourcing of tasks related to AML/CFTP to service providers established in third countries should be subject to additional safeguard measures in order to ensure that the outsourcing does not, as a result of the location of the service provider, disproportionately increase the risk of non-compliance with the legal and regulatory requirements or of inefficient performance of the outsourced tasks, nor hinders the supervisory authority's capacity to effectively exercise its supervisory power with regard to the service provider.

The NBB also stresses that the use of outsourcing should not be so extensive as to lead to the creation of “empty shells” in terms of AML/CFTP. As a result, any financial institution outsourcing tasks of the AMLCO should take care to internally maintain, in addition to the decision-making power (see above), the effective power to manage outsourced tasks. This implies that the outsourcing financial institution should itself implement appropriate measures to monitor the outsourced tasks and remedy any shortcomings and deficiencies found. For this purpose, each outsourcing financial institution should in particular be able to demonstrate that it has sufficient internal resources to effectively exercise its decision-making power, its monitoring of the outsourced tasks and, where appropriate, its remediation obligation.

These principles also apply in case of outsourcing of due diligence obligations. For the performance of due diligence obligations, please refer to the section “Performance of due diligence obligations by third parties” below.

## 1.2. Practical arrangements for the implementation of the outsourcing process

The outsourcing of tasks of the AMLCO function to a service provider requires the following conditions to be met:

1. The decision to outsource should be preceded by a documented analysis to identify the risks that would be associated with this outsourcing, including the risks related to the use of new technologies in this context, in order to define the measures to be implemented to manage and reduce these risks.
2. The decision to outsource should be duly justified in the light of the objectives pursued, clearly indicating whether it is taken pursuant to the principle of proportionality and/or whether it aims to ensure an optimal allocation of AML/CFTP resources throughout the group to which the financial institution concerned belongs.
3. The financial institution which outsources tasks of the AMLCO function entrusts its AMLCO or, where appropriate, its senior officer acting as AMLCO with:
  - monitoring the service provider's performance to ensure that the outsourcing effectively enables the financial institution to comply with all its legal and regulatory AML/CFTP obligations, and
  - reporting on the outsourcing to the management committee (or, where applicable, to the senior management) and to the board of directors as part of the AMLCO's annual report or whenever circumstances require, in particular so that any necessary remediation measures are implemented as soon as possible.

When the financial institution makes use of the possibility to combine the function of senior officer with the AMLCO function, in accordance with Article 9, § 3, of the Anti-Money Laundering Law, the NBB recommends that this senior officer acting as AMLCO be assisted in carrying out these specific tasks by a contact person who is a staff member of the financial institution and who has the knowledge and expertise required for this purpose. Where such a contact person has not been designated, the financial institution must be able to demonstrate that its senior officer acting as AMLCO is effectively able to perform these specific tasks alone.
4. The financial institutions referred to in the aforementioned Guidelines of the European Banking Authority of 25 February 2019 on outsourcing arrangements are required to enter the outsourcing agreements relating to tasks of the AMLCO function in the registry of outsourcing arrangements, and keep these entries up-to-date, within the time frame and according to the rules set out in those Guidelines. The institution should be able to submit the whole or specific sections of this registry to the NBB at its first request, in accordance with Article 91 of the Anti-Money Laundering Law.
5. The financial institution should ensure that a proper framework is established for outsourcing, in accordance with the prudential rules in force in this area (for credit institutions and stockbroking firms: the aforementioned Guidelines of the European Banking Authority of 25 February 2019 on outsourcing arrangements and Circular NBB\_2019\_19; for insurance companies: Circular NBB\_2016\_31; for payment institutions and electronic money institutions: the aforementioned Guidelines of the European Banking Authority of 25 February 2019 on outsourcing arrangements and Circular NBB\_2019\_19; for settlement institutions: Circular PPB\_2007\_5). This implies in particular that:
  - the outsourcing complies with the financial institution's outsourcing policy;
  - the decision to outsource is subject to a prior analysis in accordance with the aforementioned Guidelines of the European Banking Authority;
  - the financial institution verifies, prior to the conclusion of the outsourcing agreement, the proposed subcontractor's professional integrity, AML/CFTP expertise, knowledge of the Belgian legal and regulatory framework and effective availability, throughout the duration of the outsourcing agreement, for performing the tasks of the AMLCO that will be outsourced to him; the required availability of the

- subcontractor should be determined on the basis of a reasonable assessment, using objective and relevant criteria, of the working time which will be required for the complete and timely performance of the outsourced tasks with a high quality standard;
- the outsourcing arrangements, including a precise list of the tasks assigned to the subcontractor and the procedures to be followed by the subcontractor in carrying out those tasks, and the arrangements for the regular monitoring by the financial institution of the completeness, timeliness and quality of the services provided by the subcontractor, are laid down in writing (the service level agreement);
  - the service level agreement explicitly states whether or not the subcontractor is authorised to make use of sub-outsourcing and, if so, it specifies the precise arrangements thereof;
  - the financial institution ensures that the outsourcing agreement contains the necessary explicit provisions to prevent this agreement from obstructing the control tasks of the financial institution's internal audit, compliance and AMLCO functions, or the NBB's exercise of its AML/CFTP off-site control and on-site inspection powers, in accordance with the Anti-Money Laundering Law.
6. The financial institution allocates adequate and sufficient resources to monitor, under the responsibility of the AMLCO or, as the case may be, of the senior officer acting as AMLCO, the subcontractor's performance, particularly in terms of completeness, timeliness and quality of the tasks performed.
  7. The financial institution is able to promptly take adequate and effective remediation measures in the event of subcontractor shortcomings and, where applicable, to terminate the outsourcing agreement without delay in the event of serious failings on the part of the subcontractor, without such termination jeopardising the continuity of the relevant tasks of the AMLCO function.

A financial institution intending to outsource tasks of the AMLCO function should notify the NBB.

Any financial institution outsourcing or intending to outsource such tasks should also compile a dossier to demonstrate that it has taken the measures required to comply with all the conditions listed above. This dossier should be available for submission to the NBB at its first request.

## 2. Performance of due diligence obligations by third parties

In addition to the cases in which financial institutions outsource tasks of the AMLCO function (see the section on the outsourcing of tasks of the AMLCO function), they may also rely on third parties to fulfil their legal and regulatory due diligence obligations with regard to AML/CFTP.

This refers to the use of third parties to fulfil the obligations to identify and verify the identity of customers, their agents and their beneficial owners, as well as the obligations to identify the customer's characteristics and the purpose and nature of the business relationship or occasional transaction. For agents or subcontractors, this outsourcing can also include the ongoing due diligence obligation and the obligation to detect atypical facts and transactions (see below)

In this regard, a distinction can be made between two types of situations in which different rules apply:

- the use of an agent or subcontractor: in such cases, the agent or subcontractor fulfils the due diligence obligations in the name of and on behalf of the financial institution, in accordance with the financial institution's procedures and instructions; and
- the use of a "third-party business introducer": in such cases, the third-party business introducer is himself subject to the due diligence obligations imposed by the Anti-Money Laundering Law and fulfils them according to his own procedures.

### 2.1. Use of an agent or subcontractor

Where a financial institution uses an agent or a subcontractor for the purposes listed above, this person participates in the fulfilment, in the name of and on behalf of the financial institution, of the due diligence obligations imposed on it by the Anti-Money Laundering Law.

The financial institution should therefore set out in writing the procedures to be implemented and ensure that they are adequately monitored. In this respect, Article 19 of the Anti-Money Laundering Regulation of the NBB stipulates that financial institutions which make use of agents or subcontractors to enter into or maintain business relationships

with customers or carry out occasional transactions on behalf of them should set out in writing to these intermediaries the procedures to be implemented for identifying and verifying the identity of the persons involved, in compliance with the Law and the Regulation, and that they should ensure that these procedures are complied with.

Furthermore, Article 20 of the Anti-Money Laundering Regulation of the NBB specifies that, if the agents or subcontractors are in direct contact with customers, these procedures should cover:

- appropriate criteria enabling them to detect atypical transactions; and
- the procedure to be followed to subject these transactions to a specific analysis under the responsibility of the AMLCO in order to determine whether these transactions can be suspected of being linked to ML/FT.

The agents and subcontractors operate under the supervision and responsibility of the financial institution.

In this regard, please refer to the section on the outsourcing of tasks of the AMLCO function (see the section on the outsourcing of tasks of the AMLCO function) of this AML site, which specifies the actual principles and arrangements to be complied with by the outsourcing. In line with these principles and arrangements, it should be noted in particular that, when a financial institution outsources tasks in relation to the due diligence obligations imposed on it by the Anti-Money Laundering Law:

1. this outsourcing should not lessen the responsibility of the institution concerned to fully meet its legal and regulatory obligations, nor transfer this responsibility to the agent or subcontractor;
2. the outsourcing should not pertain to the power to make AML/CFTP strategic decisions, particularly the adoption of AML/CFTP procedures to be complied with by the agent or subcontractor, the decision to enter into a business relationship or assign a risk profile to a customer, the decision to report suspicious transactions to CTIF-CFI or to notify the FPS Finance of assets freezes, etc.;
3. the financial institution is required to implement appropriate measures to monitor the tasks performed by the agent or subcontractor, in order to detect any shortcomings or deficiencies therein, and should be able to promptly take adequate and effective remediation measures in the event of agent or subcontractor shortcomings and, where applicable, to terminate the agency or outsourcing agreement without delay in the event of serious failings, without such termination jeopardising the continuity of the tasks assigned to the agent or subcontractor;
4. etc.

## 2.2. Use of a third-party business introducer

Using a third-party business introducer differs from using an agent or a subcontractor in that the third-party business introducer does not primarily act in the name of and on behalf of the institution on the basis of a mandate received from the latter. As the third-party business introducer is himself subject to identical or equivalent due diligence obligations, in accordance with the Anti-Money Laundering Law or with a comparable law of another country, he primarily performs his customer due diligence obligations according to his own procedures, independently of the financial institution. He then submits the result of his own due diligence obligations to the financial institution to which he introduces his customer, enabling that financial institution to take this result into consideration for the fulfilment of its own due diligence obligations and avoiding, to the extent possible, the same due diligence obligations being fulfilled twice.

For instance, when a customer applies for a mortgage loan with a credit institution which requires a life insurance contract to be concluded and used as collateral, the insurance company may make use of the identification and identity verification performed by the credit institution for its own purposes, to fulfil its own obligations to identify and verify the identity of its customer and, where appropriate, of his agents and beneficial owners. In this context, the credit institution acts as a “third-party business introducer” for the insurance company.

Another common example of the use of a third-party business introducer is when a life insurance company uses the result of the due diligence obligations fulfilled by an insurance intermediary in accordance with its own relevant legal and regulatory obligations.

### 2.2.1. Due diligence obligations for which a third-party business introducer may be used

Pursuant to Article 42 of the Anti-Money Laundering Law, obliged entities may rely on third-party business introducers to fulfil the following general due diligence obligations:

- the identification and identity verification obligations (Articles 26 to 32);
- the obligation to identify the customer's characteristics and the purpose and nature of the business relationship (Article 34);
- the obligation to update the information (which constitutes the second part of the ongoing due diligence obligation – see Article 35, § 1, 2°)

These also include the obligations relating to the collection and verification of the information necessary to fulfil the due diligence obligation with regard to occasional transactions and transactions carried out during the business relationship. However, this ongoing transaction due diligence obligation may not be fulfilled by third-party business introducers.

### **2.2.2. Authorised third-party business introducers**

In accordance with Article 43 of the Anti-Money Laundering Law, the following third-party business introducers may be used:

1° the obliged entities referred to in Article 5;

2° the obliged entities within the meaning of Article 2 of Directive 2015/849 that are governed by the law of another Member State;

3° the obliged entities within the meaning of Article 2 of Directive 2015/849 that are governed by the law of a third country and that:

- are subject to legal or regulatory customer due diligence obligations and record-keeping requirements that are consistent with those laid down in Directive 2015/849; and
- have their compliance with these legal or regulatory obligations supervised in a manner consistent with the requirements set out in Chapter VI, Section 2 of Directive 2015/849.

The notion of “third-party business introducer” has thus been expanded compared to its description in Article 10 of the Law of 11 January 1993, as any obliged entity can now act as third-party business introducer, and no longer only the entities listed in the law. Given that, due to the developments in European legislation, the Anti-Money Laundering Law no longer stipulates that the King should draw up a list of “equivalent third countries”, each obliged entity wishing to use a third-party business introducer governed by the law of a third country should verify whether the legal and regulatory provisions and the supervision imposed on the third party meet the equivalence conditions described above.

In contrast, § 2 of Article 43 of the Anti-Money Laundering Law prohibits obliged entities from using third-party business introducers established in high-risk third countries. However, the second paragraph of this § 2 provides for an exception to this prohibition. Obligated entities may rely on their own branches and majority-owned subsidiaries or on those of other entities in their group, even if they are established in a high-risk third country, if the three conditions listed in the second paragraph of § 2 of Article 43 of the Anti-Money Laundering Law have been met. It should be noted that all - direct or indirect - branches and subsidiaries are considered eligible, provided they are covered by the group policy.

### **2.2.3. Concrete rules for using a third-party business introducer**

In accordance with Article 44, § 1, of the Anti-Money Laundering Law, financial institutions that rely on a third-party business introducer should demand that the latter immediately provide it with the information on the identity of the customer and, where appropriate, of his agents and beneficial owners, as well as on the customer's characteristics and on the purpose and intended nature of the business relationship, which results from the due diligence requirements performed by the third-party business introducer in accordance with Article 42 of the Law or with the equivalent provisions of the foreign legislation to which he is subject.

Obligated entities using a third-party business introducer should also take appropriate measures to enable the third-party business introducer to, immediately and at first request, send them a copy of the supporting documents or of the reliable sources of information he used to verify the identity of the customer and, where appropriate, of his agents and beneficial owners.

Conversely, Article 44, § 2, of the Anti-Money Laundering Law stipulates that financial institutions acting as third-party business introducers should immediately provide the relevant information and, without delay and at first request, the copies of the supporting documents used. For example, where an insurance broker acts as an intermediary for a customer taking out life insurance, he should immediately provide the customer's identification data and, without delay and at first request, the copies of the supporting documents used.

Obligated entities may accept the results of the due diligence obligations performed by a third-party business introducer situated in an EEA country or in a third country, even when the data or supporting documents used for the identification or identity verification differ from those required by the Belgian law or its implementing measures.

Furthermore, Article 21 of the Anti-Money Laundering Regulation of the NBB provides that the intervention of a third-party business introducer in accordance with Article 42 of the Anti-Money Laundering Law is subject to the condition that the internal procedures of the financial institution stipulate:

1° that the financial institution verifies beforehand and keeps the documents on which it has based its verification that the third-party business introducer meets, where appropriate, the conditions laid down in Article 43, § 1, 3°, and § 2, second paragraph, of the Money Laundering Law;

2° that the third-party business introducer undertakes, in writing, beforehand to:

- a) immediately provide the financial institution with the information concerning the identity of the customers that will be introduced and, where appropriate, of their agents and beneficial owners, concerning the customer's characteristics and the purpose and intended nature of the business relationship, that is necessary for fulfilling the due diligence requirements conferred upon them in accordance with Article 42 of the Anti-Money Laundering Law;
- b) provide the financial institution, without delay and at first request, with a copy of the supporting documents or of the reliable sources of information he used to verify the identity of customers and, where appropriate, of their agents and beneficial owners.

It should be stressed, however, that when a financial institution uses a third-party business introducer, the former's responsibility is not shifted to the latter. As a result, financial institutions using third-party business introducers should implement appropriate internal control measures enabling them to ensure that the identification data collected by third-party business introducers and the verifications performed by them with regard to this data are adequate and sufficient to enable this financial institution to comply fully with its relevant legal and regulatory obligations. Should this not be the case, the financial institution should supplement the due diligence obligations or even perform them again.

In this respect, it should be noted in particular that the third-party business introducer, on the one hand, and the financial institution to which the customer is introduced, on the other, may assign different risk profiles to that same customer when justified. Where the customer has been assigned a lower risk profile by the third-party business introducer than by the financial institution, the latter should ensure that the due diligence obligations performed by the third-party business introducer are nevertheless sufficient to fulfil its own obligations.

For example, if the third-party business introducer was able to relax his due diligence obligations because he deemed the risk level low, the financial institution could be required to supplement the due diligence obligations or even perform them again if it did not itself assign a low risk profile to this customer or if its internal procedures do not allow the due diligence obligations to be relaxed. The same applies when the financial institution, as opposed to the third-party business introducer, assigns a high risk profile to the customer, in which case it is legally obliged to perform the enhanced due diligence obligations that have not been performed by the third-party business introducer.

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



# Brexit

Home > Financial oversight > Combating money laundering and the financing of terrori...

## Reference documents

- EBA Opinion dated 12 October 2017 on Brexit issues
- EIOPA Opinion dated 11 July 2017 on supervisory convergence in light of the Brexit

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



# Customer and transaction due diligence

Home > Financial oversight > Combating money laundering and the financing of terrori...

## Explanatory Memorandum to the Anti-Money-Laundering Law of 18 September 2017

- Steps of the procedure to be followed to meet general due diligence requirements

### Individual risk assessment

### Anonymous or numbered accounts and contracts

### Identification and identity verification

Persons to be identified

Object of the identification and identity verification

Time of identification and identity verification

Non-compliance with the identification and identity verification obligation

### Identification of the customer's characteristics and of the purpose and nature of the business relationship or the occasional transaction

### Ongoing due diligence and detection of atypical facts and transactions

### Special cases of enhanced due diligence

Identity verification over the course of the business relationship: Comments and recommendations by the NBB

High-risk third countries

States with low or no taxes

Correspondent relationships

Politically exposed persons (PEPs)

### Due diligence requirements and compliance with other legislation

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



# Individual risk assessment

[Home](#) > [Financial oversight](#) > [Combating money laundering and the financing of terrori...](#)

## Legal and regulatory framework

- [Anti-Money Laundering Law: Article 19](#)

## Explanatory Memorandum of the Anti-Money Laundering Law

- [Article 19](#)

## Risk factors to be taken into account

- [ESAs Risk Factor Guidelines dated 4 January 2018](#)

## Comments and recommendations by the NBB

- [Comments and recommendations](#)

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



# Individual risk assessment: Comments and recommendations by the NBB

Home > Financial oversight > Combating money laundering and the financing of terrori...

## Contents

- 1. Background
- 2. Process
- 3. Documentation and updates
- 4. Internal control measures

## 1. Background

The requirement to adopt a risk-based approach for the prevention of ML/FT, the basis of which is laid down in Article 7 of the Anti-Money Laundering Law, is one of the key elements in the FATF Recommendations as revised in 2012 and in Directive 2015/849. At the Belgian level, this requirement has inter alia resulted, with regard to the preventive measures to be implemented by obliged entities, in the obligation to perform a dual risk assessment, namely:

- *an overall assessment of the risks to which they are exposed ("business-wide risk assessment"), in accordance with the provisions of Articles 16 and 17 of the Anti-Money Laundering Law on the one hand, and of Title 2 of the Anti-Money Laundering Regulation of the NBB on the other hand (see the page "Risk-based approach and overall risk assessment"); and*
- *an assessment of the risks associated with each business relationship or occasional transaction (see below).*

In accordance with Article 19 of the Anti-Money Laundering Law, any decision to enter into a business relationship or to carry out the proposed transaction, or on the nature and intensity of the due diligence measures referred to in the said Article (see point 2.3 below) and applied by an obliged entity should, from now on, be based on an assessment of the ML/FT risks associated with each business relationship or occasional transaction. This so-called "individual risk assessment" is a central component of the new Anti-Money Laundering Law and constitutes an instrument that, in conjunction with the overall risk assessment, should enable financial institutions to identify, adequately manage or, where appropriate, limit the ML/FT risks to which they are exposed, and to optimise the allocation of their resources.

A risk-based approach therefore implies gaining in-depth and up-to-date knowledge and an understanding of the ML/FT risks to which the institution is objectively exposed, taking into account its activities and the manner in which they are performed (type of customers, geographical area...), and of the ML/FT risks associated with each business relationship, taking into account the different transactions carried out by the customer concerned in the context of this relationship, or with each occasional transaction.

## 2. Process

### 2.1. Individual risk assessment

The individual ML/FT risk assessment requires these risks to first be identified and then assessed.

In accordance with Article 19, § 2, of the Anti-Money Laundering Law, when identifying the ML/FT risks linked to a business relationship or occasional transaction, financial institutions should at least take into account:

- *the overall risk assessment*, performed beforehand in accordance with Article 16 of the Anti-Money Laundering Law and *all elements taken into account in the context of this overall assessment*. This includes, in particular:
  - the variables set out in Annex I of this Law,
  - the factors indicative of a potentially higher risk, as referred to in Annex III of the same Law, and possibly those indicative of a potentially lower risk, as referred to in Annex II,
  - but also the relevant conclusions of the report drawn up by the European Commission and the national risk assessment, ESA risk factor guidelines, etc. (see the reference documents mentioned on the page “Risk-based approach and overall risk assessment”);
- *the characteristics of the customer and of the business relationship or occasional transaction concerned*. The financial institution should take account of all information collected while fulfilling its due diligence obligations, such as information on:
  - the identity of the customer, his agents and his beneficial owners,
  - the customer’s characteristics and the purpose and nature of the business relationship or the occasional transaction,
  - and all other information collected as part of its ongoing due diligence.

As soon as they have an overall view of the ML/FT risk factors they have identified, financial institutions can determine the ML/FT risk level associated with the intended business relationship or occasional transaction. This could be done by assigning a score to each of the risk factors identified and combining these scores to determine the level of ML/FT risk. As highlighted in the ESAs Risk Factor Guidelines of 4 January 2018 (p. 16, paragraphs 36 and 37), when obliged entities weight risk factors in this way, they “*should make an informed judgement about the relevance of different risk factors in the context of a business relationship or occasional transaction. (...) for example, firms may decide that a customer’s personal links to a jurisdiction associated with higher ML/TF risk is less relevant in light of the features of the product they seek*”. Moreover, they also stress that “*the weight given to each of these factors is likely to vary from product to product and customer to customer (or category of customer) and from one firm to another. When weighting risk factors, firms should ensure that:*

- *weighting is not unduly influenced by just one factor;*
- *economic or profit considerations do not influence the risk rating;*
- *weighting does not lead to a situation where it is impossible for any business relationship to be classified as high risk;*
- *the provisions of Directive (EU) 2015/849 or national legislation regarding situations that always present a high money laundering risk cannot be over-ruled by the firm’s weighting; and*
- *they are able to over-ride any automatically generated risk scores where necessary. The rationale for the decision to over-ride such scores should be documented appropriately”.*

As regards the penultimate point mentioned above, it should indeed be stressed that, in accordance with Directive 2015/849, Articles 37 to 41 of the Anti-Money Laundering Law identify situations in which risks must always be considered high and which require the specific enhanced due diligence measures provided for therein to be implemented (see the pages dedicated to “Special cases of enhanced due diligence”). However, these special cases of enhanced due diligence still require an individual risk assessment taking account of all risk factors associated with the business relationship or occasional transaction, in particular to determine the appropriate intensity of the enhanced due diligence measures to be implemented to adequately manage and reduce these risks.

## 2.2. Classification of risks in risk categories

In line with the individual risk assessment, financial institutions should classify the business relationship or occasional transaction concerned in one (or more) risk categories specified following the overall risk assessment (see the page “Risk classification”), depending on the ML/FT risk level identified. Each business relationship or occasional transaction should thus be assigned a risk profile (high, standard or possibly low). The risk classification method established by the financial institution in its internal procedures should enable it to determine the appropriate

scope of the ongoing due diligence measures to be implemented in order to take account, where appropriate, of the different levels and nature of the ML/FT risks associated with the various products and services provided to the customer.

In this respect, it should be noted that financial institutions must ensure that they are able to modify the initial classification of a business relationship or transaction decided on by applying the internal procedures on the basis of the information initially collected at the start of the relationship, and that they can reclassify this business relationship or transaction in another risk category when they collect additional information in the context of the individual risk assessment that leads them to identify higher risks or risks of a different nature or, where appropriate, lower risks. While the initial classification should first and foremost reflect the risks inherent to the activities performed as identified in a generic manner in the context of the overall risk assessment, it should be possible for the specific analysis of the risk level presented by each business relationship or occasional transaction, taking into account all its characteristics and all specific information obtained in the context of the individual risk assessment, to lead to the reclassification of this business relationship or transaction from its initial risk category to another one that is more suitable for effectively reducing and managing specific and material ML/FT risks associated with this business relationship or transaction rather than generic and theoretical risks.

### 2.3. Implementation of appropriate due diligence measures

Following the individual risk assessment, financial institutions should define appropriate due diligence measures for adequately managing or mitigating risks.

By assigning a risk profile to a business relationship or occasional transaction and classifying it in one or more risk categories, the financial institution should be able to determine the level of due diligence (standard, enhanced, simplified) to be applied to the transactions carried out in the given situation, in accordance with the organisational framework defined by it (see the page "Policies, procedures, processes and internal control measures") and, in particular, with its customer acceptance policy.

The due diligence obligations thus subject to the risk-based approach are mentioned in Article 19, § 1, and specified in Title 3 of the Law. While, under the previous Law of 11 January 1993, these obligations could often wrongly be assumed to be limited to identifying and knowing the customer (so-called "KYC" measures), the legal framework now makes clear that they comprise three separate components, each with its own regulations:

- the identification and identity verification obligations (detailed on the pages dedicated to this topic);
- the obligations to identify the customer's characteristics and the purpose and nature of the business relationship or occasional transaction (detailed on the page dedicated to this topic);
- the ongoing due diligence obligations (detailed on the page dedicated to this topic).

## 3. Documentation and updates

Article 19, § 2, paragraph 3, of the Anti-Money Laundering Law stipulates that financial institutions should, in all cases (i.e. regardless of the risk level presented by a business relationship or occasional transaction), be able to demonstrate to the NBB that the due diligence measures applied by them are appropriate in light of the ML/FT risks they have identified.

Additionally, it should be noted that the individual risk assessment which financial institutions are required to perform with regard to each business relationship or occasional transaction under Article 19, § 2, of the Anti-Money Laundering Law, is not a one-off exercise but a continuous process. This risk assessment - where appropriate like the overall risk assessment - should be updated whenever one or more events occur that could have a significant impact on the risks associated with the given situation.

It is therefore advisable for each financial institution to describe the following in their internal procedures, which should be made available to the NBB:

- the **methodology** followed to perform the individual assessment of the risks associated with the business relationship or occasional transaction concerned.

In this regard, the internal procedure should describe the arrangements for the analysis of all information collected on the customer and the intended business relationship or occasional transaction in order to determine for each specific case which risk class defined following the overall risk analysis is appropriate (see point 3.2 below) to ensure that the most relevant due diligence measures are applied to the business relationship or the occasional transaction, taking into account its characteristics or special features (see point 3.3 below);

- the process for monitoring and timely **updating** the individual risk assessment process in order to ensure its permanent accuracy, including as regards existing customers.  
This process should specify the measures to be implemented to identify events that could influence the individual assessment of the risks linked to each business relationship over the course of that relationship, so as to take note of them and, subsequently, start the process for updating this assessment.

To ensure that the individual risk assessments are still relevant, it could also be useful for the internal procedure, where appropriate in light of the activities performed, to provide for a periodic review of these assessments and of the information available on which they are based. The frequency of these reviews can differ according to the risk profile assigned to the business relationship concerned.

It is for each financial institution to determine these different frequencies based on its own experience, with a view to adequately managing ML/FT risks. However, by way of indication, when the business relationship requires continuously or regularly carrying out a large number of transactions with characteristics that could change significantly over time, the NBB considers that these periodic reviews should reasonably occur at least annually in case of high risks or even more frequently in case of particularly high risks (for example in case of reportings to CTIF-CFI), at least every three years for business relationships presenting a standard risk profile and at least every five years for business relationships presenting a low risk profile. However, it should be stressed that the frequencies that can be determined in the procedures constitute complementary precautionary measures that may not be invoked under any circumstances to justify not updating the individual assessment of the risks linked to a business relationship when events occur that could significantly influence this assessment.

In the case of life insurance contracts that do not require carrying out a large number of successive transactions and do not present high ML/FT risks, it may be more appropriate for the internal procedures to stipulate that the individual risk assessment should be reviewed when one of the events provided for in the internal procedures occur which cannot influence the individual assessment of the risks linked to the business relationship concerned in and of themselves, but which trigger the review process in order to ensure that this assessment is still relevant.

In this respect, the NBB also notes that the provisions of the Anti-Money Laundering Law not only apply to the business relationships or the occasional transactions which financial institutions conclude with new customers, but also - without a transitional period - to the ongoing business relationships entered into with customers before the entry into force of these new legal provisions. The NBB therefore expects financial institutions to reassess the business relationships they entered into before the entry into force of the Anti-Money Laundering Law, prioritising business relationships which were considered to present a high risk before this reassessment.

Please refer:

- to the page "Policies, procedures, processes and internal control measures" for more information on the internal procedures;
- to the page "Ongoing due diligence and detection of atypical facts and transactions" for more information on the obligation to update individual risk assessments.

Moreover, it is advisable to **document** the individual assessment of the risks linked to each business relationship or occasional transaction, including changes made to it as part of an update, in a written document or in the form of data stored on an IT system, so that they can be reconstructed unaltered at any moment and be made available to the NBB.

## 4. Internal control measures

Financial institutions are expected to periodically verify whether their internal procedures regarding individual risk assessments are complied with on an ongoing basis and whether the process for fulfilling the related updating obligation is adequate.

The NBB therefore urges the internal audit function to pay particular attention to:

- the adequacy of the risks factors considered by the financial institution and the weighting assigned to each factor in order to perform the individual assessment of the ML/FT risks associated with the business relationships or occasional transactions;
- the inclusion, in the assessment of the risks linked to a business relationship, of any diversity in the services and products offered in the context of this relationship and of the relevance of the separate assessment of the risks associated with each of these products or services;
- the adequacy of the updates of the individual assessments performed.



# Anti-Money Laundering Law of 18 September 2017 - Article 19

## Art. 19

§ 1. Obligated entities shall take customer due diligence measures that involve:

1° identifying and verifying the identity of the persons referred to in Section 2, in accordance with the provisions of the said Section;

2° assessing the customer's characteristics and the purpose and intended nature of the business relationship or occasional transaction as well as, where appropriate, obtaining additional information for this purpose in accordance with the provisions laid down in Section 3; and

3° performing ongoing due diligence towards the business relationships and transactions in accordance with the provisions laid down in Section 4.

§ 2. The due diligence measures referred to in paragraph 1 shall be based on an individual ML/FT risk assessment, taking into account the characteristics of the customer and of the business relationship or transaction concerned. Moreover, this individual risk assessment shall take into account the overall risk assessment referred to in Article 16, first subparagraph, as well as the variables and factors referred to in the second subparagraph of the same Article, which are in particular taken into consideration in the latter assessment.

If obliged entities, in the context of their individual risk assessment referred to in the first subparagraph, identify cases of high risk, they shall take enhanced due diligence measures. They may apply simplified due diligence measures if they identify cases of low risk.

In all cases, obliged entities shall ensure that they can demonstrate to the supervisory authorities competent pursuant to Article 85 that the due diligence measures applied by them are appropriate in view of the ML/FT risks they have identified.

# Explanatory Memorandum to the Anti-Money-Laundering Law of 18 September 2017 - Article 19

## Art. 19

In practice, due diligence measures could often in the past be wrongly perceived as measures limited to the identification and knowledge of the customer (measures which are commonly known as 'KYC' or 'Know Your Customer'). However, the general due diligence obligations do appear to be far broader and must be understood as a coherent set of measures that aim to enable the obliged entities to identify suspicious transactions that must be reported to the CTIF-CFI. This is why draft Article 19, § 1 starts by recalling that the general due diligence obligations entail three separate obligations:

- The obligation to identify and check the identity of the clients and beneficiaries of life insurance policies, as well as, where applicable, that of their agents and beneficial owners (*the obligation to identify and verify the identity* which is explained in detail in section 2); the notion of 'life insurance' is defined in Article 4, 25°, as a life insurance policy within the meaning of those that fall under class 21 as referred to in Annex II of the Law of 13 March 2016 on the legal status and supervision of insurance or reinsurance companies, but also all insurance policies that fall under another insurance class (especially those that fall under classes 23, 25, 26 or 27) where the investment risk is borne by the policy-holders;
- The obligation to assess the customer's characteristics and the purpose and intended nature of the business relationship (or of the occasional transaction) and, where applicable, to obtain additional information for this purpose (the obligation to identify the customer's characteristics and the purpose and intended nature of the business relationship, which is explained in detail in section 3); and
- The obligation to perform ongoing due diligence as regards the business relationships and transactions; this obligation has two sides: careful examination of transactions carried out over the course of the business relationship; and updating the data held (the obligation of ongoing due diligence, which is explained in detail in section 4).

These three due diligence obligations are already set out in the Law of 11 January 1993, but in a more fragmented way. Moreover, considerably unequal importance is placed on this aspect: barely one paragraph mentions the obligation to identify the purpose and intended nature of the business relationship, in an Article that is otherwise focused on the identification of customers (Article 7). The draft Law aims to rationalise the way of presenting the three due diligence obligations and to emphasise that there are indeed three separate obligations, each of which is subject to its own rules and each of which the obliged entities have to comply with.

Article 19, § 2 transposes Article 13, paragraph 2 of Directive 2015/849, pursuant to which the risk-based approach applies to each of the general due diligence obligations. This entails a substantial review introduced by the Directive, which brings European legislation into line with Recommendation 10 of the FATF. Henceforth, all due diligence measures applied by an obliged entity, including the measures to identify customers, their agents and beneficial owners, and to verify their identity, must be taken by virtue of the assessment of ML/TF risks conducted by this entity vis-à-vis each business relationship or occasional transaction. This assessment, which is called an 'individual risk assessment' is therefore a key aspect of the system introduced by the draft Law.

The individual risk assessment entails the obliged entity analysing the ML/TF risks associated with a particular customer, taking into account two types of aspects:

- all information acquired by the obliged entity during the performance of its due diligence obligations. More particularly: the information regarding the identity of the customer, the customer's agents and beneficial owners, the information regarding the characteristics of the customer and the purpose and intended nature of the business relationship (or the transaction concerned) as well as all other information acquired as part of

ongoing due diligence. This is information which allows an understanding of the specific characteristics of the customer and of the business relationship or transaction concerned;

- the conclusions from the general risk assessment conducted pursuant to Article 16 of the draft Law, as well as the variables taken into consideration in this general risk assessment such as, in particular, the factors indicating a higher or lower risk, as referred to in Annexes II and III of the draft Law, but also the relevant conclusions from the report drawn up by the European Commission and the coordinating bodies, and the national risk assessment (see comment on Article 16). By way of reminder, the general risk assessment is a business-wide assessment, which is more objective than the individual assessment, which is specific to a particular customer. The general assessment entails the obliged entity determining the risks to which it is objectively exposed, taking into account its activities and the manner in which it conducts them (type of customer, geographical area, etc.). In practice, the general risk assessment determines the general theoretical framework within which the individual risk assessment should take place.

It should also be noted that Chapter 2 of this Title identifies situations in which the risk should in any case be deemed high, and in which the specific enhanced due diligence measures, as listed in the aforementioned Chapter 2, are consequently required. Without prejudice to the application of these specific measures, the obliged entities must also take into account these specific situations when they conduct an individual assessment of the risks associated with their customers.

After completion of the individual assessment, each customer is attributed a high, standard or low risk profile. Based on its general risk assessment, the obliged entity may need to further subdivide the categories of high risks and low risks to ensure the pertinence of the due diligence measures that apply to each risk profile.

By virtue of the risk-based approach, this risk profile will be decisive for:

- acceptance or refusal of a customer, in accordance with the customer acceptance policy defined by the obliged entity;
- the quantity of information necessary to identify the persons referred to in the Law, and the extent of the measures to be taken to verify this identity;
- the extent of the measures to be taken to understand the characteristics of the customer and the purpose and intended nature of the business relationship (or the transaction) concerned;
- the extent of the measures to be taken for ongoing due diligence, especially as regards examination of the transactions executed.

Where obliged entities come to the conclusion as part of their individual risk assessment that there is a high risk, they are required to apply stricter due diligence measures. These enhanced due diligence measures are set out in the entity's policies and internal control. The situation is different in the case of low risk. In that case, it is up to each obliged entity to decide whether the simplified due diligence measures apply for low risk, or whether the standard measures continue to apply. This *ab initio* (rather than case-by-case) decision must be justified and any simplified due diligence measures must be laid down in the policies and internal control measures.

Obliged entities must at all times be able to demonstrate to the supervisory authorities that the due diligence measures they apply are appropriate in light of the ML/TF risks they have identified in their individual risk assessment.



# Anonymous or numbered accounts and contracts

Home > Financial oversight > Combating money laundering and the financing of terrori...

## Legal and regulatory framework

- Anti-Money Laundering Law: Article 20
- Anti-Money Laundering Regulation of the NBB: Article 11

## Explanatory Memorandum of the Anti-Money Laundering Law

- Article 20

## Comments and recommendations by the NBB

### 1. Anonymous accounts or accounts under false names or pseudonyms

Article 20 of the Anti-Money Laundering Law prohibits financial institutions from opening anonymous accounts or accounts under false names or pseudonyms for their customers.

As entering into a business relationship with a customer requires the latter to be identified, the opening of anonymous accounts, i.e. accounts where the identity of the account holder is not known, cannot be permitted. Likewise, no account may be opened in a name that does not correspond to the true identity of the customer. However, this prohibition is without prejudice to the possibility to add details corresponding to a legitimate reality to a name, for example a trade name, the name of a subdivision of the customer or a collective name designating customers in a situation of joint ownership. However, the financial institution should carefully ensure that the detail added to the name is easily identifiable as such, and that it is not under any circumstances misleading as to the identity of the customer.

### 2. Numbered accounts

In accordance with Article 11 of the Anti-Money Laundering Regulation of the NBB, the opening of a numbered account for a customer is subject to the condition that the internal procedures set by the financial institution stipulate (i) the conditions under which these accounts may be opened or these contracts concluded, (ii) the terms of their operation and (iii) that these conditions and terms should be without prejudice to the application of the financial institution's AML/CFTP policies, procedures and internal control measures.

What is permitted, however, is the practice whereby, for reasons of confidentiality requested by the customer, the number of persons within the financial institution who have access to information that can reveal the identity of the customer concerned, are limited, inter alia by solely mentioning the account number on statements of account and other documents. Nevertheless, such a practice may not constitute a hindrance to the application of the rules of

identification and of other AML/CFTP measures. In such a case, the identity of the customer has to be known by the (i) senior officer responsible for AML/CFTP, (ii) the AMLCO and (iii) the persons in the financial institution who need that information in order effectively to comply with their due diligence obligations.

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



# Anti-Money Laundering Law of 18 September 2017 - Article 20

## Art. 20

The obliged entities referred to in Article 5, § 1, 3° to 22°, may not open anonymous accounts or accounts under false names or pseudonyms. They shall take all measures necessary to ensure compliance with this prohibition.



# NBB anti-money laundering regulation of 21 November 2017 - Article 11

## Art. 11

The opening of numbered accounts for customers or the conclusion of numbered contracts shall be subject to the condition that the internal procedures set by the obliged financial institution pursuant to Article 8 of the Law stipulate:

1° the conditions under which these accounts may be opened or these contracts concluded;

2° the terms of operation;

3° that these conditions and terms should be without prejudice to the obligations arising from the provisions laid down in Article 8, § 1, of the Law and in this Regulation.



# Explanatory Memorandum to the Anti-Money-Laundering Law of 18 September 2017- Article 20

## Art. 20

Article 20 prohibits credit institutions and other financial institutions from opening anonymous accounts or accounts under a false name or pseudonym, or in other words, any accounts in which the identity of the customer is unknown. This is not a new prohibition, but one taken over in the draft Law from Article 5 of the CBFA Regulations. It does indeed seem preferable to include the principle of the prohibition in the Law and to specify the appropriate measures to ensure compliance therewith by way of a regulation.

Article 20 thereby transposes Article 10, paragraph 1, first sentence of the Directive. The second sentence of Article 10, paragraph 1, which regulates the time frame for identification of the holders/beneficiaries of anonymous accounts, does not need to be transposed as anonymous bank accounts are not permitted in Belgium.

It should be noted that this is in analogy to what was previously stated on the subject of securities. Bearer securities in fact no longer exist under Belgian law (see Law of 14 December 2005 abolishing bearer securities, which came into full effect on 1 January 2014).



# Identification and identity verification

Home > Financial oversight > Combating money laundering and the financing of terrori...

## **Persons to be identified**

## **Object of the identification and identity verification**

## **Time of identification and identity verification**

## **Non-compliance with the identification and identity verification obligation**

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



## Persons to be identified

Home > Financial oversight > Combating money laundering and the financing of terrori...

### Legal and regulatory framework

- Anti-Money Laundering Law: Articles 21 to 25
- Anti-Money Laundering Regulation of the NBB: Article 10

### Explanatory Memorandum of the Anti-Money Laundering Law

- Articles 21 to 25

### Other reference documents

- ESAs Risk Factor Guidelines dated 4 January 2018
- BCBS Guidelines dated June 2017 on Sound management of risks related to money laundering and financing of terrorism (see Annex 4)
- FATF Guidance dated 27 October 2014 on Transparency and Beneficial Ownership

### Comments and recommendations by the NBB

- Comments and recommendations

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



# Anti-Money Laundering Law of 18 September 2017 - Articles 21 to 25

## Art. 21

§ 1. Obligated entities shall identify and verify the identity of customers:

1° who establish a business relationship with them;

2° who, outside the framework of a business relationship referred to in 1°, occasionally carry out:

a) one or more transactions which appear to be linked amounting to a total of EUR 10 000 or more; or

b) without prejudice to the obligations laid down in the European Regulation on transfers of funds, one or more credit transfers or transfers of funds within the meaning of that Regulation that appear to be linked and that amount to a total of more than EUR 1 000, or regardless of the amount if the obliged entity receives the funds concerned in cash or in the form of anonymous electronic money.

For the purposes of the first subparagraph, a transfer of funds carried out in Belgium on the payment account of a beneficiary shall not be considered a credit transfer or a transfer of funds within the meaning of the European Regulation on transfers of funds if each of the following conditions is met:

i) the account concerned only enables payment of the price for the provision of goods or services;

ii) the payment service provider of the beneficiary is an obliged entity;

iii) the payment service provider of the beneficiary is able to trace, by means of a unique transaction identifier and through the beneficiary, the person who has entered into an agreement with the beneficiary for the provision of goods and services; and

iv) the amount of the transfer of funds does not exceed EUR 1 000;

3° in the case of the operators of games of chance referred to in Article 5, § 1, 33°, without prejudice to 5° and 6°, who perform a transaction which consists of the wagering of a stake or, if the customer has yet to be identified and his identity yet to be verified, the collection of winnings amounting to EUR 2 000 or more, regardless of whether the transaction is performed in a single operation or in several operations that appear to be linked;

4° who are not referred to in 1° to 3°, and with regard to whom there is a suspicion of money laundering or terrorist financing;

5° with regard to whom there are doubts regarding the veracity or accuracy of the data that was previously obtained in order to identify them.

§ 2. For the purposes of § 1, 3°, transactions shall be deemed to be linked if they are performed by a single person, pertain to a single transaction of the same nature, have the same or a similar goal and are performed in the same place, regardless of whether these transactions are carried out simultaneously or at regular intervals.

§ 3. On the advice of the supervisory authorities competent pursuant to Article 85, the King may, by Decree deliberated in the Council of Ministers, set a lower threshold than that referred to in paragraph 1, 2°, a), for certain types of transactions and/or certain obliged entities, particularly taking into account the risk assessment conducted by the supervisory authorities competent by virtue of Article 87, § 1.

## Art. 22

Where appropriate, obliged identities shall identify and verify the identity of the agent(s) of the customers referred to in Article 21.

## Art. 23

§ 1. Where appropriate, obliged entities shall identify and take reasonable measures to verify the identity of the beneficial owner(s) of the customers referred to in Article 21 and of the agents referred to in Article 22.

Identifying the beneficial owners in accordance with the first paragraph includes taking reasonable measures to understand the ownership and control structure of the customer or of the agent who is a company, a legal person, a foundation, fiducie, trust or a similar legal arrangement.

§ 2. Paragraph 1 shall not apply if the customer, the customer's agent or a company that controls the customer or the agent is a company listed on a regulated market within the meaning of Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU, in a Member State, or on a regulated market in a third country where the listed company is subject to legal provisions that are equivalent to those laid down in the aforementioned Directive and that in particular impose disclosure requirements with regard to the shareholdings in the company concerned that are equivalent to those provided for in European Union Law.

## Art. 24

Without prejudice to Articles 21 to 23, the obliged entities referred to in Article 5, § 1, 4° to 22°, shall identify and verify the identity of the beneficiaries of life insurance policies.

Where appropriate, the obliged entities referred to in the first paragraph shall identify and verify the identity of the beneficial owners of the beneficiaries of the life insurance policies concerned. In that case, the provisions of Article 23 shall apply.

## Art. 25

Obliged entities that issue electronic money may, based on an appropriate ML/FT risk assessment conducted in accordance with Article 16 that demonstrates a low ML/FT risk, derogate from Articles 21 to 23 with regard to customers in the course of their business related to the issuance of electronic money, if the following risk mitigation conditions are met:

- 1° the payment instrument is not reloadable or can only be used in Belgium to make payments up to a maximum monthly limit of EUR 250;
- 2° the maximum amount stored electronically does not exceed EUR 250;
- 3° the payment instrument is used exclusively to purchase goods or services;
- 4° the payment instrument cannot be funded with anonymous electronic money;
- 5° the electronic money issuer concerned carries out sufficient monitoring of the transactions or business

relationship to enable the detection of unusual or suspicious transactions.

However, the electronic money issuer shall identify and verify the identity of every person to whom he redeems the monetary value of the electronic money for an amount exceeding EUR 100 in cash, or who withdraws such an amount in cash.



# NBB anti-money laundering regulation of 21 November 2017 - Article 10

## Art. 10

Obligated financial institutions shall identify and verify the identity of customers in accordance with Articles 26 to 32 of the Law when there are reasons to doubt that the person wishing to carry out a transaction under a business relationship entered into previously is actually the customer identified for this business relationship or his/her authorised and identified representative.



# Explanatory Memorandum to the Anti-Money-Laundering Law of 18 September 2017 - Articles 21 to 25

## Art. 21

Article 21 details the first category of natural persons that should be identified by obliged entities, i.e. customers. This category is essential as it forms the basis for whether or not there is an obligation to identify other persons (authorised agent or beneficial owner). After all, if a customer does not need to be identified, his/her authorised agents and beneficial owners do not need to either.

Not all customers of an obliged entity need to be identified. Article 21, § 1 lists the customers that are subject to the obligation to be identified. It thereby transposes Article 11, paragraph 1 of Directive 2015/849 and takes over the essential aspects of Article 7, first paragraph, of the Law of 11 January 1993. The following aspects should, nevertheless, be highlighted:

1° By virtue of paragraph 1, 1°, customers who establish a business relationship with the obliged entities must be identified. The notion of 'business relationship' is defined in the implementing regulations of the Law of 11 January 1993. For more clarity and uniformity, it was deemed necessary to define this notion in the draft Law itself. Article 4, 33° defines a business relationship as "a professional or commercial relationship with a client which is expected to have an element of duration, a) whether this business relationship results from entering into a contract under which several successive transactions are carried out between the parties during a specific or indefinite period, or which gives rise to permanent obligations; or b) whether this relationship results from the fact that, apart from entry into a contract as referred to in a), a customer regularly requests the intervention of the same obliged entity to carry out successive operations". The definition supplied by Article 3, 13) of the Directive is thereby supplemented to include the de facto business relationships referred to in Article 4 of the CBFA Regulation. This gives rise to a succession of occasional transactions also being able to constitute a (de facto) business relationship. It should be noted that this has an impact on the obligations of the obliged entity when several successive occasional transactions, which do not amount to a total of EUR 10 000, are requalified as a business relationship. In fact, unless there is a suspicion of money laundering, the Law does not require customers to be identified if they carry out occasional transactions which appear to be linked amounting to less than EUR 10 000 (cf. draft Article 21, § 1, 2°, a)). However, if the successive transactions are requalified by the obliged entity as a business relationship, the customer must be identified, without the threshold of EUR 10 000 applying (i.e. even if the total of the successive occasional transactions does not reach EUR 10 000).

2°, a) By virtue of § 1, 2° a) of the draft Article, customers need to be identified if they occasionally carry out a transaction amounting to EUR 10 000 or more, whether it is carried out in a single transaction or several transactions which appear to be linked. The threshold of EUR 10 000 is taken over from Article 7, § 1, 2° of the Law of 11 January 1993. It follows from this that, apart from cases in which there is a suspicion of ML/TF, a customer carrying out a single occasional transaction for an amount that is less than EUR 10 000 does not have to be identified. In the same way, a customer carrying out a succession of occasional transactions which are linked does not have to be identified if the total of these transactions does not reach EUR 10 000. However, if these successive transactions are requalified as a de facto business relationship, Article 21, § 1, 1° applies.

2°, b) By virtue of § 1, 2° b), first paragraph, the obligation to identify customers and to verify their identity applies when they occasionally carry out one or more transfers of funds that appear to be linked and that amount to a total of more than EUR 1 000. By way of derogation from this rule, these obligations apply regardless of the amount of

the transaction if the obliged entity receives the funds to be transferred in cash or in the form of electronic money that was issued without giving rise to the identification and verification of the identity of the customer (in particular pursuant to Article 25 of the draft Law or an equivalent provision of the law of another Member State).

As a reminder, the notion of 'European Regulation on transfers of funds' to which this provision refers is defined in Article 4, 5° of the draft Law. This term enables reference to be made successively to Regulation (EC) No 1781/2006, which will still be in force on the date of approval of the present Law and, from 26 June 2017, to Regulation (EU) 2015/847.

As a reminder, transfers of funds as referred to in draft Article 21, § 1, 2°, b) are defined in Article 3, 9) of Regulation (EU) 2015/847 as "any transaction at least partially carried out by electronic means on behalf of a payer through a payment service provider, with a view to making funds available to a payee through a payment service provider, irrespective of whether the payer and the payee are the same person and irrespective of whether the payment service provider of the payer and that of the payee are one and the same".

Although the introduction of a threshold of EUR 1 000 in Article 21, § 1, 2°, b) of the draft Law is new, it will only make a limited change to the obligations of the obliged entities under Article 7, § 1, first paragraph, 2°, b) of the Law of 11 January 1993, which imposes the identification and verification of the identity of the payer of the transfer of funds in all cases whatever the amount of the transaction.

In the first place, pursuant to both the current Regulation (EC) No 1781/2006 and Regulation (EU) 2015/847 which will replace it, the identification of the customer who is the payer of an electronic funds transfer is required whatever the amount transferred. The thresholds provided for by these EU Regulations, and by the present draft Law, only apply to determine if the payer's payment service provider has to additionally proceed to verify the identification details it has collected from the payer.

Secondly, it should be noted that the requirement to verify the identity of the payer, whatever the amount transferred, which was provided for by the Law of 11 January 1993, was essentially motivated by the high ML/TF risks associated with funds transfers (money remittance) where the payer remits the funds to be transferred in cash or anonymous electronic money. From now on, this high risk will, however, be covered by Regulation (EU) 2015/847. This latter provides that where the funds to be transferred are remitted in one of these forms, the identification details of the payer must be verified by the payment service provider, whatever the amount of the transaction. It is therefore advisable that the provisions of the draft Law be in line with the provisions of the new EU Regulation in this respect.

It should furthermore be noted that the threshold of EUR 1 000 is not applicable if the funds are transferred from a bank account. In such a case, both the identification and verification of the identity of the customer occurs in any case at the time of opening the account, pursuant to § 1, 1°, of this same Article 21 of the draft Law.

In practice, the EUR 1 000 threshold provided for in § 1, 2°, b) first paragraph, will especially be applicable for verifying the identity of the payer who occasionally calls on fully electronic payment services, which are therefore traceable, and where at least one intervening obliged entity has had to proceed with this verification. For example, in the case of an electronic funds transfer carried out using electronic money, the payment institution carrying out the transfer for the payer may make use of the threshold of EUR 1 000 if the issuer of the transferred electronic money has proceeded not only to identify the customer but to verify the customer's identity when issuing the electronic money.

The second paragraph of § 1, 2°, b) maintains in the draft Law Belgium's use in Article 7, § 1, second paragraph of the Law of 11 January 1993 of the option referred to in Article 3, § 6 of Regulation (EC) No 1781/2006 and which will from now on be provided for by Article 2, § 5 of Regulation 2015/847. This option aims to exclude, under certain conditions, certain transfers of very small amounts (maximum EUR 1 000) from the definition of funds transfers if they are made for the payment of goods or services by a consumer by way of a transfer of funds to an account opened by the service provider to receive these payments. A typical example of such situations is that of payment in cash, over the counter at bpost, of water, gas or electricity bills by persons who do not have a bank account from which they can make transfers.

3° providers of games of chance, for which the King does not provide for any exemption, are only obliged to identify their customers and verify their identity in certain specific cases, without prejudice to the provisions of the Law of 7 May 1999 on games of chance, bets, gaming establishments and the protection of players as explained below.

Identification and verification of the identity is above all necessary as soon as a business relationship is established. A business relationship is defined as a professional or commercial relationship with a customer which is expected to have an element of duration.

If a player appears in person, bets money and picks up any wins, this does not immediately turn into a business relationship because this relationship does not have an element of duration. After the game has ended and any wins have been paid out, the relationship between the player and operator comes to an end. As a result, this is an occasional transaction. It is a different matter if the player registers on a website to play games offered on this website. The player must create an account before being able to pay money into his/her player account. Communications relating to bets and wins go through the player account who may leave any positive balance on that account without requesting effective payment thereof. The relationship between the operator of the game of chance and the player therefore has an element of duration and constitutes a business relationship. Any online provider of games of chance must therefore proceed to identify and verify the identity of players at the time at which the business relationship is established.

Even if a business relationship is not established and there is a case of an occasional transaction, identification and verification of the identity remain necessary as soon as the transaction exceeds a certain amount. Although the upper limit for occasional transactions is EUR 10 000 for the different obliged entities, it goes down to EUR 2 000 for providers of games of chance. The EU Directive also offers the option of applying this limit to the bet, the payment of a win or to both.

As regards games of chance, the choice was made to apply the upper limit to a player's bets or, if there has been no identification yet, at the time of the payout of a win.

This choice arises from the fact that the Law of 7 May 1999 on games of chance, bets, gaming establishments and the protection of players already imposes very strict rules on the identification of certain customers.

In accordance with the Law on games of chance, Class I and Class II gaming establishments are subject to the obligation to register. Anyone who visits a Class I or Class II gaming establishment must be identified by way of their ID and if not, be refused admission to the gaming establishment. This identification and verification of identity therefore takes place in the Class I and Class II gaming establishments before any financial transaction has occurred. The player is as a result already identified prior to effectively betting any money. The operator of the gaming establishment is obliged to register all players who effectively bet EUR 2 000 or more, which is perfectly possible given that the players are already identified.

In a Class IV gaming establishment and a racecourse, the same registration is obligatory from the moment at which a player wishes to bet EUR 1 000. Here too, the obligations arising from the current legislation on games of chance are therefore stricter than required by the EU Directive.

A newsagent that offers bets may only accept bets of a maximum of EUR 200 per day and per customer. Bets exceeding EUR 200 per day must be refused by the newsagent. Depending on the amounts spent by the customer, a newsagent does not need to proceed with identification.

The need to provide for the possibility of identification has however been established for newsagents when small bets may bring in large wins ensuing in a higher risk of money laundering or fraud. As part of the fight against 'match fixing', where bets are placed on fixed matches to be able to bring in major wins, the player's identity is recommended to be verified before proceeding with the payout of major wins.

It is for this reason that the obligation to identify the customer has been provided for if a win of EUR 2 000 must be paid out to him/her, but only if the identity of the player is not yet known.

Games of chance that can be operated in a Class III gaming establishment or drinking establishment do not lend themselves to money laundering from the point-of-view of the player because of the restrictions these machines entail. Average hourly losses are EUR 12.5. The maximum bet per game is EUR 6.25 and the maximum win is EUR 500. Moreover, the probability of such a win is smaller than one per cent for all games. Because of this, this type of game is not an attractive channel for money laundering. In terms of day-to-day reality, there are hardly any bets or wins of EUR 2 000 associated with a single player in Class III gaming establishments. Players will therefore very rarely need to be identified.

In television games offered under a G1 licence, considerable restrictions are imposed by the King concerning the maximum bet of EUR 2 per call and a maximum win of EUR 5 000 over the entire period of the game. These bets are made through telephone calls and the money bet is either paid through the player's telephone bill or directly through a prepaid telephone card. The bets and wins of all other media games are even more limited. Here too, the player's identification would not be required under this legislation, even though in reality, the player is often identified before proceeding to pay out on the win.

Finally, and in application of the present draft Law, all obliged entities must proceed with identifying the player if they suspect money laundering or terrorism financing whatever the size of the amount bet or the win paid out. As soon as an operator of games of chance spots a suspicious act or a suspicious transaction, it must identify the player.

4° By virtue of § 1, 4° of the draft Article, customers who are not referred to in points 1° to 3° but with regard to whom there is a suspicion of ML/TF must be identified by the obliged entities. This is the case for example when a customer requests that an obliged entity carry out an occasional transaction for an amount of less than EUR 10 000 or a funds transfer transaction for an amount of less than EUR 1 000, which is not paid by the customer in cash or in the form of anonymous electronic money, and the circumstances of the customer's request raise a suspicion of ML/TF.

5° Paragraph 1, 5° requires obliged entities to repeat the exercise of their duty of identifying and verifying the identity of an existing client as soon as doubts arise, whatever the reason, as to the veracity or the accuracy of the data that was previously obtained. This obligation differs from the obligation to update the data, as provided for by Article 35, § 1, 2° of the draft Law in that, in the hypothesis referred to here, the entity has reasons to believe that the data sent to it were false or inaccurate from the start. Given these special circumstances, the obligation to repeat the duty of identifying and verifying the identity of the customer concerned is combined, where applicable, with the prohibition of maintaining the business relationship referred to in Article 33, as well as with the obligation to report to the CTIF-CFI in accordance with Article 47 if doubts as to the veracity or accuracy of the identification data give rise to a suspicion of ML/TF.

Article 21, § 3 gives the King the power, based on the recommendation of the competent supervisory authorities by virtue of Article 85, to set an identification threshold for certain types of transactions and/or certain types of obliged entities that is lower than that referred to in § 1, 2°, a), in particular taking into account the risk assessment conducted by the competent supervisory authorities in accordance with Article 87, § 1.

The amount of EUR 2 000 specified in this draft Article may be bet in a single operation or in several operations, when the player perhaps thinks he/she can elude the obligation of identification, but it must always be bet by one and the same person, in one and the same place. It is after all impossible for an operator to know whether a customer has already bet sums of money on games of chance elsewhere or has been paid winnings from them. If an operator notices that several customers collaborate, it must consider this suspicious and potentially proceed with an identification based on Article 21, 4°.

The notion of linked transactions in terms of games of chance must be understood to mean transactions (either betting or collecting winnings) in identical games by the same person with the same operator of games of chance during the same uninterrupted chronological sequence in the hope of obtaining a win. It is physically impossible in the real world to link the sequences of different games with different player return rates (chance of winning) which can be played in different gaming establishments at different times.

## Art. 22

Draft Article 22 refers to the second category of natural persons that should be identified by obliged entities, i.e. authorised agents of customers. It transposes Article 13, § 1, second paragraph of the Directive and thereby partially takes over Article 7, § 2 of the Law of 11 January 1993. The obligation to identify the authorised agent(s) of the customer constitutes an extension to the obligation to identify the customer. Consequently, the authorised agent of a customer who does not need to be identified pursuant to Article 21, § 1, does not need to be identified either.

## Art. 23

Draft Article 23, § 1, details the third category of natural persons that should be identified by obliged entities, i.e. beneficial owners.

## A. Definition

### A.1. General definition

The notion of 'beneficial owner' is defined in Article 4, 27° of the draft Law, transposing the definition provided by Article 3, 6) of the Directive. This is a complex notion that needs to be commented in detail.

The general definition essentially takes over that from Article 8, § 1, second paragraph of the Law of 11 January 1993, subject to the following:

- The definition in the draft Law from now on expressly includes beneficial owners of authorised agents and beneficiaries of life insurance contracts (within the meaning of Article 4, 25° of the draft Law. Following the comments on Articles 23 and 24, only the beneficial owners of customers will be referred to for the sake of brevity. However, the comments also apply to beneficial owners of authorised agents and beneficiaries of life insurance contracts.
- The proposed definition refers, in French, to natural persons on behalf of whom an "opération" is carried out whilst the French text of Article 8, § 1, second paragraph, of the Law of 11 January 1993 refers to natural persons on behalf of whom a "transaction" is executed. This amendment aims to clarify that it is both bilateral and strictly unilateral operations (such as for example a payment operation initiated only by the payer with no intervention by the beneficiary) that are referred to.

Although the general definition of this notion remains essentially unchanged, it should nevertheless be noted that Directive 2015/849 includes important clarifications introduced by the FATF Recommendations in 2012 (in particular, Recommendation 10 and the Interpretive Note to this Recommendation) for the specific implementation of this notion when the customer is a company, a legal person or a legal arrangement. It follows that the new definition included in the draft Law is considerably more detailed from this point of view than the definition provided in the Law of 11 January 1993.

The exclusion of listed companies included in the definition contained in Article 8, § 1, third paragraph, 1° of the Law of 11 January 1993 is transferred to the specific provisions of this draft Law on the obligation to identify beneficial owners. This does not constitute part of the definition but rather an exception to the obligation to identify beneficial owners.

As was already the case previously, the notion of beneficial owner in the sense of the draft Law refers to two types of natural persons:

- Natural persons who are considered to be persons who ultimately own or control the customer, the customer's authorised agent or the beneficiary of the life insurance contracts (Article 4, 27°, second paragraph).
- Natural persons on whose behalf a transaction is carried out or a business relationship is established (Article 4, 27°, third paragraph).

There may be several beneficial owners to be identified for the same customer or the same transaction and these beneficial owners may come under one or the other category.

### A.2. Natural persons who own or control the customer

Article 4, 27°, second paragraph identifies the persons who are considered to be persons who ultimately own or control the customer. As in Article 8, § 1, third paragraph of the Law of 11 January 1993, a distinction is made based on whether the customer is a) a corporate entity, b) a *fiducie* or trust, c) (international) non-profit organisations and foundations, or d) legal arrangements similar to *fiducies* or trusts.

The concept of a 'trust' is not defined in Directive 2015/849. The legal form of a trust does not form part of the Belgian legal system either. However, Chapter VII of the Belgian Code of Private International Law (CDIR) recognises the figure of a trust. The comments in Title 4, Chapter 1 of the Programme Law of 10 August 2015 (Parliamentary document, Chamber of Representatives, 54-1125/001, p. 25-35) gives a detailed description of what is meant in the 1992 Income Tax Code by "legal arrangement", including the trust.

To nevertheless provide an unequivocal definition of the concept of a “trust” in this draft Law, draft Article 4, 26° gives a definition of a trust, by referring to the definition provided in Article 122 of the CDIR, which makes an additional distinction by indicating that it refers only to an “express trust”. The CDIR also includes in its scope trusts enforced by a legal decision. This limitation to the “express trust” is also expressly repeated in Article 31, first paragraph of Directive 2015/849. An express trust is a trust established by the express wish of its founder.

The choice of definition provided in Article 122 of the CDIR is firstly dictated by the fact that it is the only legal definition that currently exists under the Belgian legal system. This choice is then motivated by legal certainty, i.e. to avoid there being several different definitions of a trust in Belgian law, which run the risk of comprising vague or subjective aspects. The description and definition of legal arrangements (including the trust) in the comments on Article 38 of the Programme Law of 10 August 2015 (Parliamentary documents, idem, p. 34) are very broad and refer to “any corporate entity, association, establishment, body or entity whatsoever, which has a legal personality and which, by virtue of the provisions of the legislation of the State or the jurisdiction in which it is established, is either not subject to income tax or is subject to income tax of less than 15 per cent of the taxable income of this legal arrangement, (...)”. This definition is considerably broader than the concept of “trust” in this draft Law. The comments in Title 4, Chapter 1 of the aforementioned Programme Law do properly describe the concept of trust as it should be understood under this Programme Law, and consequently under the 1992 Income Tax Code, but this is only a comment and not strictly speaking a definition. For the aforementioned reasons of legal certainty, the choice was made not to use this description, which only appears in the comments on the articles, as a definition in the draft Law.

The description of the legal arrangements in the aforementioned Programme Law then refers to legal forms that have already been covered separately in this draft law: corporate entities, associations, foundations, and other entities with legal personality. This would create confusion if the definition of trust was based on such a broad definition of what is referred to by this draft Law.

As already stated (see above), this draft law only refers to express trusts. The definition of trust in the comments of the aforementioned Programme Law does not expressly state that it does not refer to this form of trust. Apart from the trust enforced by a legal decision, the express trust is the only form of trust recognised under Belgian law. This does not prevent other forms of trusts and other forms of special purpose fund from being recognised under Belgian law. They fall in the category referred to by draft Article 4, 26°, b) relating to *fiducies* and in point d) of the same article for legal arrangements similar to trusts and *fiducies*. These other arrangements will not come under the scope of a trust but could for example be qualified as sui generis contracts. It should also be emphasised that under draft Article 74, § 1, second paragraph, the King, by way of a Decree deliberated in the Council of Ministers, determines which legal arrangements are similar to express trusts or *fiducies*.

The distinction between (international) non-profit organisations and foundations and legal arrangements similar to *fiducies* or trusts was introduced taking into account the specific legal structure of non-profit organisations and foundations, which is closer to that of commercial companies, in such a way that the identification of beneficial owners of non-profit organisations and associations by simple reference to those of trusts and *fiducies* became legally unreliable. Therefore, for the sake of legal certainty, it was necessary to expressly specify to which categories of natural persons the notion of beneficial owner applies in the specific case of non-profit organisations and foundations.

Therefore, the persons who are considered to be persons who ultimately own or control the customer are:

a) where the customer is a company:

Where the customer is a company, the identification of the persons considered to “ultimately own or control the customer” implies following a three-stage process. These latter are described in points i), ii) and iii) of Article 4, 27°, second paragraph, a) of the draft Law:

- Stage i) consists of determining the persons who possess, directly or indirectly, a sufficient percentage of voting rights or a sufficient ownership interest in that company;
- Stage ii) consists of determining the persons who, where applicable, exercise control of the company by other means;
- Stage iii) consists of determining who holds the position of principal manager.

Stages i) and ii) must be followed in all cases. Stage iii) is necessary only if no beneficial owner was able to be identified at the end of the two first stages.

**Stage i):** Firstly, the natural person(s) who possess, directly or indirectly, *ua sufficient percentage of voting rights or*

a sufficient ownership interest in the company must be identified:

- *A sufficient percentage of voting rights*: the Directive does not specify situations in which this percentage may be considered sufficient. However, as is the case by virtue of Article 8, § 1, third paragraph, 1° of the Law of 11 January 1993, the draft Law specifies that a natural person who possesses, directly or indirectly, more than twenty-five per cent of the voting rights must be considered as possessing a sufficient percentage of voting rights.
- *A sufficient ownership interest in the company*: in accordance with the Directive, Article 4, 27°, second paragraph, a), i), indicates that there is a sufficient ownership interest where:
  - a natural person holds more than twenty-five per cent of shares or more than twenty-five per cent of the company's capital;
  - a natural person controls, alone or with others, a company which itself holds more than twenty-five per cent of the shares or more than twenty-five per cent of the capital of the company;
  - a natural person controls, alone or with others, several companies which together hold more than twenty-five per cent of the shares or more than twenty-five per cent of the capital of the company.

Bearer shares (by definition governed by foreign law) must be taken into account.

**Stage ii):** Secondly, the natural person(s) who control the company by means other than the possession of a sufficient percentage of voting rights or a sufficient ownership interest in the company must be identified. The exercise of control "via other means" is not defined in the Law of 11 January 1993 but in Article 15 of the CBFA Regulation. Article 4, 27°, second paragraph, a), ii) of the present draft Law from now on specifies that the exercise of control "via other means" may in particular be established in accordance with the criteria referred to in Article 22, paragraphs 1 to 5 of Directive 2013/34/EU.

This second category notably refers to the natural person who exercises de facto control on a company or who possesses the right to appoint or revoke the majority of the members of the administrative body, management body or supervisory body of this company (Article 22, § 1, b) of Directive 2013/34/EU). This is the case currently referred to in Article 15 of CBFA Regulation by reference to Article 5, § 2, 2° of the Company Code.

In these cases, the voting rights are calculated as indicated in Article 22 of Directive 2013/34/EU.

**Stage iii):** If stages i) and ii) enabled identification of one or more natural persons and the obliged entity has no doubt as to the fact that the person or persons identified as such are indeed the beneficial owners, the process for identifying the beneficial owners may come to an end. Otherwise, the third stage is required. It should be noted that the obliged entity must put in place all means possible to try to identify the natural persons referred to in point i) and ii). An obliged entity may not for example, in order to accelerate the process of identification of beneficial owners, go straight to the third stage without doing everything possible to identify the persons referred to in point i) and ii). An obliged entity acting in this way would breach its obligation of identifying the beneficial owners. In this respect, the obligation for obliged entities to keep information relating to the measures taken in order to identify beneficial owners should be noted (cf. Article 60).

If stages i) and ii) have not enabled identification, with sufficient certainty, of one or more natural persons, and as long as there are no motives for suspicion, the third stage must be applied and consists of identifying the natural person(s) who occupy the position of principal manager. It is these people who will as a last resort be considered the customer's beneficial owners.

It should be noted that, as this third stage only needs to be observed if the first two have not allowed identification of the beneficial owners, it constitutes a reversal of the former system. Pursuant to the Law of 11 January 1993, as implemented by the CBFA Regulation (Article 15), persons who have an office within the company's administrative body and who influence its management in this respect are considered to belong to the category of natural persons who "otherwise exercise the power of control on the management of the company" and should in principle always be identified as beneficial owners.

This third stage contained in the draft Law differs from the previous system in that:

- this third stage only needs to be observed if the first two have not allowed identification of the beneficial owners, and

- it doesn't consist of identifying as beneficial owners all the managers of the company, but only those who occupy the position of "principal managers".

The notion of "principal managers" is not defined in the Directive. It should be understood to include the managers of a company who exercise, in practice, the most influence on the company's management. As a general rule, this will be the Chief Executive Officer or the Chairman of the Board of Directors.

b) where the customer is a *fiducie* or trust:

Draft Article 4, 27°, § 1, second paragraph, b) refers to the cases in which the customer is a *fiducie* or trust. As a reminder, Belgian law does not recognise these legal arrangements. This therefore refers to *fiducies* and trusts governed by foreign law, and in particular trusts under Anglo-Saxon law and *fiducies* under French and Luxembourg law.

Where the customer is a *fiducie* or trust, the latter's beneficial owners are:

- the founder;
- the fiduciaries or trustees;
- the protector, where applicable;
- the beneficiaries or, where the persons who will be the beneficiaries of the *fiducie* or the trust have not yet been designated, the category of persons in whose principal interest the *fiducie* or trust has been constituted or operates;
- any other natural person ultimately exercising control of the *fiducie* or trust as a result of being the owner thereof, directly or indirectly or by other means;

c) where the customer is an (international) non-profit organisation or a foundation:

It should be noted that (international) non-profit organisations are not expressly referred to in the Directive; however, given that they may be used in certain cases to finance terrorism, they should be contemplated here. They were already contemplated in the Law of 11 January 1993 (Article 8, § 1).

In particular, the following natural persons should be considered the beneficial owners of an (international) non-profit organisation:

- i. Administrators, as referred to in Article 13, first paragraph, Article 34, § 1 and Article 49, second paragraph of the Law of 27 June 1921 on non-profit associations, foundations, and European political parties and foundations;
- ii. Persons with the power to represent the non-profit organisation by virtue of Article 13, fourth paragraph, of the same Law;
- iii. Persons tasked with the day-to-day management, referred to in Article 13bis, first paragraph, and in Article 35, first paragraph and Article 49, second paragraph of the same Law;
- iv. The founders of a foundation, referred to in Article 27, first paragraph of the same Law. However, the founders of an (international) non-profit organisation may hardly be considered beneficial owners if they do not at the same time come under one of the other categories of beneficial owners referred to in this Law. (International) non-profit organisations are in fact generally founded for a specific aim which often requires a long-term commitment. (International) non-profit organisations therefore often have a long lifespan and several generations of members and administrators succeed each other with a view to pursuing the disinterested aim of the (international) non-profit organisations. It often happens that the founders leave after a certain time to make way for others and attract fresh blood to the organisation. The founders who are no longer members of the (international) non-profit organisation and no longer exercise any role or office in it, sometimes for a long period of time or dozens of years, may therefore hardly be considered their beneficial owners;
- v. Natural persons or, where these persons are not yet designated, the category of natural persons in the principal interest of which the (international) non-profit organisation or foundation was constituted or operates;

This point implements Article 3, § 6, b, iv), of the aforementioned Directive. This can be the person or persons (non-members) for the benefit of whom the aim of the foundation or of the non-profit organisation provides for support, a benefit, aid etc. An example is a non-profit organisation which aims to support victims of war. The beneficiaries are for example victims of the war in Syria. Another example is a foundation to help the disabled. In this case, it can be a person named in the articles of association, or otherwise a category of persons, for example only those who live in the Brussels-Capital Region;

vi. All other natural persons ultimately exercising control by other means of the (international) organisation or foundation. This residual category takes over the formulation, *mutatis mutandis*, used in Article 4, 27°, b, v) as regards *fiducies* and trusts. The term 'beneficiaries' arises in their case from the general definition included in Article 4, 27°, first paragraph and relates, among others, to persons who ultimately exercise control on the association without being a member, for example a person who works behind the scenes via one or more front men, or a member who, through accumulated mandates of representation combined with the absence of other members of the general meeting, would in this case exercise ultimate control on the (international) association during several successive accounting years.

The information referred to in points i) to iv) is already contained in the Crossroads Bank for Enterprises. The information referred to in points v) to vi) should for their part be sent within the month by electronic means to the register of beneficial owners, established by Article 73 of the draft Law.

d) where the customer is a legal arrangement similar to a *fiducie* or a trust:

Where the customer is a legal arrangement similar to a *fiducie* or trust, the beneficial owners are the natural persons who occupy the roles that are equivalent or similar to those of the persons referred to in point b).

### A.3. Natural persons for whom a transaction is executed or a business relationship is entered into

Draft Article 4, 27°, third paragraph identifies the natural persons for whom a transaction is executed or a business relationship is entered into. This is a clarification not provided by the Directive, this latter only explaining the first category of beneficial owner (natural persons who "own or control the customer"). This second category of beneficial owners therefore refers to natural persons:

- who profit or will profit from this transaction or this business relationship; and
- who have the power, in law or in fact, directly or indirectly, to decide to execute the said transaction or enter into the said business relationship and/or to establish the methods to consent thereto.

It should be noted that in this case, the transaction may be executed or the relationship entered into by a customer who is a natural person. It is therefore important not to limit the search for beneficial owners only to the cases in which the customer/authorised agents are not natural persons.

If transactions aim to enable a financial institution to effectively supply to its own clientele the products or services it offers, these transactions are to be considered as transactions on behalf of the financial institution itself and not on behalf of its customers. In this case, they are not able to determine any methods of these transactions. This is the case, for example, when a credit institution contracts interbank lending to finance its credit portfolio or where it calls on clearing/settlement services provided by another financial institution to ensure the proper execution of the services it offers its customers for payments or securities transactions.

However, where a customer carries out a financial transaction (deposit, loan, securities transactions etc.) at a financial institution whilst having the power to determine all or part of the methods of the subsequent financial transactions that this establishment will carry out in its own name but on the customer's behalf, at other financial counterparties, these latter must consider the customer of the financial institution the beneficial owner of the transactions that this institution performs in this context with them.

## B. Specific provisions

Paragraph 1 of Article 23 of the draft Law lays down the obligation to identify the beneficial owner(s) of customers and the authorised agents of customers.

This obligation is the extension to the obligation to identify the customer and the customer's authorised agents. Consequently, the beneficial owners of a customer who does not need to be identified pursuant to Article 21, § 1, do not need to be identified either. This also applies to beneficial owners of authorised agents of such a customer.

With that proviso, the obligation to identify the beneficial owners constitutes a general obligation of obliged entities. Meeting it requires, in the first instance, that the obliged entity determine whether its customer has one or more beneficial owners.

In this respect, it should be noted that it is not only the natural persons who "ultimately own or control the customer", but also those "for whom a transaction is executed or a business relationship is entered into", that are qualified as beneficial owners. An obliged entity would therefore be wrong to limit the exercise of its obligation to identify the beneficial owners only to the cases in which the customer is a legal person or a legal arrangement such as a trust or a fiducie. After all, if customers who are natural persons act most often on their own behalf, they may also act on behalf of other persons, even if in their own name, and must therefore be qualified as beneficial owners of the customer.

Where the customer or the authorised agent is a legal person, a fiducie, a trust, a company, a foundation or a similar legal arrangement, the second paragraph of draft Article 23, § 1 expressly specifies that the obligation to identify the beneficial owners includes that of taking reasonable measures to understand the ownership and control structure of the customer. Article 23, § 1 thereby transposes Article 13, § 1, first paragraph, b) of the Directive.

Paragraph 2 of this article transposes the exemption, provided for by Article 3, 6), a), i), first paragraph of Directive 2015/849, from the obligation to identify and verify the identity of the beneficial owners if the customer, the customer's authorised agent, or a company that controls the customer or authorised agent is a company listed on the regulated markets referred to. This takes over the exemption provided for in the definition of beneficial owner in the Law of 11 January 1993.

Paragraph 2 refers to the regulated markets in a Member State and the regulated markets in a third country, on the condition that in this third country, the listed company is subject to the legal provisions equivalent to those laid down by Directive 2004/39/EC on markets in financial instruments and which in particular impose obligations as to the advertisement of holdings in the company concerned which are equivalent to those provided for by the Law of the European Union. The regulated markets referred to in Article 23, § 2 are the regulated markets within the meaning of the aforementioned Directive 2004/39/EC.

## Art. 24

Article 24, first paragraph, which transposes Article 13, § 5, first paragraph of Directive 2015/849, refers to the very specific case of life insurance contracts within the meaning of Article 4, 25° of the draft Law. This is why a specific article is devoted to that case. It provides that over and above their obligations to identify and verify the identity of customers, their authorised agents and beneficial owners, the financial institutions concerned that enter into life insurance contracts must identify and verify the identity of the beneficiaries of these contracts, who may be different to the beneficial owners of the customer who enters into the life insurance contract.

Article 21 of Directive 2015/849 imposes taking reasonable measures to determine whether the beneficial owners of the beneficiaries of life insurance contracts are PEPs. Although this is not expressly stated in the Directive, this presupposes that these beneficial owners are known. Article 24, second paragraph, therefore provides for the obligation for obliged entities to identify and also to verify the identity of the beneficial owners of the beneficiaries of the contracts concerned. In this case, the provisions of Article 23 apply. For the rest, reference is made to the comment on the latter.

## Art. 25

As part of the general risk assessment to which the obliged entities that issue electronic money must proceed in accordance with Article 16 of the draft law, these obliged entities are required to identify and assess the ML/TF risk specifically related to their issuance activity. If this assessment reveals that the activity of issuance of electronic money presents a low ML/TF risk, electronic money issuers may decide not to apply measures to identify and verify

the identity of customers who remit funds to them to with a view to issuing electronic money (and consequently, authorised agents and beneficial owners of these customers), where the conditions listed below are met. It should be underlined that the decision not to apply measures to identify and verify the identity should be justified based on the low risk, in the internal policies and procedures of the obliged entity, which will have to clearly define the cases in which no measure to identify and verify the identity of the customer will need to be applied.

In accordance with Article 12, § 1 of Directive 2015/849 transposed herein, dispensing with identification the customer is subject to the following conditions:

- the payment instrument concerned is not reloadable, or if it is, it may only be used in Belgium and only to make payments subject to the monthly limit of EUR 250; the official French translation of this provision of Directive 2015/849 seems inappropriate so it has been reworded;
- the maximum amount stored on the electronic support may not exceed EUR 250;
- the payment instrument may be used solely for the purchase of goods or services;
- the payment instrument may not be credited with anonymous electronic money;
- the electronic money issuer concerned exercises sufficient oversight of the transactions or the business relationship to be able to detect any unusual or suspicious transactions.

Paragraph 2 of this draft Article, which transposes Article 12, § 2 of Directive 2015/849, provides that, where a customer of an electronic money issuance service obtains a refund in cash of the monetary value of the electronic money or withdraws this amount in cash, he/she must be identified and his/her identity verified by the obliged entity (as well as the authorised agents and beneficial owners) if the amount effectively refunded/withdrawn is above EUR 100. In this case, the Directive considers that the risk of ML/TF linked to the transaction may not be considered low and the measures for identification and verification of the identity must be applied at the time of withdrawal or refund of the electronic money issued previously without proceeding with the identification and verification of the identity of the customer.

# Persons to be identified: Comments and recommendations by the NBB

Home > Financial oversight > Combating money laundering and the financing of terrori...

## Contents

- 1. Categories of persons to be identified and whose identity should be verified
- 2. Specific derogation: low-risk issuance of electronic money

## 1. Categories of persons to be identified and whose identity should be verified

### 1.1 Enumeration

The Anti-Money Laundering Law and the Anti-Money Laundering Regulation of the NBB distinguish four categories of persons who should be identified by the financial institutions and whose identity should be verified:

- **the customers** (Article 21 of the Law and 10 of the Regulation):
  - with whom they establish a business relationship;
    1. one or more transactions which appear to be linked and which amount to a total of EUR 10 000 or more; or
    2. without prejudice to the obligations laid down in the European Regulation on transfers of funds, one or more credit transfers or transfers of funds that appear to be linked and that amount to a total of more than EUR 1 000, or regardless of the amount if the financial institution receives the funds concerned in cash or in the form of anonymous electronic money; who, outside the framework of a business relationship, occasionally carry out: Pursuant to Articles 5(3)(a) and 7(4)(a) of the European Regulation on transfers of funds, the obligation to identify and verify the identity of the payer and payee in case of a transfer of funds applies regardless of the amount of the transaction when the payment service provider receives or remits the transferred funds in cash or in anonymous electronic money;
  - who are not referred to above and with regard to whom there is a suspicion of ML/FT;
  - with regard to whom there are doubts regarding the veracity or accuracy of the data that was previously obtained in order to identify them;
  - when there are reasons to doubt whether the person wishing to re-establish a previously established business relationship is actually the customer identified in the framework of this business relationship or his authorised and identified agent;
- **the agents** of the aforementioned customers (Article 22 of the Law),
- **the beneficial owners** of the customers and of their agents (Article 23 of the Law)
- and **the beneficiaries of life insurance policies** or of equivalent policies (Article 24 of the Law).

For more information on the persons to be identified and whose identity should be verified and, in particular, on the notions of “business relationship”, “transfer of funds” and “beneficial owner”, see the comments in the Explanatory Memorandum of Articles 21 to 24 of the Anti-Money Laundering Law.

### 1.2 Application of a risk-based approach

As for all due diligence obligations, a risk-based approach is also adopted for the identification and identity verification obligation, in accordance with Article 19 of the Anti-Money Laundering Law. Each financial institution must henceforth determine, based on the risk identified by it, which information should be obtained to identify a person and which information should be verified to ascertain his/her identity. This is a substantial change compared to the Law of 11 January 1993, which adopted a rule-based approach and listed which information should be obtained and verified in all cases in order to fulfil the identification and verification obligation.

Consequently, the legal exemptions from the identification obligation that were previously mentioned in Article 11 of the Law of 11 January 1993 are not included in the Anti-Money Laundering Law. Henceforth, when business relationships are established or occasional transactions concluded with customers who were mentioned in the aforementioned Article 11 of the Law of 11 January 1993, it will fall upon the financial institution to perform an individual risk assessment in accordance with Article 19, § 2, of the Law and to determine, on the basis of the results of this assessment, the intensity of the measures to be taken to identify and verify the identity of the customer, which may be lower in cases of low risk but must be higher in cases of high risk.

For more information in this regard, see the page “Object of the identification and identity verification”.

### 1.3. Internal procedures

As a reminder, the NBB recommends that financial institutions, in the context of the internal procedures to be adopted pursuant to Article 8 of the Anti-Money Laundering Law, establish, in particular, procedures for the due diligence measures to be implemented with regard to customers and transactions, which notably enable them to ensure that the persons to be identified are listed exhaustively.

For more information on this subject, see the page “Policies, procedures, processes and internal control measures”.

## 2. Specific derogation: low-risk issuance of electronic money

### 2.1. Possibility of derogation

Article 25 of the Anti-Money Laundering Law provides for the possibility of derogation for financial institutions issuing electronic money. These institutions may, where the overall assessment of the ML/FT risks specifically associated to their issuing activity shows that these risks are low, decide to neither identify nor verify the identity of the customers (and, where appropriate, of their agent(s) and beneficial owner(s)) who provide them with funds for the issuance of electronic money.

### 2.2. Conditions for application of the derogation

However, this possibility of derogation is subject to multiple **conditions**. **In addition to the fact that the overall risk assessment carried out by the electronic money issuer must demonstrate that the level of ML/FT risks to which it is exposed as a result of this activity is low**, the following cumulative conditions must be met:

1. the payment instrument cannot be reloaded or, if it is reloadable, it can only be used in Belgium and only to make payments up to a maximum monthly limit of EUR 250;
2. the maximum amount stored electronically does not exceed EUR 250;
3. the payment instrument is used exclusively to purchase goods or services; it follows in particular that it cannot be accepted to perform a money remittance operation;
4. the payment instrument cannot be funded with anonymous electronic money;
5. the electronic money issuer concerned carries out sufficient monitoring of the transactions or business relationship to enable the detection of unusual or suspicious transactions.

### 2.3. Non-application of the derogation

Even if all the conditions listed above are met, the derogation is **not applicable** when a customer:

1. is redeemed in cash, at the monetary value of the electronic money, or
2. withdraws this value in cash,

if the amount redeemed or withdrawn, as the case may be, exceeds EUR 100.

In these two cases, where the legislator considered that the risk could not be regarded as low, the electronic money issuer is required to take appropriate measures to identify and verify the identity of the customer concerned (and, where appropriate, of his agent(s) and beneficial owner(s)) **at the time of the refund or withdrawal of the electronic money** (that was previously issued without any such measures).

In the same vein, the NBB highlights the fact that, where circumstances have given rise to suspicions of ML/FT, either at the time of establishment of the business relationship with the customer or subsequently, that lead the electronic money issuer to report a suspicion to CTIF-CFI and, in accordance with Article 22 of the Anti-Money Laundering Regulation of the NBB, to carry out an individual re-assessment of ML/FT risks revealing that the level of risk associated with the given situation can no longer be regarded as low (which should logically be the case - see the page "Reporting of suspicions"), the said issuer can no longer invoke the derogation provided for in Article 25 of the Law. The issuer should immediately identify and verify the identity of the customer (and, where appropriate, of his agent(s) and beneficial owner(s)), in accordance with Articles 21 to 23 of the Law.

## 2.4. Documentation

Finally, since the above-mentioned possibility of derogation is not absolute but subject to certain limitations, the NBB recommends that the financial institutions applying the derogation be able not only to submit the overall risk assessment that establishes the low level of risk, which must be documented, updated and made available to the NBB pursuant to Article 17 of the Law (see the page "Reporting by financial institutions"), but also to demonstrate to the NBB that, in all cases where they have applied Article 25 of the Law, each of the legal conditions to benefit from this derogation is met.

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



# Object of the identification and identity verification

Home > Financial oversight > Combating money laundering and the financing of terrori...

## Legal and regulatory framework

- Anti-Money Laundering Law: Articles 26 to 29
- Anti-Money Laundering Regulation of the NBB: Articles 12 to 14
- Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

## Explanatory Memorandum of the Anti-Money Laundering Law

- Articles 26 to 29

## Other reference documents

- Opinion of the ESAs dated 23 January 2018 on the use of innovative solutions by credit and financial institutions
- ESAs Risk Factor Guidelines dated 4 January 2018
- FATF Guidance dated 4 November 2017 on AML/CFT measures and financial inclusion, with a supplement on customer due diligence
- BCBS Guidelines dated June 2017 on Sound management of risks related to money laundering and financing of terrorism (see Annex 4)
- EBA Opinion dated 12 April 2016 on the application of customer due diligence measures to customers who are asylum seekers from higher-risk third countries or territories

## Comments and recommendations by the NBB

- Comments and recommendations

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**





# Anti-Money Laundering Law of 18 September 2017 - Articles 26 to 29

## Art. 26

§ 1. In order to fulfil their obligation to identify the persons referred to in Articles 21 to 24, obliged entities shall collect relevant information on these persons that enables the entities to distinguish them from any other person with reasonable certainty, taking into account the risk level identified in accordance with Article 19, § 2, first subparagraph.

§ 2. Without prejudice to the low-risk situations referred to in paragraph 3 or the high-risk situations referred to in paragraph 4, the relevant information referred to in paragraph 1 shall comprise:

1° where the identification obligation pertains to a natural person: his last name, first name, date and place of birth and, to the extent possible, address;

2° where the identification obligation pertains to a legal person: his corporate name, registered office, the list of his directors and the provisions governing the power to make binding agreements on behalf of the legal person;

3° where the identification obligation pertains to a trust or a similar legal arrangement: its corporate name, the information referred to in 1° or in 2° regarding its trustee(s), its founder(s) and, where appropriate, its protector(s), as well as the provisions governing the power to make binding agreements on behalf of the trust or similar legal arrangement.

By way of derogation from the first subparagraph, 1°:

1° if the identification obligation pertains to a natural person in his capacity as beneficial owner, his date and place of birth shall be identified to the extent possible;

2° where the identification obligation pertains to natural persons in their capacity as beneficial owners of a foundation, a(n) (international) non-profit organisation, a fiducie or a trust or a similar legal arrangement that appoints its beneficiaries based on their special characteristics or the specific category to which they belong, the obliged entity shall collect sufficient information on the characteristics or category concerned in order to be able to identify the natural persons who are beneficial owners at the time of the exercise of their vested rights or at the time of the pay-out.

By way of derogation from the first subparagraph, 1° to 3°, if the identification obligation pertains to the beneficiary of a life insurance policy:

1° where the beneficiary of the policy is designated by name, the obliged entity shall collect information on the first and last name or the corporate name of the beneficiary;

2° where the beneficiary of the policy is designated by his or its characteristics, by category or by other means, the obliged entity shall collect sufficient information on this beneficiary to ensure that it is able to determine the identity of this beneficiary at the time of the pay-out.

§ 3. If the individual risk assessment conducted in accordance with Article 19, § 2, first subparagraph, shows that the risk associated with the customer and with the business relationship or with the transaction is low, the obliged entity may reduce the amount of information it collects in comparison with the information listed in paragraph 2. The collected information must however remain sufficient in order to make it possible to distinguish the person concerned from any other person with reasonable certainty.

§ 4. If the individual risk assessment conducted in accordance with Article 19, § 2, first subparagraph, shows that the risk associated with the customer and with the business relationship or with the transaction is high, the obliged entity shall pay particular attention to ensure that the information it collects pursuant to paragraph 2 enables it to conclusively distinguish the person concerned from any other person. If necessary, it shall collect additional information for this purpose.

## Art. 27

§ 1. In order to fulfil their obligation to verify the identity of the persons referred to in Articles 21 to 24, obliged entities shall check all or part of the identification data collected pursuant to Article 26 against one or more supporting documents or reliable and independent sources of information which enable them to confirm this data, in order to have a sufficient degree of certainty that they know the persons concerned. To that end, obliged entities should take into account the risk level identified in accordance with Article 19, § 2, first subparagraph.

§ 2. Without prejudice to the application of paragraphs 3 and 4, obliged entities shall verify all identification data collected pursuant to Article 26, § 2.

§ 3. If the individual risk assessment conducted in accordance with Article 19, § 2, first subparagraph, shows that the risk associated with the customer and with the business relationship or with the transaction is low, the obliged entity may verify a smaller amount of information collected pursuant to Article 26. However, a sufficient amount of information must be verified in order to enable the obliged entity to have a sufficient degree of certainty as to its knowledge of the person concerned.

§ 4. If the individual risk assessment conducted in accordance with Article 19, § 2, first subparagraph, shows that the risk associated with the customer and with the business relationship or with the transaction is high, the obliged entity shall verify all the information collected by it pursuant to paragraph 2, and it shall pay particular attention to ensure that the documents and sources of information it uses to verify this information enable it to have a high degree of certainty as to its knowledge of the person concerned. If necessary, it shall collect additional information for this purpose.

## Art. 28

§ 1. Upon request from an obliged entity referred to in Article 5, § 1, and solely for the purposes of the verification, by such an entity, of the identity of the customers and their agents who are natural persons and who are not present during their identification, for the purposes of the verification of the identity of the beneficial owners of the customers, as well for the purposes of updating the data relating to the identification of the customers, agents and beneficial owners, in accordance with this Law, the professional associations designated by the King shall be authorised to:

1° use the identification number from the National Register;

2° access the data of the National Register of natural persons referred to in Article 3 of the Law of 8 August 1983 establishing a National Register of natural persons;

3° make a paper or electronic copy of the information consulted in the said Register.

They shall provide the obliged entity that requested it with the information necessary to fulfil its obligations listed in the first subparagraph.

They may, together or each separately, create or use an institution which, where appropriate, has received the authorisation referred to in the first paragraph in their stead and which provides the obliged entity that requested it with the information necessary to fulfil its obligations listed in the first subparagraph.

Without prejudice to the provisions of other laws, regulations or implementing decrees, the institutions referred to in the third paragraph shall meet the following requirements:

1° they possess legal personality;

2° their registered office and general management are established in Belgium;

3° they are under the exclusive control of the professional associations that created them pursuant to the first subparagraph or of the obliged entities that are members of these professional associations.

§ 2. The obliged entities referred to in paragraph 1, first subparagraph may, for the purpose of compliance with the obligations listed therein, use, process, maintain and make a paper or electronic copy of any information they receive from the professional associations or the institutions created by them pursuant to paragraph 1, third subparagraph.

§ 3. When designating the professional associations referred to in paragraph 1, the King shall ensure that they are qualified to perform their function as intermediary in the context of the application of this Article, particularly in the context of their suitability to represent the obliged entities, of their sustainability, their governance and their organisation or, where appropriate, that of the institution they create.

## Art. 29

Obliged entities that have access to the central register of beneficial owners referred to in Article 73, to the equivalent registers held in other Member States pursuant to Article 30(3) of Directive 2015/849 or in third countries, or to the registers of the beneficial owners of trusts, fiducies or similar legal arrangements held in other Member States pursuant to Article 31(4) of Directive 2015/849 or in third countries, shall not rely solely on the consultation of these registers in order to fulfil their obligation to identify and verify the identity of the beneficial owners of their customers, their customers' agents or the beneficiaries of life insurance policies. To that end, they shall implement additional measures that are proportionate with the risk level identified in accordance with Article 19, § 2, first subparagraph.



# NBB anti-money laundering regulation of 21 November 2017 - Articles 12 to 14

## Art. 12

The internal procedures defined by the obliged financial institution pursuant to Article 8 of the Law shall also provide for:

1° precise rules concerning supporting documents or reliable and independent sources of information accepted by the obliged financial institution for the purposes of verification of identity pursuant to Article 27, § 1, of the Law, depending on the characteristics of the persons in question, the individual risk assessment made pursuant to Article 19, § 2, of the Law, and the risk classification carried out pursuant to Article 4 of this Regulation.

For the purposes of verification of identity, a specific identification technology may be accepted as a supporting document or reliable and independent source of information within the meaning of the above-mentioned Article 27, § 1, of the Law, if an analysis of the reliability of this technology so justifies;

2° if the individual risk assessment conducted in accordance with Article 19, § 2, 1st indent, of the Law, shows that the risk associated with the customer and the business relationship or the occasional transaction is low:

information which, pursuant to Article 26, § 3, of the Law, must not be collected by the obliged financial institution;

information which, pursuant to Article 27, § 3, of the Law, must not be verified;

3° if the individual risk assessment conducted in accordance with Article 19, § 2, 1st indent, of the Law, shows that the risk associated with the customer and the business relationship or the occasional transaction is high:

information which, pursuant to Article 26, § 4, of the Law, is considered by the obliged financial institution as enabling an indisputable distinction of the person concerned from anyone else, as well as any additional information to be collected if necessary;

the measures to be taken by the obliged financial institution paying particular attention to ensure that the documents or sources of information used to verify this information enable it, pursuant to Article 27, § 4, of the Law, to acquire a high degree of certainty as to its knowledge of the person concerned;

4° the measures to be taken by the obliged financial institution when it identifies the agent(s) of a customer, pursuant to Article 22 of the Law, the representative(s) of a customer, and verifies their identity, to ascertain the powers of representation of the person(s) concerned;

5° the measures to be taken by the obliged financial institution to understand, pursuant to Article 23, § 1, 2nd indent, of the Law, the ownership and control structure of the customer or of the agent who is a company, a legal person, a foundation, a fiducie, a trust or a similar legal arrangement;

6° the measures to be taken by the obliged financial institution to identify and verify the identity of the beneficial owners of its customers, agents of its customers or beneficiaries of life insurance contracts, in addition to consultation of the registers referred to in Article 29 of the Law, if necessary.

## Art. 13

Without prejudice to the identification and verification of the identity of customers who are professional counterparties, as well as their beneficial owners, in accordance with Articles 21, 23 and 26 of the Law and this Regulation, and provided that the obliged financial institutions which establish a relationship with these counterparties or carry out transactions with them shall ensure that they themselves and their transactions do not present high ML/FT risks, obliged financial institutions may extend identification of customers' employees who they have mandated to conclude transactions on their behalf to cover the last name, first name, date and place of birth and the rank or functions of these employees in the customer chart, with the exception of their address.

The internal procedures of obliged financial institutions that make use of the option provided for in the first paragraph shall list exhaustively the categories of professional counterparties, as well as the categories of business relationships or transactions, to which these specific terms for the identification and verification of the identity of customers' agents may be applied.

## Art. 14

Obliged financial institutions which make use of the derogation provided for in Article 31 of the Law and verify the identity of persons referred to in Articles 21 to 24 of the Law in the course of the business relationship shall determine, in their internal procedures, appropriate measures guaranteeing that the conditions set out in the above-mentioned Article 31 are met.



# Explanatory Memorandum to the Anti-Money-Laundering Law of 18 September 2017 - Articles 26 to 29

## Art. 26

Article 26 of the draft Law refers to the information to gather to meet the obligation of identifying the persons referred to in Articles 21 to 24 (i.e. the clients, authorised agents, beneficial owners and beneficiaries of life insurance contracts). We note that the identification data listed in the Law of 11 January 1993 had to be obtained whatever the level of risk of the situation concerned. This “rule-based” approach is from now on replaced by a “risk-based” approach by virtue of which the obliged entities must adapt the identification they gather to the ML/TF risk they identify.

To this end, Article 26 reads as follows:

- Article 26, § 1 specifies that the aim of the identification obligation is to be able to distinguish, with reasonable certainty, the person or the legal arrangement identified from any other person or legal arrangement. This specification is important. If the obliged entities from now on adapt the information they gather based on the risk identified, the information gathered in this way must allow the above aim to be achieved in all circumstances.
- Article 26, § 2, lists the information to be gathered in the case in which the individual risk assessment shows a standard ML/TF risk.
- Paragraphs 3 and 4 of this article specify that in the case in which the individual risk assessment shows a lower or higher ML/TF risk than standard, the obliged entity may or must, whichever applies, adapt the amount of information to be obtained, with the proviso that it must always enable the aim reminded of above to be achieved.

We underline that Article 26 does not specify the source of the information to be gathered. It is not required to be gathered from an independent source, meaning that it can be gathered directly from the person to be identified or from another source. This distinguishes the obligation of identification from the obligation of verification of identity (cf. Article 27).

In the case in which the individual risk assessment shows a standard ML/TF risk, Article 26, § 2 essentially takes over the list of information currently required pursuant to the Law of 11 January 1993. However, for more clarity, Article 26, § 2 restructures the way of presenting the information to be gathered for identification. In fact, this information essentially varies based on whether the obligation of identification relates to a natural person, a legal person or a legal arrangement such as a trust, a *fiducie*, or any other similar construction. Whether it is a case of identifying a client, an authorised agent or a beneficial owner is only of minor importance. However, the Law of 11 January 1993 gave the wrong impression that the information varied based on the capacity (client, authorised agent or beneficial owner) in which the person or legal arrangement was identified.

Article 26, § 2, first paragraph, therefore from now on distinguishes the information to be gathered based on whether the identification relates to: a natural person (Article 26, § 2, first paragraph, 1°), a legal person (Article 26, § 2, first paragraph, 2°), or a trust, a *fiducie* or a similar legal arrangement (Article 26, § 2, first paragraph, 3°).

a) Paragraph 2, first paragraph, 1°, refers to the case in which the identification relates to a natural person, whether this person is identified in the capacity of a client, authorised agent, or beneficial owner. It is in fact recalled that, by definition, the beneficial owners are always natural persons (cf. Article 4, 27°). Also by way of reminder, in the very specific case in which the beneficiary of a life insurance contract is to be identified, the information to be collected is described in Article 26, § 2, 4°.

The general definition essentially takes over the one provided in Article 7, § 1, second paragraph of the Law of 11 January 1993, subject to the following: It puts forward the principle that, where the identification relates to a natural person, it is necessary to obtain his/her surname, first name, place and date of birth and address. It should be noted that, just as in the Law of 11 January 1993, the address remains an item that should be obtained "if possible". This specification enables the "address" to be distinguished from the items that must be obtained as an obligation of result. As regards the address, this is often a volatile piece of information, and sometimes difficult to verify, as it is not always mentioned on supporting documents. However, although this information can contribute to distinguishing the person to be identified from any other, it is also very useful for the CTIF-CFI from an operational point of view. In fact, thanks to an address, even a fictional one, the CTIF-CFI is able to investigate and establish links between persons who belong to the same criminal network. This is an essential investigation criterion. A false address is an indication that the customer wishes to hide something. The experience of the CTIF-CFI has already shown on several occasions that persons who apparently have nothing in common may reside at the same address, which could be the first indication of belonging to criminal - and especially terrorist - networks. This is why, other than the identification and the verification of the surname, name, and place and date of birth, it is also necessary to know, if possible, the customer's address.

b) Paragraph 2, first paragraph, 2°, refers to the case in which the identification relates to a legal person. This Article does not distinguish between the legal person being identified as a customer or beneficial owner (by definition a beneficial owner is never a legal person) and takes over Article 7, § 1, paragraph 4 of the Law of 11 January 1993.

It sets out the principle that, where the obligation of identification relates to a legal person, it is necessary to obtain the registered name, registered office, the list of directors and the provisions governing the power to bind the legal person.

c) Paragraph 2, first paragraph, 3° refers to the case in which the obligation of identification relates to a trust, a fiducie or a similar legal arrangement (i.e. an entity with no legal personality), without distinguishing whether this legal arrangement is identified as a customer or an authorised agent (by definition, a beneficial owner is never a legal arrangement such as a trust or *fiducie*). Article 26, § 2, first paragraph, 3° sets out the principle by which, where the obligation of identification relates to a trust, a *fiducie* or a similar legal arrangement, it is necessary to obtain its name, the information referred to in 1° or 2° regarding its trustees or fiduciaries, its founders and where applicable its/their protectors (in the sense of the law that applies to the trust concerned), as well as the provisions governing the power to make binding agreements on behalf of the trust, *fiducie*, or similar legal arrangement. It should be noted that the identification of the trustees, of the founder of the trust and where applicable, of the protector was not expressly required by the Law of 11 January 1993. It is however necessary to guarantee effective identification of a trust.

The general rules as regards the identification data to be gathered which are listed in Article 26, § 2, first paragraph, are however subject to the following derogations, stated in paragraphs 2 and 3:

a) Where the identification obligation pertains to a natural person, the general rule described below is attenuated to the extent that, as provided for by Article 8, § 1, fourth paragraph of the Law of 11 January 1993, the identification of his/her location and date of birth is only required if possible (Article 26, § 2, second paragraph, 1°);

b) where the natural persons to be identified are the beneficiaries of an (international) non-profit organisation, a foundation, a trust, a fiducie or a similar legal arrangement which designates them based on their special characteristics or on the fact that they belong to a specific category, the information referred to in the first paragraph (the surname, first name, place and date of birth and address) is not available when entering into the relationship or realising the transaction. The fact that the natural persons who will be the beneficiaries will only be identifiable later on means that it is sufficient to initially gather the information on "the characteristics or category of beneficiaries concerned" in order to ensure that they are able to be identified at the time of the exercise of their vested rights or at the time of the pay-out. Gathering sufficient information on the "characteristics or category concerned" implies at least being able to specifically define, even if *in abstracto*, the "group" or category concerned.

This would, for example, be the case in the situation in which an obliged entity enters into a business relationship with a trust, the beneficiaries or which would be defined as persons benefiting, on the occurrence of a future event, from the assistance of such a charitable organisation. In this case, the obliged entity will have to identify the customer, i.e. the trust (see Article 26, § 2, first paragraph, 3°), and the beneficial owner(s) of the customer. In the example below, if the persons who will benefit from the assets of the trust are already identifiable, each of these persons will have to be identified in their capacity of beneficial owner. If this is not the case, the obliged entity must have full knowledge of the characteristics, *in abstracto*, of the persons who will later on benefit from the assets of the trust so that this information can be taken into consideration for exercising ongoing due diligence on the business relationship with the customer.

This draft Article 26, § 2, second paragraph, 2° transposes Article 13, § 6 of the Directive and takes over the philosophy of the last phrase of Article 8, § 1, fourth paragraph of the Law of 11 January 1993 which refers to § 1, third paragraph, 2°, b) of the same Article. In this respect, we point out that:

- For more clarity, the new draft provision uses the same terminology as Article 13, § 6 of the Directive and therefore refers to the case in which the beneficiaries are designated by “a specific category or characteristics”. The cases referred to by this include those described in Article 8, § 1, third paragraph, 2°, b) of the Law of 11 January 1993 in which the beneficiaries are natural persons not yet individually designated but are identifiable by the fact that they belong to a “group of persons”.
- Just as in Article 8, § 1, fourth paragraph, last sentence of the Law of 11 January 1993, the new provision extends to foundations and non-profit organisations.

c) The third paragraph of Article 26, § 2, derogated from the first paragraph where the obligation of identification relates to the beneficiary of a life insurance contract, whether this is a natural person, a legal person, a trust, a *fiducie* or a similar legal arrangement. In this case, the information to be obtained is less important than the information that needs to be gathered when it is for the purpose of identifying the customer, an authorised agent or a beneficial owner. When entering into a business relationship or carrying out an occasional transaction, the information referred to in the first paragraph is not always available.

Article 26, § 2, third paragraph distinguishes between two situations. In the first, the beneficiary is designated by name. In this case, it suffices to obtain the name and surname (if it is a natural person) or the name (if it is a legal person, trust, a *fiducie* or a similar legal arrangement). In the second situation, the beneficiary is designated by characteristics, category or other means. In this case, the obliged entity must obtain sufficient information on the characteristics, categories or other means of identification to have the assurance of being able to establish the identity of this/these beneficiary/beneficiaries at the time of paying out the benefits.

This provision transposes Article 13, § 5, first paragraph of the Directive.

Article 26, § 3 refers to the case in which the individual risk assessment shows that the ML/TF risk associated with the customer is low. In such a case, the obliged entity may (but does not have to) decide that some information referred to in § 2 does not need to be obtained. By way of reminder, § 2 refers to the information to be obtained in the case of a standard ML/TF risk. The information gathered pursuant to § 3 must however remain sufficient to be able, with reasonable certainty, to distinguish the person concerned from any other person.

As an example, where the obligation of identification relates to a natural person and the risk is low, the entity may not be able to gather information on his/her address or place and date of birth; however, it is ruled out that it may refuse to gather the information on his/her name and surname as this information is indispensable to identify the customer.

Article 26, § 4 refers to the case in which the individual risk assessment shows that the ML/TF risk associated with the customer is high. In such a case, the obliged entity must ensure, with heightened attention, that the information it gathers in application of § 2 enables it to indisputably distinguish the person concerned from any other. If necessary, it must gather additional information to this end.

## Art. 27

The Law of 11 January 1993 does not specify how the obligation to verify the identity of a person is distinguished from the obligation to identify, meaning that in practice, these two obligations are often confused with each other. This very often culminates in obliged entities meeting these two obligations at the same time. However, these have different aims and objectives. In order to distinguish them more clearly, the draft Law devotes two different Articles to them. After having detailed the obligation of identification (Article 26), it then attempts to clarify, in Article 27, that the obligation of verification consists of checking all or some of the identification data gathered as part of the obligation of identification against one or more supporting documents or reliable and independent sources of information in order to confirm that these data correspond with reality.

The obligation of verification is subject, just like the other obligations of due diligence, to a risk-based approach. The identification data that are verified and the measures taken to conduct this verification are therefore based on the risk identified.

It should however be underlined that the level of risk associated with a customer must be determined, both for the obligation of identification and for the obligation of verification of the identity, based on the individual risk assessment referred to in Article 19, § 2, first paragraph. The same risk assessment associated with the customer therefore simultaneously determines the extent of one and the other of these two obligations, the execution of which is generally simultaneous. The same customer may therefore not be considered "low risk" from the identification and "high risk" from the verification of identity.

In order to introduce the risk-based approach in terms of verification of the identity of customers, beneficial owners or beneficiaries of life insurance contracts, draft article 27 states the following, based on a structure parallel to that of Article 26:

- Paragraph 1 reminds that the verification carried out must be proportionate to the risk identified and specifies that the aim of the verification is to have a sufficient degree of certainty that they know the persons concerned. The actual wording of this aim in the draft Law is important. If the obliged entities must from now on adapt the information they verify based on the risk, the verification made in this way must allow the aim above to be achieved in all circumstances.
- Paragraph 2 provides that where the individual risk assessment shows a standard ML/TF risk, all the information gathered in application of Article 26 must be subjected to one or more supporting documents or reliable and independent sources of information that confirm it.
- Paragraphs 3 and 4 of this Article specify that in the case in which the individual risk assessment shows a lower or higher ML/TF risk than standard, the obliged entity may, or, where applicable, must adapt the number of identification information to be verified, with the proviso that the verification conducted in this way must in all cases allow a sufficient degree of certainty that the persons identified are actually known.

More specifically:

- where the level of risk is low, other than the obliged entity being allowed to reduce the amount of information it gathers to identify the customer (cf. Article 26, § 3, above), it may decide to reduce the verification tasks to that of the information it has effectively gathered that it deemed necessary to verify to sufficiently confirm the identity of the person or the legal arrangement;
- where the level of risk is high, the obliged entity increases as needed the amount of identification information it gathers (cf. Article 26, § 4 above) and must furthermore:
  - verify all the information it has obtained (including the additional information gathered), and
  - pay heightened attention to the validity of the documents used for verification.

## Art. 28

Article 28 of the draft Law essentially takes over the provisions of Article 16, § 3 of the Law of 11 January 1993 which attributes the obliged entities referred to in Article 5, § 1 of the draft Law an indirect right of access to the national register of natural persons solely for the aim of meeting two of their obligations provided for by the present draft Law, and which are listed exhaustively by the present provision, i.e.:

- their obligation to verify the identity of their customers, the authorised agents of their customers or their beneficial owners, and
- their obligation to keep updated the identification data they hold concerning the same persons.

Moreover, just as provided for by the Law of 11 January 1993, indirect access to the data from the national register is exclusively granted when the person whose identification data must be verified and/or updated is not present at the time of this verification or this update, meaning that the obliged entity may not resort to consulting the ID card of the person concerned.

With a view to there being equal treatment of obliged entities and with the aim of promoting effective exercise of the obligation of due diligence provided for by the present draft Law by all the categories of obliged entities, the *ratione personae* scope of this provision extends to all these categories.

As provided for in Article 16, § 3 of the Law of 11 January 1993, the obliged entities are not attributed the right to directly access the data in the national register but rather to do so indirectly through their professional associations. They do not however acquire the right to consult the national register on their own initiative but rather only at the request of an obliged entity. The professional association must ensure, when such a request is addressed to it, that all the conditions for access to the data in the national register are fulfilled before following up this request. Given the important role of the professional associations concerned, they only receive this access insofar as they are designated by the King for this end. Contrary to the Law of 11 January 1993, this Article of the draft Law moreover expressly lists the conditions that the professional association must fulfil to be able to be designated by the King (see § 3 below).

It should be underlined that this mechanism of indirect access to the national register for the reasons and under the conditions described above was covered in opinion No 16/2008 of 9 April 2008 of the Privacy Commission. Pursuant to the request for an opinion as part of the work for the Law of 18 January 2010 amending the Law of 11 January 1993 on preventing use of the financial system for purposes of money laundering and terrorism financing, and the Company Code, the Commission issued a favourable opinion, albeit recommending:

- to limit the access to situations in which the identity of the person concerned is unable to be verified using a supporting document produced by the person himself/herself,
- to limit this access to the identification data required by law (name, surname, date and place of birth and address),
- not to authorise periodic and systematic recourse to the national register for to update identification data of all the customers, authorised agents, and beneficial owners,
- and to grant access to the national register indirectly to financial undertakings, via, for example, their professional associations.

All of these recommendations are met by the present article of the draft Law.

In these conditions, the professional associations designated by the King are authorised to use the identification number of the natural person from the national register that features in the request from the obliged entity, to access the data from the national register of natural persons, to take a paper or electronic copy of the information consulted, and to communicate to the obliged entity that made the request the information necessary to execute their obligations are listed above.

As already decided by the professional associations for the financial and insurance sector for the implementation of Article 16, § 3, of the Law of 11 January 1993, the professional associations may assume their role of intermediaries between the obliged entities and the national register by creating one or several specialised institutions for this purpose. Moreover, nothing prevents these from being simultaneously tasked with the same role of intermediary for the implementation of similar provisions provided by other legislation. However, these must be associations with a legal personality, with registered office and general management based in Belgium, and which are exclusively held by the professional association(s) which created them or by obliged entities which are members of these professional associations.

Where an obliged entity receives the information consulted in the national register in the conditions and based on the methods described above, draft Article 28, § 2 authorises it to process it, keep it and take a paper and electronic copy thereof. However, because the request to consult the national register is only allowed to fulfil the obligation of verifying the identity of the natural person concerned or update the identification data of this person in application of the present draft Law, the use of the data received in response to this request is subject to the same restriction in terms of purpose. Any other use of these data is henceforth prohibited.

Paragraph 3 of this draft Article gives a non-exhaustive list of certain conditions that the professional associations need to meet to be able to be designated by the King, in accordance with § 1, in order to exercise the function of intermediary between the obliged entities and the national register. These conditions are worded in very general

terms to allow the King to assess the qualities required from these professional associations, all the while providing a framework for the power of designation by indicating the nature of the criteria to take into consideration (especially their representation of the obliged entities, their continuity, their governance and their organisation or, where applicable that of the institution they create to take on the role of intermediary).

## Art. 29

The central register of beneficial owners created by Article 73 of this draft Law, as well as the equivalent registers held in other Member States or third countries have the particular purpose of assisting the obliged entities with the exercise of their duty of identification of the beneficial owners of their customers, of their customers' authorised agents or of the beneficiaries of life insurance contracts. It should be emphasised however that based essentially on declarations by legal persons or representatives of legal arrangements covered by these registers, the exactitude and completeness of the information registered therein cannot be fully guaranteed. A fortiori, because these registers are based essentially on the declarations of customers, authorised agents, or beneficiaries of life insurance of which the obliged entities have to identify and verify the identity of the beneficial owners, these registers do not fully fit in with the notion of "independent source of information" enabling full and complete verification within the meaning of Article 27, § 1 of the draft law. These are the reasons why its Article 29, which transposes Article 30, § 8 and 31, § 6 of the Directive, imposes that obliged entities which call on these registers to identify and verify the identity of beneficial owners must adopt additional measures to identify and verify the identity of these persons, and to determine the measures that they take to this end based on their assessment of the risk associated with the customer concerned.

# Object of the identification and identity verification: Comments and recommendations

Home > Financial oversight > Combating money laundering and the financing of terrori...

## Contents

- Introduction: the risk-based approach in performing the obligations to identify and verify the identity of the persons involved in a business relationship or occasional transaction
- 1. Objectives of the obligations to identify and verify the identity of the persons involved
- 2. Cases of “standard risk”
- 3. Cases of “high risk”
- 4. Cases of “low risk”
- 5. Update of the identification and verification of the identity of the persons involved
- 6. Inability to fulfil the obligations to identify and verify the identity of the persons involved

---

## Introduction: the risk-based approach in performing the obligations to identify and verify the identity of the persons involved in a business relationship or occasional transaction

The previous AML/CFT regulations detailed the manner in which the obligations to identify and verify the identity of customers, agents and beneficial owners should be performed, without requiring that the level of ML/FT risk associated with the business relationship or occasional transaction concerned be taken into account. By contrast, the Anti-Money Laundering Law extends the principles of the risk-based approach to all due diligence obligations, including the obligation to identify and verify the identity of the persons involved. Articles 26 and 27 of the Law (i) define the objectives to be achieved when performing these obligations, (ii) establish the level of requirements in cases of “standard risk”, (iii) require these requirements to be strengthened in high-risk situations and (iv) allow them to be relaxed in low-risk situations. However, the exemption from the identification and identity verification obligations in certain cases (when the customer or his beneficial owner is a Belgian or European financial institution, a public authority, etc.), which was previously set out in Article 11 of the Law of 11 January 1993, has been removed as this legal presumption of low risk is contrary to the risk-based approach. It should also be noted that neither the Anti-Money Laundering Law nor the Anti-Money Laundering Regulation of the NBB lists the supporting documents or the reliable and independent sources of information that can or should be used to fulfil the obligation to verify the identity of the persons involved.

Consequently, **each obliged financial institution** is required to incorporate in its ML/FT risk management policy an **appropriate reference framework** for the application of the risk-based approach implemented by it with regard to the identification and verification of the identity of the persons involved. This reference framework should be established taking full account of the financial institution’s overall risk analysis and risk classification. This framework should subsequently serve as the basis for the establishment of the financial institution’s internal procedures on the subject.

For this purpose, as noted on the page “Policies, procedures, processes and internal control measures”, the NBB recommends that the procedure relating to the customer and transaction due diligence measures (the part on “identification and verification of the identity of customers, agents and beneficial owners”) include a **correlation table of the supporting documents accepted for each risk class**, as well as a **list of the circumstances in which certain supporting documents need not be submitted**.

As regards the latter point, documents with low probative value could for instance be accepted if one of the following **ML/FT risk reducing measures** applies in the context of a business relationship posing a low ML/FT risk:

- excluding any transaction involving the handling of cash,
- excluding cross-border transfers of funds
- only authorising flows of funds to or from a single account opened in the name of the same customer with a Belgian or European credit institution,
- capping the amount of the flows of funds authorised per period of time and/or per transaction,
- significantly limiting the offer of payment instruments linked to the account,
- etc.

Additionally, the **legislation on basic banking services** also provides for restrictive measures (Chapter 8 of Title 3 of Book VII of the Code of Economic Law).

It should also be recalled that, pursuant to Article 17, paragraph 2, of the Anti-Money Laundering Law, financial institutions should be able to **demonstrate to the NBB** that their reference framework and the procedures established on that basis are appropriate in view of the ML/FT risk identified through their overall risk assessments. In this respect, see the page “Policies, procedures, processes and internal control measures”. Moreover, in accordance with Article 19, § 2, paragraph 3, of the Anti-Money Laundering Law, financial institutions should be able to demonstrate to the NBB that the due diligence measures effectively implemented, by applying these procedures, in the context of each of their business relationships with customers or each of the occasional transactions they perform for them are appropriate in view of the ML/FT risk identified through the individual risk assessment.

The NBB considers that the internal procedures based on this reference framework should be binding for the entire staff of the financial institution, regardless of whether they are employees, agents or distributors. It follows in particular that, without prejudice to the consequences of a reclassification justified on the basis of the individual risk assessment, the obligations to identify and verify the identity of the persons involved **may in no way be relaxed** in individual cases because of low ML/FT risk **if the extent and the terms of this relaxation are not authorised and specified in the internal procedures**.

## 1. Objectives of the obligations to identify and verify the identity of the persons involved

It should be recalled, in accordance with Articles 26, § 1, and 27, § 1, of the Anti-Money Laundering Law, that fulfilling the obligations to identify and verify the identity of the persons involved requires (i) collecting relevant information on these persons that enables them to be distinguished from any other person with reasonable certainty, as well as (ii) checking all or part of the identification data collected against one or more supporting documents or reliable and independent sources of information which enable this data to be confirmed, in order to have a sufficient degree of certainty regarding the identity of the persons involved.

These objectives should be pursued regardless of the level of ML/FT risk associated with the business relationship or transaction concerned, but the degree of certainty to be achieved is determined according to the risk level assigned on the basis of the individual risk assessment.

## 2. Cases of “standard risk”

### 2.1. Notion of “standard risk”

“Standard risk” here refers to all situations that are not recognised as presenting a high risk in the context of the

individual risk assessment referred to in Article 19, § 2, of the Anti-Money Laundering Law.

Situations that only present a low ML/FT risk can only be excluded from the notion of “standard risk” if they have been specifically identified as low-risk situations by the overall risk assessment referred to in Article 16 of the Anti-Money Laundering Law and if the financial institution’s internal AML/CFTP procedures explicitly specify the relaxed due diligence measures that can be applied when the individual risk assessment leads to the conclusion that the risk level is low.

## 2.2 Identification data

For the list of the data to be collected on the person concerned for the purposes of his identification, see Article 26, § 2, of the Anti-Money Laundering Law.

The identification data relating to the **address** of natural persons and to the place and date of birth of beneficial owners need only be collected “to the extent possible”. The NBB considers that each financial institution’s internal AML/CFT procedures should specify the measures to be taken by its staff when data cannot be collected using regular data collection measures, in order to be able to document, where appropriate, the inability to include the data in the identification of the person concerned.

It should also be stressed that the European Regulation on transfers of funds (Article 4(1)) requires transfers of funds to be accompanied by specific identification information, namely (i) the payer’s name, (ii) the payer’s payment account number, and (iii) one of the following additional information elements: the payer’s address, official personal document number, customer identification number or date and place of birth. For further information, see the page “Transfers of funds”.

## 2.3. Identity verification

### 2.3.1. Identification data to be verified

In accordance with Article 27, § 2, of the Anti-Money Laundering Law, all identification data collected on the person concerned should be checked against supporting documents or reliable and independent sources of information to confirm their accuracy.

It should also be noted that the European Regulation on transfers of funds requires the customer’s address or date and place of birth, if the payment service of the payer chooses this information to accompany a transfer of funds (see Article 4(1) of the aforementioned Regulation and point 2.2 above), to be verified by the payment service of the payer before being sent together with the funds to the payment service of the payee, in the same way as the payer’s last name, first name and account number (see Article 4(4) of the aforementioned Regulation). However, if this identification information has already been verified in the context of the due diligence obligations pursuant to Article 27, § 2, of the Law (e.g. at the start of the business relationship) and if the information obtained during this verification has been kept in accordance with legal requirements (see the page “Retention and protection of data and documents”) and updated in accordance with the legal obligations (see point 5 below), it is not necessary to verify this information again for every transfer of funds (Article 4(5) of the aforementioned Regulation). On the other hand, if the customer’s last and first name, account number, address or date and place of birth have not been verified before the transfer of funds (e.g. if this information has not been verified at the start of the business relationship because it was considered to pose low ML/FT risk), it should therefore, like all other identification information, be verified before being sent with the transfer of funds concerned. For further information, see the page “Transfers of funds”.

### 2.3.2. Supporting documents and reliable and independent sources of information

Neither the Anti-Money Laundering Law nor the Anti-Money Laundering Regulation of the NBB lists the supporting documents or the reliable sources of information that may be used to verify the identification data of the person concerned. **Consequently, each financial institution should include this list in its internal procedures** relating to the identification and verification of the identity of the persons concerned.

This list should be based on an assessment of the level of reliability of each supporting document or source of information, to ensure that this level is sufficient to achieve the objective set out in Article 27, § 1, of the Anti-Money Laundering Law. Where appropriate, the level of reliability required may be the result of the combined use of two or more supporting documents. For example, the NBB does not consider the identification data accompanying an

**initial transfer of funds** carried out from a bank account opened in the name of the same person with another credit institution to be a “supporting document or reliable source of information” as such that can be sufficient to fulfil the obligation to verify the customer’s identity. However, verifying identification data through the information accompanying such an initial transfer of funds can be useful to corroborate the result of the verification of this data through another supporting document or source of information and thus increase the level of reliability of the verification performed.

As regards **address verification**, the NBB considers that financial institutions’ internal procedures should determine the measures to be taken to fulfil this legal obligation in a sufficiently precise manner. When the supporting document used to verify the customer’s identity provides relevant information on the customer’s address, this document should logically also be considered as the source of relevant information on his address. When this is not possible (in particular if the supporting document does not mention the customer’s address), the internal procedures should determine how this information can be obtained. In these cases, a simple declaration signed by the customer, agent or beneficial owner concerning his address generally suffices if the customer, business relationship or transaction does not present a high ML/FT risk.

Additionally, the NBB recommends taking into account the remarks below.

### **a) Verification of the identity of natural persons**

#### **§ 1. Identity card and passport**

If the person to be identified is a natural person subject to a face-to-face identification, the NBB recommends that his identity generally be verified using his valid official identity documents such as his identity card or, where appropriate, his passport. It should be noted that these supporting documents should include a photograph of their legitimate holder and thus enable a visual check to reduce the risk of identity theft.

This measure appears particularly relevant for persons domiciled in Belgium that are holders of an identity card issued by the Belgian authorities. In case of doubt regarding the legitimacy of an identity card presented, it is however recommended to verify that it has not been registered as stolen or lost in the ad hoc database of the FPS Home Affairs (see <https://www.checkdoc.be>).

When financial institutions verify the customer’s identity by electronically reading the data registered on the microprocessor of his identity card, there should also be a simultaneous electronic verification to ensure that the data included on the chip was signed electronically by the National Register. In this respect, it is recommended to design the IT procedures in such a way that this verification takes place systematically and automatically without requiring the employee or agent who performs the identification to intervene and without enabling him to deactivate this check. To detect potential falsifications, it could moreover be useful to check the compliance of the data registered on the chip with the data legible on the identity card. Finally, it should be ensured that the certificate has not been revoked by the National Register.

If the verification is carried out through the customer’s passport, appropriate measures should be prescribed to ensure that this document meets the specifications for passports issued by the foreign country concerned. There should also be a check which allows to conclude reasonably that the passport presented has not been forged or falsified.

Identification data can also be verified remotely through the information registered on the microprocessor of the Belgian electronic identity card. However, it should be noted that this verification may be less reliable than a face-to-face verification as it does not allow for a visual check using the photograph included in the supporting document to ensure that the person using it is indeed its legitimate holder. It could therefore be necessary to systematically verify the legitimacy of the document presented by consulting <https://www.checkdoc.be>. Furthermore, a financial institution using this method of verifying the identity of the persons involved should implement measures that enable it to ensure that the objective set out in Article 27, § 1, of the Anti-Money Laundering Law will be met notwithstanding the lack of a visual check, where appropriate by implementing an additional verification measure.

#### **§ 2. Other official documents**

In specific cases listed in the internal procedures, for example when awaiting the issuance of the customer’s identity card or passport, other documents issued by Belgian or foreign authorities can be accepted as supporting documents until the verification can subsequently be performed using the customer’s identity card.

If the customer is a child below the age of 12 who is not yet required to hold an identity card ("Kids ID"), and until his identity can be verified upon his 12th birthday using his identity card, which he will receive at that time, the use of other official documents is recommended, such as his certificate of registration in the population register of his place of residence, a copy of his birth certificate or his parents' marriage certificate.

The identity of foreign nationals residing in Belgium who do not hold an identity card or a passport may be verified in a valid manner using the document issued to them by Belgian authorities according to their status on Belgian territory, particularly their certificate of registration in the register of foreigners and the other documents included in the annexes to the Royal Decree of 8 October 1981 on access to the territory, residence, settlement and removal of foreign nationals. It should be noted in this regard that, although a residence permit issued by the Belgian State can be considered sufficient, the other documents referred to in the Annexes to the Royal Decree of 8 October 1981 on access to the territory, residence, settlement and removal of foreign nationals could be considered less reliable. Such documents cannot be accepted as supporting documents in standard-risk situations unless they are corroborated by other supporting documents, without prejudice to the measures governing the business relationship or transaction based on which they can be considered to pose a low risk (see below).

§ 3. The "electronic identification means" within the meaning of Regulation (EU) No 910/2014 of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market

Taking into account the provisions of Regulation (EU) No 910/2014 of 23 July 2014 and of Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of the aforementioned Regulation (EU) No 910/2014, financial institutions can, in standard-risk situations, verify the identity of the persons concerned using electronic identification means referred to in these European regulations. Institutions that authorise the use of these instruments are required to fix the terms and conditions for their use based on an analysis of the level of reliability of these instruments with regard to the objective set out in Article 27, § 1, of the Anti-Money Laundering Law, taking particular account of the conditions relating to the identification of the person concerned upon the creation of the electronic identification means, of the specific qualities of the service provider who issued the electronic instrument concerned, of the instrument's "assurance level" and of any other relevant element.

§ 4. Use of other innovative technological instruments

If a financial institution intends to make use of innovative technology to verify the identity of the persons involved in business relationships or occasional transactions, it is required to comply with Article 12, 1°, paragraph 2, of the Anti-Money Laundering Regulation of the NBB, which stipulates that the acceptance of new technologies as instruments for verifying the identity of these persons must be based on a prior analysis conducted by the financial institution itself of the reliability of these new instruments with regard to the objective set out in Article 27, § 1, of the Anti-Money Laundering Law. The NBB expects this analysis to be correctly documented and retained so that it can be transmitted to it at its request.

The NBB moreover recommends taking full account of the Opinion of the ESAs dated 23 January 2018 on the use of innovative solutions.

§ 5. Copies of supporting documents and consultation of the National Register

A photocopy or electronic image of a supporting document (particularly the identity card or passport) of the person concerned is obviously not as reliable as the original supporting document itself and therefore cannot be accepted as such as a sufficiently reliable supporting document in standard-risk situations.

However, by producing both a simple copy or electronic image of the identity card or passport of the person concerned and another supporting document, the reliability of the verification could be increased. In that case, the financial institution providing for such a dual method for verifying the identity of the persons concerned should be able to demonstrate that it has obtained an adequate overall level of reliability of the verification in this manner.

Furthermore, Article 28 of the Anti-Money Laundering Law grants financial institutions the right to indirectly access the National Register to corroborate a copy of a supporting document and to verify the identity of the persons concerned (i.e. customers, their agents and their beneficial owners) where these persons are not physically present during their identification. This is the case when establishing business relationships with or carrying out transactions for a customer remotely, when identifying and verifying the customer's beneficial owners or when updating the identification data of customers or beneficial owners that are not present at the time of the update.

However, it should be noted in these situations that, if there is no visual contact with the person providing the copy of the supporting document, the financial institution cannot use the photograph included in the supporting document to ensure that the person using it is its legitimate holder. As is the case when an electronic identity card is used to remotely verify the identity of a person involved, a financial institution providing for the verification of the identity of persons involved through a copy of a supporting document that is corroborated by consulting the National Register, should ensure and be able to demonstrate that the objective set out in Article 27, § 1, of the Anti-Money Laundering Law is nevertheless met or should, where appropriate, require the application of an additional verification measure to reach the level of reliability required.

The access to data from the National Register granted by the Law to financial institutions is indirect and requires the involvement of the professional associations designated by the King or of the institutions created by them for that purpose. The aim of the parallelism with the legal provisions on dormant accounts, safe deposit boxes and insurance contracts is to provide financial institutions with the same tools and procedures as those implemented by the professional associations in order to allow them to fulfil their obligations regardless of the legislative context.

It should however be stressed that the data that can be consulted in the National Register, can differ depending on the legislation. This procedure for consulting data in the National Register can only be used in the aforementioned circumstances for the verification of identification data required by or pursuant to the Anti-Money Laundering Law. Furthermore, the indirect access to the data of the National Register to verify the identity of customers or their agents or beneficial owners in accordance with the Anti-Money Laundering Law remains otherwise subject to the provisions of the Law of 8 August 1983 establishing a National Register of natural persons and to the General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC). For these legislations to be implemented correctly, please refer to the relevant decisions, opinions and recommendations from the Commission for the Protection of Privacy (CPP). It should be stressed, in particular, that the CCP deems it preferable, whenever possible, to perform the remote identity check by using the functions of the electronic identity card rather than by consulting the National Register.

#### § 6. Consultation of the register of beneficial owners

Article 73 et seq. of the Anti-Money Laundering Law create a central register of beneficial owners (the "UBO register") with the aim of providing useful assistance to the different AML/CFT stakeholders, including the obliged entities, for the identification and the verification of the identity of the beneficial owners of companies and legal arrangements. However, it should be noted that Article 29 of the Anti-Money Laundering Law does not allow obliged entities to rely solely on the consultation of this register to identify and verify the identity of beneficial owners, but requires them to take additional measures to corroborate the data obtained by consulting the register. In standard-risk situations, the NBB recommends that these additional measures at least include obtaining supporting documents from the customer regarding the identity of his beneficial owners and/or consulting information published on the internet or any other publicly available information.

#### **b) Verification of the identity of companies and legal persons**

In standard-risk situations, the NBB generally recommends verifying the identification data of companies and legal arrangements governed by Belgian law using documents that are generally accepted in Belgian law as proof of their existence, such as the latest coordinated statutes or the updated statutes of the company or legal person that have been lodged with the Commercial Court or published in the annexes of the Belgian Official Gazette.

As regards the list of directors of companies and legal persons governed by Belgian Law, financial institutions should make use of the publication of their appointment in the Belgian Official Gazette. Other documents can also be accepted, such as the publication in the Belgian Official Gazette of notarial deeds in which these persons are mentioned as directors, or the annual accounts filed with the NBB.

The provisions governing the power to make binding agreements on behalf of the company or legal person governed by Belgian law should be established using the latest publication of the representational powers of this company or legal person in the Belgian Official Gazette.

To verify the identity of companies and legal persons governed by Belgian law, financial institutions should use supporting documents equivalent to those listed above that are provided for in accordance with the national legislation applicable to these companies and legal persons. Where appropriate, these supporting documents should be completed by a reliable translation of these documents into one of the national languages or into English.

These supporting documents can be obtained from the customer himself, from official sources such as the Belgian Official Gazette or any other sources of information that can be considered reliable such as the Crossroads Bank for Enterprises established by the Law of 16 January 2003, or from other sources of the same nature created by the Member States governing the foreign companies and legal persons.

Financial institutions can also use the “electronic identification means” issued to companies and legal persons in accordance with Regulation (EU) No 910/2014 of 23 July 2014 and with Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of the aforementioned Regulation (EU) No 910/2014. As is the case for the verification of the identity of natural persons, the NBB expects institutions that authorise the use of these instruments to fix the terms and conditions for their use based on an analysis of the level of reliability of these instruments with regard to the objective set out in Article 27, § 1, of the Anti-Money Laundering Law, taking particular account of the conditions relating to the identification of the person concerned upon the creation of the electronic identification means, of the specific qualities of the service provider who issued the electronic instrument concerned, of the instrument’s “assurance level” and of any other relevant element.

### **c) Verification of the identity of legal arrangements**

Financial institutions should verify identification data of legal arrangements such as trusts using documents that have probative value in the legislation applicable to this trust or legal arrangements. The relevant rules should be specified in the financial institution’s internal procedures.

## **3. Cases of “high risk”**

### **3.1. Notion of “high risk”**

“High risk” here refers to all situations that are identified as such by the individual risk assessment required by Article 19, § 2, of the Anti-Money Laundering Law. These situations include those in which enhanced due diligence measures are required by Articles 37 to 41 of the Anti-Money Laundering Law.

### **3.2. Identification data**

Pursuant to Article 26, § 4, of the Anti-Money Laundering Law, if the individual risk assessment performed in accordance with Article 19, § 2, paragraph 1, of the Law establishes that there is a high risk associated with the customer and with the business relationship or transaction, financial institutions should take particular care to ensure that the identification data required in standard-risk situations is sufficient to distinguish, in a manner that leaves no room for doubt, the person concerned from any other person. If this is insufficiently the case, financial institutions should collect additional information to achieve the desired result.

Where the persons concerned are natural persons, the additional information to be collected may for instance pertain to their professional activity, their nationality, their gender, etc. The internal procedure could also provide for an extension of the address verification obligation by stipulating that this information, which in a standard-risk situation need only legally be collected “to the extent possible”, must be collected in all high-risk cases. The additional identification data provided for by the internal procedures could also include the expiry date of the supporting document used to verify the identity of the person concerned. It should be noted that, if the financial institution includes this information in the list of identification data required, it should update the identification and verification of the identity of the person concerned when the validity of the supporting document expires.

For legal persons, the additional identification data could include their company number or, where appropriate, their Legal Entity Identifier if they have such a unique identification code, their line of business, the number of their places of business apart from their registered office and/or the countries in which these places are established, their trade names, if any, etc.

### **3.3. Identity verification**

### 3.3.1. Identification data to be verified

Pursuant to Article 27, § 4, of the Anti-Money Laundering Law, all identification data collected should be verified using particularly reliable means of verification.

### 3.3.2. Supporting documents and reliable and independent sources of information

In high-risk situations, the internal procedures should only authorise the use of the supporting documents accepted in standard-risk situations (see above) that are deemed the most reliable or, where appropriate, require the use of a combination of these supporting documents.

When verifying the identity of natural persons, it is recommended to only use supporting documents including a photograph of the person to be identified, and to require a visual check in order to ensure that the person presenting the supporting document is its legitimate holder.

When the financial institution authorises the use of “electronic identification means” issued in accordance with European legislation on the subject (see above) in high-risk situations, the NBB expects it to tighten the terms and conditions for the application of this authorisation.

In any case, the financial institution should establish its list of supporting documents or sources of information that are accepted to verify the identity of the persons involved in high-risk situations based on a thorough analysis of the reliability of these verification tools that enables it to demonstrate that their high level of reliability is appropriate in view of the high level and the nature of the ML/FT risk incurred.

The NBB notes that it is even more important to know the customer’s address with a sufficient degree of certainty when there is a high ML/FT risk, particularly if this risk materialises. It therefore deems it necessary to implement enhanced due diligence measures to confirm the accuracy of the address provided by the customer. These measures could include sending a letter to the address specified by the customer stating that the relationship can only enter into force or the transaction can only be performed after the customer has sent back the acknowledgement of receipt attached to the letter.

## 4. Cases of “low risk”

### 4.1. Notion of “low risk”

In order to benefit from the legally authorised relaxed identification and identity verification obligations with regard to persons involved in business relationships or occasional transactions posing a low ML/FT risk, **the financial institution must choose**, in its ML/FT risk management policy, to make use of and determine the terms of this possibility in its internal procedures. Moreover, the low risk level should be duly recognised in the overall risk assessment required by Article 16 of the Anti-Money Laundering Law and, in each specific case where relaxed obligations are being considered, in the individual risk assessment required by Article 19, § 2, of the Law. In this regard, please refer to the introduction of this page for existing measures to reduce the level of ML/FT risk, particularly in the legislation on basic banking services.

### 4.2. Identification data

In accordance with Article 26, § 3, of the Anti-Money Laundering Law, financial institutions’ internal procedures may reduce the amount of identification data that should be collected for the identification of persons involved in low-risk situations compared to the data required by the Law in standard-risk situations. However, the information collected should remain sufficient to enable the person concerned to be distinguished from any other person with reasonable certainty. For instance, the last and first name of a legal person or the corporate name of a legal person cannot reasonably be considered information that need not be collected. As this identification data alone does not suffice to eliminate an increased risk of homonymy, the NBB considers that, even in situations with low ML/FT risk, financial institutions should collect at least one additional item of identification data in order to reduce this risk of homonymy. Furthermore, the NBB expects financial institutions wishing to make use of the possibility to relax the identification obligation in low-risk situations to include in their internal procedures a detailed list of identification data that should in any case be collected.

## 4.3. Identity verification

### 4.3.1. Identification data to be verified

If the individual risk assessment required by Article 19, § 2, of the Anti-Money Laundering Law shows a case of low ML/FT risk, financial institutions are authorised to verify a smaller amount of the information collected. The amount of information verified should, however, remain sufficient to enable the obliged entity to have a sufficient degree of certainty as to its knowledge of the person concerned. The NBB therefore expects financial institutions making use of the possibility to relax the obligation to verify the identity of persons involved in the business relationship or transaction, to specify in their internal procedures the information for which verification remains obligatory.

### 4.3.2. Supporting documents and reliable and independent sources of information

Naturally, all supporting documents and reliable and independent sources of information which the financial identification has identified as eligible for verifying the identity of persons involved in a standard-risk business relationship or occasional relationship (see above) are also eligible in low-risk situations.

However, if the individual ML/FT risk assessment concludes that the level of ML/FT risk is low, financial institutions may choose to accept certain documents that they consider to have insufficient probative value to be accepted in standard-risk situations and even more so in high-risk situations.

When, for example, foreign nationals are established in Belgium without having an identity card or a certificate of registration in the register of foreigners, and taking into account the need to avoid excluding persons in precarious situations on the Belgian territory from access to financial services, the NBB considers that their identity may be verified using one of the documents referred to in the different annexes to the Royal Decree of 8 October 1981 on access to the territory, residence, settlement and removal of foreign nationals, which would be considered as having low reliability, if the level of associated ML/FT risk can be reduced using appropriate measures governing the intended business relationship or transaction. In this respect, see the Opinion of the European Banking Authority (EBA) on the application of customer due diligence measures to customers who are asylum seekers from higher-risk third countries or territories (EBA-Op-2016-07) as regards the situation of asylum seekers. Although a simple copy or electronic image of a supporting document is insufficiently reliable in itself to be accepted as a supporting document in standard-risk situations without being verified through the National Register as stipulated in Article 28 of the Anti-Money Laundering Law, it could be accepted in certain circumstances as the relationship is subject to strict limitations that can drastically reduce ML/FT risk. As regards the restrictive measures to reduce the level of ML/FT risk associated with these business relationships, please refer to the introduction of this page, which states, in particular, that financial institutions are expected to include, in their procedure relating to customer and transaction due diligence measures, a correlation table of the supporting documents required for each risk class, as well as a list of the circumstances in which certain supporting documents need not be submitted.

## 5. Update of the identification and verification of the identity of the persons involved

Article 35, § 1, 2°, of the Anti-Money Laundering Law stipulates that obliged entities should update the identification data held by them, particularly in case of changes to items that are relevant to the individual risk assessment referred to in Article 19, § 2, of the Law. In this respect, see the page “Ongoing due diligence and detection of atypical transactions”.

This update requirement also implies that, in case of a transfer of funds, any identification data received and verified beforehand over the course of a business relationship should be subject to another verification for the transfer of funds concerned if any information relevant to the individual risk assessment has been modified.

## 6. Inability to fulfil the obligations to identify and verify the identity of the persons involved

Article 33 of the Anti-Money Laundering Law provides that, if obliged entities cannot fulfil their obligations to identify and verify the identity of a customer, his agents or his beneficial owners within the time limits required, they may neither establish a business relationship with or carry out a transaction for that customer. In this respect, see the page "Non-compliance with the identification and identity verification obligation".



# Time of identification and identity verification

Home > Financial oversight > Combating money laundering and the financing of terrori...

## Legal and regulatory framework

- Anti-Money Laundering Law: Articles 30 to 32
- Anti-Money Laundering Regulation of the NBB: Article 14

## Explanatory Memorandum of the Anti-Money Laundering Law

- Articles 30 to 32

## Other reference documents

- ESAs Risk Factor Guidelines dated 4 January 2018
- BCBS Guidelines dated June 2017 on Sound management of risks related to money laundering and financing of terrorism (see Annex 4)

## Comments and recommendations by the NBB

- Comments and recommendations

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



# Anti-Money Laundering Law of 18 September 2017 - Articles 30 to 32

## Art. 30

Obligated entities shall fulfil their obligations to identify and verify the identity of the customers referred to in Article 21, § 1, and of the beneficial owners referred to in Article 23, § 1, before entering into a business relationship with their customers or carrying out occasional transactions for which they are called on.

The obliged entities shall satisfy their obligations to identify and verify the identity of the customers' agents referred to in Article 22 before these agents exercise their power to make binding agreements on behalf of customers that they represent.

In the case of life insurance policies, the obliged entities shall fulfil their obligation to identify the beneficiaries referred to in Article 24 as soon as the latter have been designated or identified. They shall fulfil their obligation to verify the identity of the said beneficiaries no later than at the time of the pay-out. In the case of assignment, in whole or in part, of a life insurance policy to a third party, obliged entities aware of the assignment shall identify the beneficiary of the policy concerned at the time of the assignment to the natural or legal person or legal arrangement receiving for its own benefit the value of the policy assigned.

## Art. 31

By way of derogation from Article 30, first and second subparagraph and without prejudice to Article 37, obliged entities may, in special circumstances that are listed exhaustively in their internal procedures and if necessary so as not to interrupt the conduct of business, verify the identity of the persons referred to in Articles 21 to 24 over the course of the business relationship, if the following conditions are met:

1° the individual risk assessment conducted in accordance with Article 19, § 2, first subparagraph, shows that the business relationship poses a low ML/FT risk;

2° in accordance with Article 27, the identities of the persons concerned are verified as soon as possible after first contact with the customer.

If an obliged entity referred to in Article 5, § 1, 4° to 22°, makes use of the derogation referred to in the first subparagraph when opening an account, particularly an account that allows transactions in financial instruments, no transfers, withdrawals or deposits of funds or securities may be performed by the customer or in his name from this account to the customer or his agent before the identities of the persons referred to in Articles 21 to 24 have been verified in accordance with Articles 27 to 29.

## Art. 32

Obligated entities that issue electronic money may, based on an appropriate assessment of the ML/FT risks conducted pursuant to Article 16 that demonstrates that these risks are low, derogate from Article 30, first and second subparagraph, with regard to customers in the course of their business related to the issuance of electronic money, if all risk mitigation conditions listed in Article 25 are met.





# Explanatory Memorandum to the Anti-Money-Laundering Law of 18 September 2017 - Articles 30 to 32

## Art. 30

Article 30 of the draft Law states the general rules that determine the moment at which the obligation of identification and verification must be fulfilled. This moment differs based on the nature of the person identified (customers, authorised agents, beneficial owners and beneficiaries of life insurance policies or equivalent):

- The customers and beneficial owners must be identified and their identity verified before entering into a business relationship or carrying out the occasional transactions concerned. This transposes Article 14, § 1 of the Directive.
- The authorised agents of customers must be identified and their identity verified before they exercise the power of engaging the customers they represent. This takes over Article 7, § 2 of the Law of 11 January 1993.
- The beneficiaries of life insurance contracts must be identified as soon as they are designated or identifiable. However, the identity of the beneficiaries may be verified any time until the time of payment of benefits by the insurer. Nevertheless, in case of partial or total transfer of a life insurance policy to a third party, the obliged entities that are aware of this transfer must identify the new beneficiary of the contract concerned at the time of the transfer. This transposes Article 13, § 5, second paragraph of the Directive.

Articles 31 and 32 provide for the ability to derogate from the rules of Article 30 in the circumstances they state.

## Art. 31

Article 31, first paragraph, refers to the possibility of deferring the obligation of verification in special circumstances. Article 31, second paragraph, describes the method for this possibility when the deferral occurs at the time of opening an account.

Article 31, first paragraph, refers to the possibility for obliged entities of deferring, in circumstances described therein, the verification of the identity of the persons identified (but not the identification of these persons) on a date later than that referred to in Article 30. This possibility of derogation was already provided for financial institutions in Article 3 of the CBFA Regulation. From now on, it is extended to all obliged entities.

However, in order to avoid abuse, this possibility of deferral is in all cases subject to meeting the following conditions:

- the deferral is only authorised if authorised by the internal procedures;
- the deferral is only authorised in the special circumstances previously listed exhaustively by the obliged entity in its internal procedures, and, if necessary, in the case in point, if it does not interrupt the exercise of the activities;
- the individual risk assessment shows that the business relationship presents a low risk of ML/TF;
- the identity of the persons concerned is verified as quickly as possible after the first contact with the customer. It should be noted that by virtue of Article 37 of the draft Law, the activities exercised in relation to the customer must be subjected to enhanced due diligence until the identity of all the persons involved is

verified, so that any anomaly, including the impossibility of verifying the identity of the persons concerned by the business relationship as quickly as possible, is reported internally as referred to in Article 45.

Article 31 transposes Article 14, § 2 of the Directive. However, it should be noted that this Article 14 provides for the possibility of derogation from the moment at which the verification of the identity of customers and beneficial owners should occur, but not when it comes to the verification of the identity of authorised agents. It does however appear logical to provide so, which Article 31, first paragraph does.

Article 31, second paragraph refers to the specific case in which financial institutions use the possibility of deferring verification of the identity (referred to in the first paragraph) when opening an account. Pending this verification, no funds or securities transfers, withdrawal or remittance of funds or securities to the customer or his/her authorised agent is allowed from this account (whether by the customer or in the customer's name) before the identity of the persons that need identifying is able to be verified. Article 31, second paragraph, assumes that the conditions referred to in the first paragraph have been met. The provision also refers to all types of accounts opened by a financial institution, including securities accounts.

Article 31, second paragraph, transposes Article 14, § 3 of the Directive. It should be noted that this provision of the Directive prohibits all transactions pending the verification of the identity. However, the objective of this prohibition is to prevent customers from having access to funds or assets on their account. Nevertheless, there is no reason to prohibit funds and assets being paid into their account (meaning that, where necessary, they can be attached if it transpires that they are of illicit origin). This is the reason for which it seems preferable to specify that the prohibition affects all transfer, withdrawal or remittance transactions of funds or securities to the customer or the customer's authorised agent.

The same Article 14, § 3 of the Directive provides for Member States to have the power to derogate from the moment at which both the obligation of identification and the obligation of verification of the identity of the customer must be executed in the specific case of a financial institution opening an account (contrary to Article 14, § 2 of the Directive which only provides for the ability to derogate from the obligation of verification). The possibility of derogation from the obligation of verification for the opening of an account was already provided for in Article 3 of the CBFA Regulation and is taken over in Article 31, second paragraph of the draft Law. Just as the CBFA Regulation did not make use of the ability to derogate from the obligation of identification, Article 31 does not include it. The obligation of identification constitutes a minimum obligation, which is not very restrictive in practice, and seems indispensable to avoid accounts being opened for unknown persons. Authorising its deferral does not therefore appear justified.

## Art. 32

If their general risk assessment reveals that their activity of issuance of electronic money presents a low ML/TF risk, electronic money issuers may decide to defer the moment at which they fulfil their obligation to identify and verify the identity of customers of the electronic money issuance service (and consequently, authorised agents and beneficial owners of these latter). This possibility is subject to compliance with the risk mitigation conditions referred to in Article 25. It does of course assume that the obliged entity has not exercised the ability referred to in Article 25 of not identifying the customer of the issuance of electronic money service.

In the event of authorised deferral, the issuer of electronic money concerned should establish in its internal procedures the term within which the obligation of identification and verification of the identity must be satisfied as well as the consequences associated with not proceeding to identify and verify the identity of the customer within the established term.

Draft Article 32 transposes Article 12, § 1 of the Directive, in that it provides for the possibility of derogating from Article 14 of the Directive.

# Time of identification and identity verification: Comments and recommendations by the NBB

Home > Financial oversight > Combating money laundering and the financing of terrori...

## Contents

- 1. Time of identification and identity verification according to the category of persons to be identified
- 2. Specific derogations
- 3. Inability to identify or verify the identity of the persons involved at the required time or within the time limit set

## 1. Time of identification and identity verification according to the category of persons to be identified

Article 30 of the Anti-Money Laundering Law specifies the time at which the identification and identity verification obligations should be fulfilled, depending on the capacity of the person concerned:

- **For customers and their beneficial owners:**
  - *identification*: before entering into the business relationship or carrying out the occasional transaction concerned;
  - *identity verification*: at the same time;
- **For agents:**
  - *identification*: before exercising their power to make binding agreements on behalf of the customers that they represent;
  - *identity verification*: at the same time;
- **For beneficiaries of life insurance policies or of equivalent policies:**
  - *identification*: as soon as they have been designated or are identifiable; in case of assignment of the policy to a third party: identification of the new beneficiary at the time of the assignment;
  - *identity verification*: may be deferred until the time of pay-out by the insurer.

## 2. Specific derogations

In accordance with the risk-based approach, financial institutions may, in certain specific cases where the ML/FT risk is low, as provided for in the Anti-Money Laundering Law, derogate from the aforementioned rules and defer the fulfilment of the obligation to verify the identities of the persons involved (see point 2.1. below) and even of the obligation to identify these persons (see point 2.2. below).

### 2.1. Need to not interrupt the conduct of business

#### 2.1.1. General possibility of derogation

Pursuant to Article 31 of the Anti-Money Laundering Law, financial institutions are authorised, **when establishing a business relationship**, to defer **verification of the identity** of the customer and, where appropriate, of his agent(s) and beneficial owner(s) **until a later time** than that determined in Article 30 of the Law, **insofar as the specific situation requires not interrupting the conduct of business**.

This possibility could for example be used when, in the context of business relationships with professional customers, specific financial activities are performed that do not allow the identity of the counterparty to be fully verified before the first transactions have been carried out.

However, the performance of the identity verification during the business relationship is subject to all the following **conditions** being met:

- The individual risk assessment must show that the business relationship concerned poses a low ML/FT risk;
- In order to avoid that not verifying the identity of the persons concerned facilitates ML/FT transactions, the identity of all these persons should be verified **as soon as possible** after first contact with the customer; in the meantime, the business relationship concerned should be subject to **enhanced due diligence** (see Article 37, § 1, of the Anti-Money Laundering Law) and any anomaly in its functioning or in the verification process should be treated as an “atypical fact” and as such be the subject of a specific analysis and documented in an internal report under the responsibility of the AMLCO, to determine whether a suspicion should be reported to CTIF-CFI (see the page “Special cases of enhanced due diligence”);
- The financial institution’s internal procedures (see the page “Policies, procedures, processes and internal control measures”) should contain a precise and exhaustive enumeration of the circumstances in which this possibility may be used and of the appropriate measures guaranteeing fulfilment of the conditions above (see Article 14 of the Anti-Money Laundering Regulation of the NBB) and of the conditions required to perform the verification as soon as possible after first contact with the customer.

Generally, pending verification of the identity of the persons involved, the specific framework of the business relationship should include a set of coherent measures which drastically limit the possibilities offered to the customer in the context of this business relationship during this period. For example, it could be envisaged deferring the settlement of the transactions, limiting the sources of funding for the account opened to a single other bank account opened in name of the customer with a credit institution established in the EEA or in an equivalent third country, etc.

### 2.1.2. Specific case: opening an account

When a financial institution that has been called on to **open an account (regardless of the nature of the account concerned, which may be a securities account)** decides to make use of the possibility to defer verifying the identity of the customer and, where appropriate, of his agent(s) and beneficial owner(s) until this account has been opened, in compliance with the conditions referred to in the previous point, no transfers, withdrawals or deposits of funds or securities may be performed to the customer or his agent **from this account** (either by or on behalf of the customer) **as long as the identities of all the persons involved have not been verified**.

However, this restriction does not prevent financial institutions from, for example, making the remote opening of an account, in particular through the internet, conditional on an initial transfer by the customer from another bank account opened in his name, without waiting for his identity and that of his agents or beneficial owners to be verified.

## 2.2 Low-risk issuance of electronic money

### 2.2.1. Possibility of derogation

In accordance with Article 25 of the Anti-Money Laundering Law and provided certain conditions are met, financial institutions issuing electronic money are authorised, when the overall assessment of the ML/FT risks specifically linked to their issuance activity shows that these risks are low, to neither identify nor verify the identity of customers (and, where appropriate, their agent(s) and beneficial owner(s)) who provide them with funds for the issuance of electronic money (see the page “Persons to be identified”). Pursuant to Article 32 of the Anti-Money Laundering Law, these institutions may, a fortiori, where they have not made use of the aforementioned possibility of derogation, decide to **defer fulfilment of the obligations to identify and verify the identity** of the aforementioned persons **until a later time** than that provided for in Article 30 of the Law, provided the same conditions are met.

### 2.2.2. Conditions for application of the derogation

However, this possibility of derogation is subject to multiple **conditions. In addition to the fact that the overall risk assessment carried out by the electronic money issuer must demonstrate that the level of ML/FT risks to which he is exposed as a result of this activity is low**, the following cumulative conditions must be met:

1. the payment instrument cannot be reloaded or, if it is reloadable, it can only be used in Belgium and only to make payments up to a maximum monthly limit of EUR 250;
2. the maximum amount stored electronically does not exceed EUR 250;
3. the payment instrument is used exclusively to purchase goods or services; it follows in particular that it cannot be accepted to perform a money remittance operation;
4. the payment instrument cannot be funded with anonymous electronic money;
5. the electronic money issuer concerned carries out sufficient monitoring of the transactions or business relationship to enable the detection of unusual or suspicious transactions.

Furthermore, the NBB recommends that the electronic money issuer specify in his internal procedures within which time limit the persons involved will be identified and their identity verified, and which measures are required for this purpose.

### 2.2.3. Non-application of the derogation

Even if all the conditions listed above are met, the derogation is **not applicable** when a customer:

1. is redeemed in cash, at the monetary value of the electronic money, or
2. withdraws this value in cash,

if the amount redeemed or withdrawn, as the case may be, exceeds EUR 100.

In these two cases, where the legislator considered that the risk could not be regarded as low, the electronic money issuer is required to take appropriate measures to identify and verify the identity of the customer concerned (and, where appropriate, his agent(s) and beneficial owner(s)) **at the time of the refund or withdrawal of the electronic money** (that was previously issued without any such measures).

In the same vein, the NBB highlights the fact that, where circumstances have given rise to suspicions of ML/FT, either at the time of establishment of the business relationship with the customer or subsequently, that led the electronic money issuer to report a suspicion to CTIF-CFI and, in accordance with Article 22 of the Anti-Money Laundering Regulation of the NBB, to carry out an individual re-assessment of ML/FT risks revealing that the level of risk associated with the given situation can no longer be regarded as low (which should logically be the case - see the page "Reporting of suspicions"), the said issuer can no longer invoke the derogation provided for in Article 32 of the Law. The issuer should immediately identify and verify the identity of the customer (and, where appropriate, his agent(s) and beneficial owner(s)), in accordance with Articles 21 to 23 of the Law.

### 2.2.4. Documentation

Finally, since the above-mentioned possibility of derogation is not absolute but subject to certain limitations, the NBB recommends that the financial institutions applying the derogation be able not only to submit the overall risk assessment that establishes the low level of risk, which must be documented, updated and made available to the NBB pursuant to Article 17 of the Law (see the page "Reporting by financial institutions"), but also to demonstrate to the NBB that, in all cases where they have applied Article 32 of the Law, each of the legal conditions to benefit from this derogation is met.

## 3. Inability to identify or verify the identity of the persons involved at the required time or within the time limit set

In this respect, see the page "Non-compliance with the identification and identity verification obligation".

---

**Disclaimer: This English text is an unofficial translation and may not be**

**used as a basis for solving any dispute**



# Non-compliance with the identification and identity verification obligation

[Home](#) > [Financial oversight](#) > [Combating money laundering and the financing of terrori...](#)

## Legal and regulatory framework

- Loi anti-blanchiment : Article 33 , § 1
- Anti-Money Laundering Regulation of the NBB: Article 15

## Explanatory Memorandum of the Anti-Money Laundering Law

- Article 33, § 1

## Comments and recommendations by the NBB

- Comments and recommendations

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



# Anti-Money Laundering Law of 18 September 2017 - Article 33

## Art. 33

§ 1. If the obliged entities cannot fulfil their obligations to identify and verify the identity of a customer, his agents or his beneficial owners within the time limits referred to in Articles 30 and 31, they may neither establish a business relationship with or carry out a transaction for that customer. Moreover, they shall end any already established business relationship.

In the cases referred to in the first subparagraph, the obliged entities shall examine, in accordance with Article 46, whether the causes of the inability to fulfil the obligations referred to in the first subparagraph could raise ML/FT suspicions and whether CTIF-CFI should be notified.

The supervisory authorities may, by way of a regulation, authorise the obliged entities that fall within their competence to implement restrictive measures as an alternative to ending the business relationship as required pursuant to the first paragraph in particular cases, specified in that regulation, where the unilateral termination of the business relationship by the obliged entity is prohibited by other mandatory statutory provisions or public policy provisions, or if such a unilateral termination would have a severe and disproportionate negative impact on the entity.

§ 2. Paragraph 1 shall not apply to the obliged entities referred to in Article 5, § 1, 23° to 28°, with the strict proviso that they ascertain the legal position of their customer or perform the task of defending or representing that customer in, or concerning, judicial proceedings, including providing advice on instituting or avoiding such proceedings.



# NBB anti-money laundering regulation of 21 November 2017 - Article 15

## Art. 15

If obliged financial institutions cannot fulfil their obligations to identify and verify the identity of a customer, or the customer's agents or beneficial owners within the time limits referred to in Articles 30 and 31 of the Law, or their obligations to keep these identification data up to date in accordance with the Law, they may apply restrictive measures as an alternative to ending the already established business relationship, as required pursuant to Article 33, § 1, 1st indent, of the Law, if it consists of:

1° a life insurance contract, unilateral termination of which is contrary to other mandatory legal or regulatory provisions or public policy provisions. In this case, the obliged financial institution may refuse payment of any supplementary premium by the policyholder, without prejudice to the consequences that the legal or regulatory provisions attach to non-payment of a premium;

2° a loan contract, unilateral termination of which would expose the obliged financial institution to a severe and disproportionate negative impact. In this case, the obliged financial institution shall refuse any increase in the amount lent and shall terminate the business relationship as soon as possible.

In the cases referred to in the 1st indent, obliged financial institutions shall apply, with regard to the business relationship, customer due diligence measures proportional to the level of re-assessed risk, in accordance with Article 19, § 2, of the Law, taking account of the fact that this business relationship has not been terminated. Moreover, obliged financial institutions shall refuse to enter into any other business relationship with the customer concerned and to carry out any occasional transaction on behalf of this customer.

# Explanatory Memorandum to the Anti-Money-Laundering Law of 18 September 2017 - Article 33

## Art. 33

Draft Article 33 concerns cases in which obliged entities are unable to comply with their obligation to identify and verify the identity of the customer, the customer's agents or their beneficial owners under the terms specified in Articles 30 to 32. In the event that

- the obligation to identify and verify the identity of customers cannot be fulfilled under the terms referred to in Article 30, the obliged entity may neither enter into the business relationship nor execute transactions for this customer, and especially transactions via a bank account;
- the obliged entity has made use of the possibility of derogation referred to in Article 31, and has entered into a business relationship prior to having fulfilled its obligation to identify the customer, it must end the business relationship, unless this obligation to verify the customer's identity can be fulfilled as quickly as possible after the first contact with the customer.

If the issuer of electronic money fulfils the conditions for derogating from the identification and identity verification measures (Article 25), but decides not to derogate therefrom, it can decide to defer the time frame for identification or verification (cf. Article 32). In such a case, the issuer of electronic money concerned should establish in its internal procedures the consequences associated with not proceeding to identify and verify the identity of the customer within the established term.

Article 33 of the draft Law adopts the provisions of Article 14, paragraph 4 of the Directive which refers to Article 13, paragraph 1, a) and b) of the Directive and takes over Article 7, § 4 and 8 § 4 of the Law of 11 January 1993. Although Article 14, paragraph 4 only refers to the obligation to identify and verify the identity, the obligation to end the business relationship must be extended to cases where updating the identification proves to be impossible: in the section on the ongoing due diligence there is therefore a similar provision for the case in which updating the identification is impossible (cf. Article 35, § 2).

If the obligation to identify or verify the identity could not be met within the required time frame, this could constitute an indication of ML/TF. For this reason, § 1, second paragraph, specifies that, in accordance with Article 46, obliged entities must examine whether there is a need to inform the CTIF-CFI. This implies that the inability to meet the aforementioned obligation must be established within the obliged entity and must be reported to the AMLCO. The methods to establish and report this should be specified in the internal procedures referred to in draft Article 8.

§ 1, third paragraph, refers to specific cases where the unilateral termination of the business relationship (provided for in the first paragraph) would be prohibited by other mandatory statutory provisions or public policy provisions (as is the case for termination of life insurance agreements), or where such a unilateral termination would have a severe and disproportionate negative impact on the entity (as could be the case with loans already granted). In these cases, § 1, third paragraph determines that the supervisory authorities may, by way of a regulation, authorise the obliged entities that fall within their competence to implement restrictive measures as an alternative to ending the business relationship, as specified in that regulation.

§ 2 provides for the possibility for certain obliged entities to derogate from § 1, which prohibits business relationships or obliges their termination. This applies in particular to lawyers, notaries, company auditors, auditors, audit firms, external chartered accountants, external tax consultants, external registered accountants and external registered tax accountants. This derogation may only occur with the proviso that the obliged entities ascertain the legal position of their customer or perform the task of defending or representing that customer in, or concerning, judicial proceedings, including providing advice on instituting or avoiding such proceedings.



# Non-compliance with the identification and identity verification obligation: Comments and recommendations by the NBB

Home > Financial oversight > Combating money laundering and the financing of terrori...

## Contents

- 1. With regard to future customers
- 2. With regard to existing customers
- 3. Reporting to the AMLCO
- 4. Specific case: electronic money issuer deferring identification and/or identity verification

---

Article 33, § 1, of the Anti-Money Laundering Law describes the consequences of an inability to identify and/or verify the identity of the persons involved in a business relationship or occasional transaction at the time required by the Law or within the time limit set pursuant to the Law.

Since these due diligence obligations must in principle be fulfilled before establishing the business relationship or carrying out the intended occasional transaction, but may in certain specific cases be fulfilled in full or in part after the business relationship has been established (see the page “Time of identification and identity verification”), a distinction should be made between the consequences for future customers and those for existing customers.

## 1. With regard to future customers

When financial institutions are unable to obtain, by the time determined in Article 30 of the Law, the information that is required by the previously identified ML/FT risk level and that is necessary to identify and verify the identity of their customers and, where appropriate, their agent(s) and beneficial owner(s), **they may**

- **neither** establish the intended business relationship,
- **nor** carry out the transaction concerned.

The identification and identity verification obligations are mostly performance obligations. In that case, the associated legal prohibition takes effect as soon as it appears that the identification or the verification cannot be carried out. However, when the identification and identity verification obligation is a best-effort obligation (see the page “Object of the identification and identity verification”), the prohibition to establish or continue the business relationship or to perform the transaction desired by the customer takes effect when the financial institution is unable, for any reason whatsoever, to take the measures commensurate with the identified risk that are imposed by the Law **before the business relationship is established or the occasional transaction carried out**.

The refusal to establish a business relationship with a potential customer or to carry out an occasional transaction he wishes to perform, should be properly justified. This refusal may not be a means for the financial institution to discriminate against certain categories of customers (see the page “Due diligence requirements and compliance with other legislations”).

## 2. With regard to existing customers

When a financial institution has established a business relationship with a customer **without having verified** his identity or, where appropriate, that of his agent(s) and beneficial owner(s) at the time determined in Article 30 of the Anti-Money Laundering Law because its internal procedures allowed this given the need to not interrupt the conduct of business (see Article 31 of the Anti-Money Laundering Law) and when it is unable to verify the identities of these persons as soon as possible after first contact with the customer, it is legally obliged to **terminate this relationship**.

However, pursuant to Article 33, § 1, third paragraph, of the Anti-Money Laundering Law, financial institutions may apply restrictive measures as an alternative to ending the business relationship in the specific cases detailed in Article 15 of the Anti-Money Laundering Regulation of the NBB:

- **in the case of life insurance policies**, the unilateral termination of which is contrary to other mandatory legal or regulatory provisions or public policy provisions, the alternative restrictive measures to be applied consist in refusing payment of any supplementary premium by the policyholder, without prejudice to the consequences attached to non-payment of a premium pursuant to the legal or regulatory provisions (Article 15, first paragraph, 1°, of the Regulation);  
It should be noted in this regard that, in accordance with Article 30, third paragraph, of the Anti-Money Laundering Law, the identities of beneficiaries of life insurance policies should be verified **at the latest at the time of pay-out of the insurance benefits**.
- **in the case of loan contracts**, the unilateral termination of which would have a severe and disproportionate negative impact on the obliged financial institution, the alternative restrictive measures to be applied consist in refusing to increase the amount lent and ending the business relationship as soon as possible (Article 15, first paragraph, 2°, of the Regulation). Examples of a severe and disproportionate negative impact would be the institution being unable, in practice, to obtain reimbursement of significant amounts or to benefit from the real or personal guarantees associated with the loan. Furthermore, the financial institution should take the first opportunity to terminate the loan without suffering this negative impact.

The NBB considers that the decision to apply alternative restrictive measures should be motivated in writing on a case-by-case basis:

- for restrictive measures as an alternative to terminating a life insurance policy, this motivation should include verification that the current legislation does not authorise the insurance company to terminate the policy unilaterally;
- for measures as an alternative to terminating a loan, the written motivation should include an estimation of the negative impact such a unilateral termination would have on the financial institution, in order to demonstrate its severe and disproportionate nature, and mention which future date or events will enable the institution to end the business relationship as soon as possible without suffering this severe and disproportionate negative impact.

In all these cases, the financial institution should also take the measures necessary to ensure that no other business relationship is established with or occasional transaction carried out on behalf of the customer concerned.

With regard to the business relationship that is subject to the alternative restrictive measures, the financial institution should also exercise enhanced due diligence, in accordance with Article 37, § 2, of the Anti-Money Laundering Law, proportionate to the re-assessed level of risk, in accordance with Article 19, § 2, of the Anti-Money Laundering Law, taking into account that this relationship has not been terminated (see the page “Special cases of enhanced due diligence”). This enhanced due diligence should also enable the institution to ensure that the restrictive measures are actually applied and that any loans will be terminated as soon as possible.

The methods for implementing the alternative restrictive measures should be specified in the financial institution’s internal procedures (see the page “Policies, procedures, processes and internal control measures”).

## 3. Reporting to the AMLCO

In accordance with Article 46 of the Anti-Money Laundering Law, financial institutions should also examine whether CTIF-CFI should be notified of cases as mentioned above where the identification and/or identity verification obligation could not be fulfilled, if this inability could be an indication of ML/FT.

This implies that this inability should first be established and reported to the AMLCO, the details of which should be specified in the internal procedures adopted by the financial institution pursuant to Article 8 of the Anti-Money Laundering Law (for more information on this subject, see the page “Policies, procedures, processes and internal control measures” and point 1.4 of the page “Ongoing due diligence and detection of atypical facts and transactions”).

## 4. Specific case: electronic money issuer deferring identification and/or identity verification

Where an electronic money issuer decides to make use of the possibility of derogation provided for in Article 32 of the Anti-Money Laundering Law, in compliance with the conditions set out therein, and thus to not identify and/or verify the identity of the customers (and where appropriate, their agent(s) and beneficial owner(s)) who provide them with funds for the issuance of electronic money before the funds concerned have been provided, but to defer fulfilment of these due diligence obligations until a later time (see point 2.2. of the page “Identification and identity verification time”), the electronic money issuer should itself, in its internal procedures, specify the consequences of the inability to identify or verify the identity of the persons involved within the time limit previously determined therein, as the provisions of Article 33 of the Anti-Money Laundering Law do not apply in that case.

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



# Identification of the customer's characteristics and of the purpose and nature of the business relationship or the occasional transaction

Home > Financial oversight > Combating money laundering and the financing of terrori...

## Legal and regulatory framework

- Anti-Money Laundering Law: Article 34

## Explanatory Memorandum of the Anti-Money Laundering Law

- Article 34

## Other reference documents

- ESAs Risk Factor Guidelines dated 04 January 2018
- BCBS Guidelines dated June 2017 on Sound management of risks related to money laundering and financing of terrorism (see Annex 4)

## Comments and recommendations by the NBB

- Comments and recommendations

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**

# Identification of the customer's characteristics and of the purpose and nature of the business relationship or the occasional transaction: Comments and recommendations by the NBB

Home > Financial oversight > Combating money laundering and the financing of terrori...

## Contents

- 1. Obligation to identify the customer's characteristics and the purpose and nature of the business relationship or the occasional transaction
- 2. 2. Specific derogation: low-risk issuance of electronic money
- 3. Time of identification
- 4. Updating of data or information
- 5. Internal control measures

## 1. Obligation to identify the customer's characteristics and the purpose and nature of the business relationship or the occasional transaction

### 1.1 Scope of the obligation

The obligation to identify the customer's characteristics and the purpose and nature of the business relationship already existed under the former Law of 11 January 1993, where it did not appear, however, as a specific obligation, distinct from the identification and identity verification obligation. Article 34 of the new Anti-Money Laundering Law contains specific provisions that introduce a specific regime for this obligation, while explicitly extending it to occasional transactions.

Thus, the entities subject to the Anti-Money Laundering Law must take adequate measures to assess the customer's characteristics and the purpose and nature of the business relationship or of the intended occasional transaction. The Law requires the obliged entities in particular to ensure that they possess the information necessary:

- to implement the customer acceptance policy (see the page "Policies, procedures, processes and internal control measures");
- to fulfil the ongoing due diligence obligations with regard to the business relationships and transactions (see the page "Ongoing due diligence and detection of atypical transactions");
- and to fulfil the enhanced due diligence obligations (see the pages on "Special cases of enhanced due diligence"). In this context, they should take reasonable measures to determine whether the persons identified, including the beneficial owner of the beneficiary of a life insurance policy, are politically exposed persons, family members of politically exposed persons or persons who are known to be closely associated with politically exposed persons (see in particular the page on "PEPs").

The obligation to collect the necessary information referred to in the first and second points above is the obligation that was formerly provided for, for financial institutions in particular, in Article 12 of the Anti-Money Laundering Regulation of the CBFA of 23 February 2010.

For further information on the scope of the obligation to identify the customer's characteristics and the purpose and nature of the business relationship or the intended occasional transaction, see the explanatory memorandum of Article 34, § 1, of the Anti-Money Laundering Law.

## 1.2 Application of the risk-based approach

Like the other due diligence obligations, the obligation to identify the characteristics of the customer and the purpose and nature of the business relationship or the intended occasional transaction should be submitted to a risk-based approach (see Article 34, §1 *in fine*, of the Anti-Money Laundering Law). In order to fulfil this obligation, the financial institutions must take measures that are commensurate with the risks identified in the given situation.

The request for information addressed to the customer in this context can depend in particular on the characteristics of the product, service or transaction requested by the customer, the distribution channel used, the country or geographic area concerned or the characteristics of the customer. If, taking into account these factors, the risk identified in the given situation appears low, the requested information can be reduced in comparison with the information required by a level of risk that is identified as standard or, *a fortiori*, as high.

## 1.3. Internal procedures

As a reminder, the NBB recommends that the internal procedures to be implemented by financial institutions pursuant to Article 8 of the Anti-Money Laundering Law, in this case the customer acceptance policy, list the relevant information that should be obtained, depending on the risk classification, to identify the characteristics of the customer and the purpose and nature of the business relationship or the intended occasional transaction (see the page "Policies, procedures, processes and internal control measures").

As for the method of collecting this information, it is recalled that the explanatory memorandum of Article 34, § 1, of the Anti-Money Laundering Law states in particular that *"the purpose and nature of a business relationship can be determined on the basis of prior or pre-contractual information about the proposed product or service that is actually communicated to the customer, provided that the purpose and nature of the business relationship to be established can be deduced in a certain, precise and unambiguous manner. On the other hand, where the product or service offered makes it possible to carry out transactions likely to have various characteristics (for example, in the case of the opening of a current account), the identification of the purpose and nature of the business relationship will require more precise and personalised information from the customer on his intentions regarding the use of the business relationship."*

## 2. 2. Specific derogation: low-risk issuance of electronic money

### 2.1. Possibility of derogation

Article 34, § 2, of the Anti-Money Laundering Law provides for the possibility of a derogation for the financial institutions issuing electronic money. These institutions may, where the overall assessment of the ML/FT risks specifically associated to their issuing activity shows that these risks are low, decide not to collect information on the characteristics of the customer or on the purpose and nature of the business relationship or intended occasional transaction with respect to customers who provide them with funds for the issuance of electronic money.

### 2.2. Conditions for application of the derogation

However, this possibility of derogation is subject to several **conditions**, which are the same as those to which the possibility of derogation from the identification and identity verification obligations is subject, as set out in Article 25 of the Anti-Money Laundering Law (see the page "Persons to be identified").

**In addition to the fact that the overall risk assessment carried out by the electronic money issuer must demonstrate that the level of ML/FT risks to which it is exposed as a result of this activity is low**, the following cumulative conditions must be met:

- 1° the payment instrument cannot be reloaded or, if it is reloadable, it can only be used in Belgium and only to make payments up to a maximum monthly limit of EUR 250;
- 2° the maximum amount stored electronically does not exceed EUR 250;
- 3° the payment instrument is used exclusively to purchase goods or services; it follows in particular that it cannot be accepted to perform a money remittance operation;
- 4° the payment instrument cannot be funded with anonymous electronic money;
- 5° the electronic money issuer concerned carries out sufficient monitoring of the transactions or business relationship to enable the detection of unusual or suspicious transactions.

## 2.3. Non-application of the derogation

Even if all the conditions listed above are met, the derogation is not applicable when a customer:

- 1° is redeemed in cash, at the monetary value of the electronic money, or
- 2° withdraws this value in cash,

if the amount redeemed or withdrawn, as the case may be, exceeds EUR 100.

In these two cases, where the legislator considered that the risk could not be regarded as low, the electronic money issuer is required to take appropriate measures to identify the characteristics of the customer concerned and the purpose and nature of the business relationship or occasional transaction, **at the time of the refund or withdrawal of the electronic money** (that was previously issued without any such measures).

In the same vein, the NBB highlights the fact that, where circumstances have given rise to suspicions of ML/FT, either at the time when the business relationship with the customer is established or subsequently, that led the electronic money issuer to report a suspicion to CTIF-CFI and, in accordance with Article 22 of the Anti-Money Laundering Regulation of the NBB, to carry out an individual re-assessment of ML/FT risks revealing that the level of risk associated with the given situation can no longer be regarded as low (which should logically be the case - see the page "Reporting of suspicions"), the said issuer can no longer invoke the derogation provided for in Article 34, § 2, of the Law. The issuer should immediately identify the customer's characteristics and the purpose and nature of the business relationship or the occasional transaction, in accordance with Article 34, § 1, of the Law.

## 2.4. Documentation

Finally, since the above-mentioned possibility of derogation is not absolute but subject to certain limitations, the NBB recommends that the financial institutions applying the derogation be able not only to submit the overall risk assessment that establishes the low level of risk, which must be documented, updated and made available to the NBB pursuant to Article 17 of the Law (see the page "Reporting by financial institutions", but also to demonstrate to the NBB that, **in all cases where** they have applied Article 34, § 2 of the Law, each of the legal conditions to benefit from this derogation is met.

# 3. Time of identification

## 3.1. Principle

In accordance with Article 34, § 1, fourth paragraph of the Anti-Money Laundering Law, the information concerning the customer's characteristics and the purpose and nature of the business relationship or of the occasional transaction should be obtained **at the latest**:

- **at the time when the business relationship is established** if the customer wishes to establish a business relationship with the financial institution, or
- **at the time when the transaction is carried out**, in case of an occasional transaction.

## 3.2. Inability to identify the customer's characteristics and/or the purpose and nature of the business relationship or the occasional transaction

### 3.2.1. Prohibition to enter into a business relationship or perform the intended transaction

According to Article 34, § 3, first paragraph, of the Anti-Money Laundering Law, when financial institutions are unable to obtain the information that is required by the level of ML/FT risk that they have previously identified, on the customer's characteristics and the purpose and nature of the business relationship or the intended occasional transaction at the latest at the time of establishment of the business relationship or the time of conclusion of the transaction, **they may**:

- **neither** establish the intended business relationship,
- **neither** carry out the transaction, especially a transaction through a bank account.

The scope of this prohibition, which also applies in case of non-identification of the customer (or of his agent or beneficial owner) or absence of the verification of his identity (see the page "Non-compliance with the identification and identity verification obligation"), cannot be dissociated from the scope of the due diligence obligation itself. Thus, as most identification and identity verification obligations are performance obligations, the associated legal prohibition generally takes effect as soon as it appears that the identification or the verification cannot be carried out. Conversely, the obligation to identify the customer's characteristics and the purpose and nature of the business relationship or the occasional transaction is an **obligation of means**. In that case, the prohibition to establish or continue the business relationship or to perform the transaction desired by the customer takes effect when the financial institution is unable, for any reason whatsoever, to take the measures commensurate with the identified risk that are imposed by the Law **before the business relationship is established or the occasional transaction carried out**.

The refusal to establish a business relationship with a potential customer or to carry out an occasional transaction he wishes to perform, should be properly justified. This refusal should not be a means for the financial institution to discriminate against certain categories of customers (see the page "Due diligence requirements and compliance with other legislations").

### 3.2.2. Reporting to the AMLCO

Beyond the prohibition to establish a business relationship with a customer or to carry out a transaction on behalf of him in these circumstances, any inability, for the financial institution, to fulfil the obligation to identify the customer's characteristics and the purpose and nature of the business relationship or the intended occasional transaction must lead the financial institution, under the responsibility of the AMLCO, to inquire into the causes of this inability and to decide whether a suspicion should be reported to CTIF-CFI (Article 34, § 3, second paragraph, of the Anti-Money Laundering Law).

This implies that this inability should first be established and reported to the AMLCO, the details of which should be specified in the internal procedures adopted by the financial institution pursuant to Article 8 of the Anti-Money Laundering Law (for more information on this subject, see the page "Policies, procedures, processes and internal control measures" and point 1.4 of the page "Ongoing due diligence and detection of atypical facts and transactions").

## 4. Updating of data or information

The financial institutions should update the information they hold pursuant to the obligation to identify the customer's characteristics and the purpose and nature of the business relationship.

With regard to this obligation to update, which should be subject to a risk-based approach, that is part of the ongoing due diligence that financial institutions must exercise with regard to business relationships and transactions pursuant to Article 35, § 1, of the Anti-Money Laundering Law, for more information see the page "Ongoing due diligence and detection of atypical facts and transactions".

## 5. Internal control measures

Financial institutions are expected to periodically verify that the internal procedures adopted to enable them to comply with the obligation to identify the characteristics of their customers and the purpose and nature of business relationships and occasional transactions are continuously and properly complied with and that the processes for implementing the obligations related to this due diligence requirement are adequate.

The NBB recommends the internal audit function to pay particular attention to:

- the appropriate nature of the information collected while fulfilling the obligation to identify the customer's characteristics and the purpose and nature of the business relationship or the occasional transaction;
- the appropriate nature of the updating of data and information held in the context of the same obligation;
- with regard to the electronic money institutions that make use of the derogation provided for in Article 34, § 2, of the Anti-Money Laundering Law, whether the risk associated with their activity of issuing electronic money effectively is low and whether the conditions listed in Article 25 of the same law for applying the above-mentioned derogation are effectively met.

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



# Anti-Money Laundering Law of 18 September 2017 - Article 34

## Art. 34

§ 1. Obligated entities shall take adequate measures to assess the customer's characteristics and the purpose and nature of the business relationship or of the intended occasional transaction.

In particular, they shall ensure that they possess the information necessary for the implementation of the customer acceptance policy referred to in Article 8, for the application of the ongoing due diligence requirements with regard to the business relationships and transactions in accordance with Section 4, and for the specific enhanced due diligence requirements in accordance with Chapter 2.

In particular, they shall take reasonable measures to determine whether the persons identified pursuant to Section 2, including the beneficial owner of the beneficiary of a life insurance policy, are politically exposed persons, family members of politically exposed persons or persons who are known to be closely associated with politically exposed persons.

This information shall be obtained at the latest when the business relationship is established or the occasional transaction is carried out. The measures taken for this purpose shall be proportionate with the risk level identified in accordance with Article 19, § 2, first subparagraph.

§ 2. Obligated entities that issue electronic money may, based on an appropriate assessment of the ML/FT risks conducted pursuant to Article 16 that demonstrates that these risks are low, derogate from the first paragraph, with regard to customers in the course of their business related to the issuance of electronic money, if the risk mitigation conditions listed in Article 25 are met.

§ 3. If obliged entities are unable to fulfil their obligation referred to in paragraph 1, they may neither establish a business relationship with or carry out a transaction, especially a transaction through a bank account, for the customer concerned. Moreover, they shall terminate any already established business relationship or shall, where appropriate, apply the alternative restrictive measures referred to in Article 33, § 1, third subparagraph.

In the cases referred to in the first subparagraph, obliged entities shall examine, in accordance with Article 46, whether the causes of the inability to fulfil the obligations referred to in paragraph 1 could raise ML/FT suspicions and whether CTIF-CFI should be notified.

§ 4. Paragraph 3 shall not apply to the obliged entities referred to in Article 5, § 1, 23° to 28°, with the strict proviso that they ascertain the legal position of their customer or perform the task of defending or representing that customer in, or concerning, judicial proceedings, including providing advice on instituting or avoiding such proceedings.

# Explanatory Memorandum to the Anti-Money-Laundering Law of 18 September 2017- Article 34

## Art. 34

Draft Article 34 refers to the obligation to identify and assess the customer's characteristics and the purpose and nature of the business relationship. This obligation is not new. It is nevertheless not explained in any depth in the Law of 11 January 1993, rendering it unclear that this is an obligation that should be distinguished from the obligation to identify and verify the identity of the customer. In the Law of 11 January 1993, only one paragraph mentions the obligation to identify the purpose and nature of the business relationship (Article 7, § 1, fifth paragraph) and it is covered in an Article that refers to the identification of customers. The obligation to collect information on the customer's characteristics (other than the identification) logically follows from the provisions on the ongoing due diligence in the Law of 11 January 1993, but the Law does not expressly mention this. The obligation to identify the characteristics of the customer and the purpose and nature of the business relationship is an obligation that should be distinguished from the other due diligence obligations, and subject to a specific rule. In particular, it should be emphasised that the collection of relevant and sufficiently reliable information on both the characteristics of customers themselves and the purpose and nature of the business relationship they wish to enter into, is a prerequisite for the ongoing due diligence required based on the risk the business relationship and the transactions entail. Failing to comply with the obligation to identify these data can therefore have similar consequences to failing to comply with the obligation to identify and verify the identity of the customer and may render the obliged entity incapable of identifying suspicious transactions and reporting them to the CTIF-CFI.

However, it is indicated that, as regards the financial sector, Article 12 of the aforementioned CBFA Regulations already provides for the obligation to collect all information necessary for enforcement of the customer acceptance policy and the obligation of due diligence regarding the business relationship and the transactions.

Taking into account the foregoing, draft Article 34, § 1 consequently specifies that obliged entities must take appropriate measures to assess the characteristics of the customer and the purpose and nature of the business relationship or the envisaged occasional transaction. "Assess" should be understood to be synonymous with "understanding", as used in Recommendation 10 of the FATF. The objective sought consists of ensuring that the obliged entity gains sufficient understanding of the specific characteristics of the business relationship or of the occasional transaction and of the characteristics of the customer to be able to assess whether the transaction is normal or atypical or even suspicious. To this end, the obliged entity is required to verify what type of business relationship the customer is seeking to enter into with it and what types of transaction the customer wishes to execute within the context of that relationship, and it is required to ascertain all useful and pertinent information that can provide an understanding of the customer's motives for entering into that relationship. The purpose and nature of a business relationship can be determined using the prior or pre-contractual information that was given to the customer on the product or service offered, insofar as it can be derived clearly, precisely and unequivocally from that information. Where however, based on the product or service offered, transactions with potentially differing characteristics can be executed (for example, when opening a current account), the customer needs to be asked for more accurate and more personal information on his/her plans for the business relationship in order to identify the purpose and nature of the business relationship. In those cases, it would not suffice to legally qualify an envisaged transaction without understanding the context and underlying reasons thereof. It should also be noted that Article 13, paragraph 1, c) of the Directive, which is transposed by Article 34 of the draft Law, requires the obliged entity to obtain information on the business relationship, but does not expressly lay down that same obligation for occasional transactions. Nevertheless, it does seem necessary, especially as regards the risk of terrorist financing, that obliged entities gain a good understanding of the envisaged occasional transaction. A good understanding — and by definition a global one — of the nature and the purpose of the business relationship or envisaged occasional transaction implies that the obliged entity should also collect information on the customer based on the ML/TF risks,

other than the identification details collected pursuant to Article 26. This is why Article 34 lays down an obligation to identify the purpose and nature of the business relationship or the envisaged occasional transaction as well as an obligation to identify the characteristics of the customer.

As is the case with all general due diligence obligations, this obligation is subject to the risk-based approach. The measures taken must therefore be appropriate for the risk level identified.

The measures implemented must in particular allow the following information to be collected:

- The information necessary for the enforcement of the customer acceptance policy referred to in Article 8; by way of reminder, the customer acceptance policy describes the procedure that must be followed to ensure that when entering into a business relationship or a transaction with customers, a prior assessment of the associated reputational risk and ML/TF risk is carried out, taking into account the specific characteristics of the client and the purpose and nature of the business relationship or transaction. This policy determines the basic risk categories (high, low, standard) into which customers are divided after completion of the individual assessment. It also determines which criteria are associated with each of these categories (for example profession or geographical area of the business activity). The enforcement of the customer acceptance policy therefore necessarily implies that the obliged entity collects relevant information on the customer's characteristics and the purpose and nature of the business relationship or the envisaged occasional transaction. This information is essential, in the first place as part of the individual risk assessment laid down under Article 19, § 2 of the draft Law. It concerns detailed information that is indispensable to complete the identification and identity verification measures and to enable the obliged entity to gain a sufficient understanding of the persons involved in the business relationship or the transaction in question (the client, agents, beneficial owners or beneficiaries of life insurance policies or similar) to assess the level of risk potentially associated therewith. Although the identification details strictly speaking already allow, where applicable, the presence of a specific risk to be identified, they are not sufficient to gain a good understanding of the customer (his/her business, his/her assets, the source of his/her income, etc.) and of his/her intentions (portfolio management, payments and withdrawals, money transfers). This information is nevertheless essential to assess the level of risk associated with the customer and to verify whether the criteria associated with the various risk categories established in the customer acceptance policy have been met. Where appropriate, the enforcement of this customer acceptance policy can lead to the obliged entity refusing to enter into a business relationship with the customer or refusing to execute the customer's desired transaction, if after completing the risk assessment it considers that the nature or importance thereof do not enable them to be managed properly;
- The information necessary to fulfil the obligation of ongoing due diligence as regards business relationships and transactions (cf. Article 35 hereinafter); the first part of that obligation namely implies that the transactions must be verified for consistency with the characteristics of the customer and the purpose and nature of the business relationship or envisaged transaction. This clearly implies that the obliged entity must strictly speaking also collect other information from the customer apart from identification details. This information must for example enable a credit institution to identify any disproportionality between payments made by a customer and his/her business activity, known income or declared assets;
- The information required for the specific obligation of enhanced due diligence measures; it is emphasised for instance that the enhanced due diligence measures that apply when the customer is a respondent financial institution in a cross-border correspondent relationship imply that sufficient information has been collected on this institution. The same applies when the customer is a politically exposed person (PEP). In this respect, the draft Law expressly determines that obliged entities must take reasonable measures to determine whether the persons identified pursuant to Section 2 are PEPs, family of PEPs or persons known to be close associates of PEPs.

As for understanding the purpose and nature of the envisaged business relationship (or transaction), it is possible that the obliged entity does not need additional information on the customer because the nature of the desired product or desired service and their objective characteristics are sufficiently unequivocal. By way of example, a credit institution that opens a savings account for a customer does not in principle need any additional information to understand the nature and purpose of the business relationship. The opening of a current account, however, can have several purposes (the account can, for example, be opened for private purposes or for business purposes) and can give rise to different transactions (namely cash transactions, transactions relating to foreign counterparties, etc.), making it necessary for the obliged entity to collect more precise information on the customer's intentions. As for

understanding the characteristics of the customer, there is more of a likelihood that the obliged entity will need to obtain additional information (as regards the customer's profession, the source of funds involved in the business relationship, etc.).

This information on the customer's characteristics and the nature and purpose of the business relationship or the occasional transaction must be obtained by the time the business relationship is entered into or by the time the occasional transaction is executed.

Paragraph 2 of this draft Article provides for the possibility of derogating from the obligation to identify the characteristics of the customer and the nature and purpose of the business relationship or the envisaged transaction when issuing electronic money. Obligated entities that exercise this activity may, based on an appropriate general risk assessment demonstrating a low risk, derogate from the obligation to identify the characteristics of the customer and the nature and purpose of the business relationship with regard to customers in the course of their business related to the issuance of electronic money. This derogation is subject to compliance with the risk mitigation conditions listed in Article 25 of the draft Law. Draft Article 34, § 2 transposes Article 12, paragraph 1 of the Directive, which provides for the possibility of derogating from Article 13, paragraph 1, c) of the Directive. Given that it is possible to derogate from the obligation to identify and verify the identity of the customer (cf. Article 25), it also seems logical to permit derogation from the obligation to identify the characteristics of the customer and the nature and purpose of the business relationship.

§ 3 of the same draft Article sets out the consequences of failure to comply, within the required time frame, with the obligation to sufficiently identify the characteristics of the customer and the nature and purpose of the business relationship or the envisaged transaction. If obliged entities are unable to comply with this obligation, they may neither establish a business relationship with nor carry out a transaction, especially a transaction through a bank account, for the customer concerned. Moreover, they must terminate any business relationship already established or, where appropriate, apply the alternative restrictive measures as referred to in Article 33, § 1, third paragraph.

In accordance with Article 46, obliged entities shall examine whether the CTIF-CFI needs to be notified of the cases where the obligation of identifying the customer characteristics and the nature and purpose of the business relationship or the transaction could not be met by the established deadlines. This implies that the impossibility of fulfilling the stated obligation must be established within the obliged entity and must be reported to the AMLCO. The methods used to establish and report this should be specified in the internal procedures referred to in draft Article 8.

Draft Article 34, § 4 provides for the possibility for certain obliged entities to derogate from § 3, which prohibits entry into the business relationship or requires the termination thereof. This applies in particular to lawyers, notaries, company auditors, auditors, audit firms, external chartered accountants, external tax consultants, external registered accountants and external registered tax accountants. This derogation may only occur with the proviso that the obliged entities concerned ascertain the legal position of their customer or perform the task of defending or representing that customer in, or concerning, judicial proceedings, including providing advice on instituting or avoiding such proceedings.



# Ongoing due diligence and detection of atypical facts and transactions

Home > Financial oversight > Combating money laundering and the financing of terrori...

## Legal and regulatory framework

- Anti-Money Laundering Law: Articles 35, §§1 and 2, and 36
- Anti-Money Laundering Regulation of the NBB: Articles 15, 16, 1°, and 17

## Explanatory Memorandum of the Anti-Money Laundering Law

- Articles 35 and 36

## Other reference documents

- Circulaire NBB\_2018\_21 / Analyse horizontale de contrôle consistant en l'examen d'un échantillon de transactions passées par des agents liés de différents établissements de paiement
- ESA guidelines of 4 January 2018 on risk factors
- BCBS Guidelines dated June 2017 on Sound management of risks related to money laundering and financing of terrorism

## Comments and recommendations by the NBB

- Comments and recommendations

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**

# Ongoing due diligence and detection of atypical facts and transactions: Comments and recommendations by the NBB

Home > Financial oversight > Combating money laundering and the financing of terrori...

## Contents

- 1. Detection of atypical facts and transactions
- 2. Updating of the data or information and of the individual risk assessment
- 3. 3. Inability to exercise ongoing due diligence
- 4. Internal control measures

---

The ongoing due diligence obligation is defined in Article 35, § 1 of the Anti-Money Laundering Law. It comprises two aspects:

- on the one hand, the obligation to carefully examine the transactions carried out over the course of the business relationship; this obligation includes monitoring the customer's occasional transactions and paying attention to intriguing facts related to the customer which, if they are suspect, should be reported to CTIF-CFI (see point 1 below), and
- on the other hand, the obligation to update the data or information collected as part of the identification and identity verification obligation and the obligation to identify the customer's characteristics and the purpose and nature of the business relationship or the occasional transaction (see point 2 below).

In implementing the on-going due diligence obligation, financial institutions should adopt a **risk-based approach**: the level of due diligence to be exercised by financial institutions must be proportionate to the level of risk identified in the individual risk assessment referred to in Article 19, § 2, first paragraph, of the Anti-Money Laundering Law, taking into account, where appropriate, any updates of this assessment (see the page "Individual risk assessment"). In determining the level of on-going due diligence, account should also be taken, where appropriate, of the high level of risk associated with situations that inherently involve such a level of risk (see the page "Special cases of enhanced due diligence").

## 1. Detection of atypical facts and transactions

### 1.1. General principles

A first implication of the due diligence obligation is that financial institutions must conduct an adequate and risk-proportionate examination of the transactions carried out over the course of the business relationship, the occasional transactions and the facts surrounding the business relationship or transaction, to determine whether these transactions or facts should be reported to the AMLCO.

Attention is drawn to the fact that this obligation also concerns transactions carried out in relation to customers established in other Member States under the freedom to provide services, i.e. without the intervention of a subsidiary, a branch, an agent or, in the case of electronic money institutions, a distributor established in that other Member State.

At that stage of the process, there is yet no need to determine whether the transaction or the fact concerned is suspected of being linked to ML/FT and must therefore be reported to CTIF-CFI, but only to identify the transactions and facts the characteristics of which are such that it is necessary to submit them to the AMLCO for further examination, in order to decide whether or not those transactions or facts are suspected to be related to ML/FT (see the page "Analysis of atypical facts and transactions").

### 1.1.1. Atypical transactions

Occasional **transactions** or transactions carried out in the context of a business relationship should be considered as "atypical" if they do not appear to be consistent with the customer's characteristics and with the object and nature of the business relationship or the proposed transaction.

Atypical transactions include in particular transactions carried out in the context of a business relationship and occasional transactions that appear abnormally complex or that involve an unusually high amount, as well as inherently unusual transactions, with no apparent economic or lawful purpose.

Examples of transactions which are atypical in light of the customer profile include:

- transactions involving amounts that cannot be justified by known sources of income of the customer,
- cash transactions involving large amounts that apparently cannot be explained by the customer's professional activity or his known assets,
- significant transactions in relation with high-risk, low-tax or no-tax countries with which the customer has not had a legitimate link that the financial institution was aware of,
- the use of shell companies, the actual activity of which is not consistent with the corporate purpose or which have their head office in a high-risk third country, a no-tax or low-tax State, or a State or territory that has not concluded with Belgium a tax convention including access to banking information;
- transactions and structures similar to those referred to in the two previous points which appear to have links with countries which, although not referred to in Article 38 of the Law, are identified by the financial institution as presenting similar risks, taking into account other credible sources of information, including the EU list of non-cooperative tax jurisdictions;
- the execution of financial transactions by companies whose Articles of Association have been amended frequently without this being justified by the economic situation of the company;
- recourse to natural persons acting only seemingly on behalf of companies or individuals involved in financial transactions;
- the use of intermediate accounts or accounts of non-financial professionals as payable-through accounts, or the use of complex corporate structures and legal and financial arrangements that make the management and administration mechanisms opaque, thereby complicating the identification of the beneficial owners and of the links between the origin and the destination of the funds;
- international financial transactions with no apparent legal or economic purpose that are usually limited to simple transits of funds from or to destinations abroad, especially when carried out with high-risk third countries;
- etc.

It should also be noted that, in accordance with Articles 9 and 13 of the European Regulation on **Transfers of Funds**, and without prejudice to the other measures required by this European Regulation, where payment service providers of the beneficiaries of such transfers or payment service providers who act as intermediaries in carrying out these transfers find that the required information concerning the payer or the beneficiary is missing or incomplete (see the page "Transfers of funds"), they should examine whether these deficiencies are such as to give rise to suspicion of ML/FT. Transfers of funds received which are not accompanied by the information required should therefore be treated as atypical transactions.

The detection of atypical transactions and facts is also the first step in the process of enabling financial institutions to collaborate effectively in the fight against **terrorist financing**, whose peculiarities do not allow to draw up an exhaustive and perennial list of transactions and behaviours requiring reporting. In these circumstances, in order to be informed as soon as possible of the typologies with regard to terrorist financing and to be able to take them into account, financial institutions should refer in particular to the documentation distributed by the competent national, European and international administrations or authorities, as well as to the media coverage on persons and their resources to finance terrorist actions. They should also refer to the national and European assets freeze measures taken to combat terrorist financing.

In particular, the NBB invites financial institutions to refer to CTIF-CFI's activity reports on the financing of terrorism, and to comply with the specific instructions and recommendations that may be addressed to them on the subject by the competent national authorities.

From the currently available public information it appears that the detection of atypical transactions which may be linked to the financing of terrorism should be aimed in particular at identifying certain "scenarios" associated with known typologies in this field, such as, for example:

- the repeated remittance of small amounts of money between individuals without apparent links (family links, economic links) between them,
- a fund remittance destination which appears to be atypical in light of the profile of the business relationship or the characteristics and habits of the customer,
- donations to non-profit associations followed by remittances of larger amounts of funds, especially to foreign countries,
- cross flows from or to associations,
- the use of electronic money instruments, in particular anonymous instruments and virtual currencies, especially when the latter are converted into legal tender money,
- the opening of a bank account, promptly followed by withdrawals of cash abroad in sensitive areas or in transit countries,
- the use of crowdfunding platforms,
- the use of consumer credit, especially when followed by cash withdrawals of all or a significant portion of the funds loaned, and/or transfers abroad,
- successive removals of a credit or debit card limit with a view to withdrawing cash,
- the total withdrawal (or almost total withdrawal, leaving a small balance) of deposits on accounts or life insurance contracts,
- reactivation of an account or bank card without a credible explanation,
- the payment of ransoms following an abduction or theft of personal data.

All these criteria remain subjective, but their combination makes the information more relevant.

In the light of the growing number of cases of proselytism with a view to recruiting terrorists in prison, financial institutions are also encouraged to closely examine business relationships with prisoners.

In accordance with the provisions of European law imposing restrictive measures against certain countries with a view to combating the proliferation of weapons of mass destruction and its financing, the due diligence measures with regard to customers, transactions and business relationships that are required to combat ML/FT must also be implemented to combat the financing of the proliferation of weapons of mass destruction. Therefore, transactions that could be related to the proliferation of weapons of mass destruction must also be considered atypical because of their intrinsic characteristics or those of persons acting as customers, agents, beneficial owners or counterparties in these transactions, in particular because of their links with the countries concerned or with persons or entities known to be involved in the proliferation of weapons of mass destruction.

In order to effectively detect these "atypical" transactions, financial institutions must be able to compare the customer's transactions with the information collected on his identity and characteristics, on the identity of the beneficial owner(s), on the object and nature of the business relationship and the transaction and, if applicable, the origin of the funds.

### 1.1.2. Atypical facts

The atypical **facts** that must be reported to the AMLCO are all facts that are mainly related to the unusual behaviour of the customer in his relationships with staff members or agents of the financial institution and which may constitute indications of ML/FT.

This does not include the actual execution of a particular transaction, but more in general facts that involve the customer or persons interacting with him.

By way of example, unusual behaviour of the customer may include an abnormal and inexplicable lack of interest for the financial conditions proposed, his ignorance of certain essential elements of the transaction (such as the amount), the execution of a transaction (for example, the execution of an electronic funds transfer or the receipt of the amount of such a transfer in cash) under the physical supervision of a third party, etc.

It should be stressed that these atypical facts must be reported to the AMLCO regardless of whether the transaction desired by the customer must or must not be considered as atypical in itself and independently of whether the transaction is actually carried out or not. In this respect, it should be noted that **attempted transactions** may constitute unusual facts which must be brought to the attention of the AMLCO, in particular when the customer renounces in extremis, unexpectedly and without credible explanation, to the execution of a transaction as soon as he is informed of the fact that such execution implies that he provides information as to his identity or that of the beneficial owners, that he discloses the purpose of the transaction or the origin of the funds involved, etc.

Atypical facts that must be reported to the AMLCO may also result from the **cumulative behaviour of several customers**. This is the case, for example, if a staff member or agent of the financial institution finds that different persons pretending to act independently of one another request, over a short period of time, the execution of similar occasional transactions which individually do not appear to be atypical, but are surrounded by circumstances such that these transactions may be considered to be connected, etc.

It should also be noted that Articles 33, § 1, second paragraph, 34, § 3, second paragraph and 35, § 2, second paragraph of the Anti-Money Laundering Law provide that if financial institutions cannot fulfil their due diligence obligations, they must examine, in accordance with Article 46 of the Law, whether the causes of this inability are such as to raise ML/FT suspicions and whether CTIF-CFI should be notified. These situations must also be detected systematically and must be treated in the same manner as atypical facts.

The receipt of information from credible external sources that may have a negative influence on the appreciation of the business relationship with a customer should also be treated as an atypical fact, for instance in case of occurrence of new events that may affect the customer's risk profile. This may be the case, in particular, where the financial institution receives an **indictment from the judicial authorities** or a request for information from CTIF-CFI concerning the business relationship with a customer or the transactions carried out by the latter. The NBB considers that the receipt of an indictment from a public prosecutor's office concerning a customer of the financial institution (or another intervention by the judicial and police authorities), constitutes an atypical fact which must lead the AMLCO to update the individual assessment of the risks associated with this customer and to re-examine, with enhanced due diligence, the transactions that have been carried out by him. However, it is necessary to proceed with caution, in order to avoid that the customer is explicitly or implicitly informed that a money laundering or terrorist financing analysis is ongoing or likely to be conducted, which would constitute a violation of the prohibition of disclosure set out in Article 55 of the Anti-Money Laundering Law, or in the case of indictments from judicial authorities, in order to avoid a violation of the secrecy obligation defined in Article 46quater, § 3, second paragraph, of the Code of Criminal Procedure. This may also be the case where the media reveal facts that may have a negative impact on the assessment of the financial institution's relationship with the customer concerned.

Likewise, the Bank considers that, in addition to being subject to the asset freezing obligations, where a financial institution finds that a customer, agent or beneficial owner of a customer is included in the Belgian list or a European list of persons subject to these measures, it should consider that this information affects the customer's risk profile. In this case, it is necessary to update the individual assessment of the risks associated with this customer and to re-examine, with enhanced due diligence, the transactions that have been carried out by him.

### 1.1.3. Operational obligations related to the detection of atypical facts and transactions

In order to effectively detect atypical transactions and facts, and in accordance with Articles 16 and 17 of the Anti-Money Laundering Regulation of the NBB, financial institutions must:

- (i) define the indicators/criteria to identify atypical facts and transactions;
- (ii) put in place a system for detecting atypical facts and transactions, including ex ante and ex post controls based on these indicators/criteria;
- (iii) develop a procedure for reporting atypical facts and transactions to the AMLCO.

## 1.2. Predefined indicators/criteria to identify atypical facts and transactions

Each financial institution should determine itself, on the basis of its overall risk assessment and of all relevant information, including the ML/FT typologies published by CTIF-CFI, which indicators/criteria lead to the facts or transactions being identified as atypical (Article 16, 1° of the NBB Regulation).

These indicators must be formalised in the internal procedure relating to the *due diligence with respect to business relationships and transactions* (Article 16, 2° of the NBB Regulation).

The NBB nevertheless considers that this list of criteria should always at least include criteria relating to:

- the objective characteristics of the transactions (e.g. unusually complex transactions or transactions of an unusually large amount);
- customer characteristics (e.g. cash transactions involving large amounts that cannot be explained by the customer's professional activity);
- the specific circumstances surrounding the transaction (e.g. an electronic funds transfer where the cash amount of the transfer seems to be collected under the supervision of third parties; e.g. new information from credible external sources).

The NBB considers that if a financial institution cannot demonstrate that it has developed adequate indicators to assess the atypical nature of facts and transactions of customers, it seriously fails to comply with the due diligence obligation.

### 1.3. System for detecting atypical facts and transactions

In order to comply with the obligation to carefully examine the transactions carried out in order to identify the atypical character of some of them, financial institutions should set up a system for monitoring and analysing occasional transactions and business relationships. This system should be based on two types of controls:

- i. **ex ante control** performed by the persons who, within the financial institution, are in direct contact with the customers and their transactions; and
- ii. **ex post control** of all transactions which have been carried out through the financial institution. In most cases, this control takes the form of a supplementary automated monitoring system, which is without prejudice to the controls that may be performed in real time, in particular in the context of the application of the European Regulation on Transfers of Funds).

#### 1.3.1. Ex ante control by persons who are in direct contact with customers or who are instructed with carrying out their transactions

Where, in order to establish business relationships or carry out transactions on behalf of customers, the financial institution interacts with these customers through its staff, agents or, in the case of electronic money institutions, distributors who are in direct contact with these customers or who are instructed with carrying out their transactions, the detection of atypical transactions may generally be entrusted in the first place to these persons. They must therefore be instructed, through the internal procedures of the financial institution, to contribute to exercising ongoing due diligence in order to detect atypical facts and transactions and to report them to the AMLCO as soon as they have knowledge of such facts or transactions.

In order for these persons to be able to fulfil their duties fully and effectively, the list of indicators/criteria referred to in point 1.2. above should be made available to them. In addition, the AMLCO must ensure that these persons receive (theoretical and practical) **training** about these indicators, to ensure that they have a proper knowledge of them and that they can easily apply them.

If the financial institution uses agents or, in the case of electronic money institutions, distributors, it must verify compliance with the relevant instructions through its internal control system.

For more information on these topics, see the pages "Policies, procedures, processes and internal control measures" and "Training and education of staff".

#### 1.3.2. Ex post control conducted by a monitoring system

In accordance with Article 17 of the Anti-Money Laundering Regulation of the NBB,, financial institutions should set up a monitoring system to detect atypical transactions that might not have been detected by the persons who are in direct contact with customers or who are instructed with carrying out their transactions. It should be noted that, in certain circumstances, for example where it is possible for the customer to initiate transactions directly via the internet without any involvement of staff members, agents or distributors of the financial institution, atypical transactions can only be detected by performing an ex post control. Therefore it is essential to ensure the effectiveness of this control.

This monitoring system should:

1. cover all customers' accounts and contracts and **all transactions** which have been carried out through the financial institution;
2. be based on **precise and relevant criteria** taking particular account of the characteristics of the institution's customers, the products, services or transactions that it offers, the countries or geographical areas concerned and the distribution channels that it uses, and be sufficiently discriminating to make it possible to detect atypical transactions effectively;
3. allow these transactions to be **detected rapidly**;
4. **be automated** (unless the financial institution can demonstrate that the nature, number and volume of transactions to be monitored do not require it (see below));
5. be subject to an **initial validation procedure** and a regular re-examination of its relevance with a view to adapting it, if necessary, in accordance with the development of the customer base targeted by the financial institution, the products, services or transactions that it offers, the countries or geographical areas concerned and the distribution channels that it uses.

As regards the **parameters** referred to in point 2 above, the criteria used should also take into account the specific ML/FT risk associated with transactions carried out by customers whose acceptance is subjected to stricter rules under the customer acceptance policy. The NBB draws attention to the fact that these parameters should exclusively aim at ensuring an efficient and discriminating detection of atypical transactions and that they may therefore not be essentially determined on the basis of the resources that the financial institution is prepared, in abstracto, to allocate to the analysis of reportings generated by the system.

The NBB therefore recommends that the parameters be based on the risk classification and the profile of the business relationships and that it be adapted to the transactions carried out by the institution (alert thresholds based on the elements of the business relationship; taking into account all transactions carried out in relation with accounts or contracts). The parameters must also be regularly updated, especially in light of the risk classification. They may not be based solely on an amount of transactions without taking into account the classification of customers or the knowledge of the business relationship.

Pursuant to Article 17, second paragraph, 4° of the Anti-Money Laundering Regulation of the NBB, the system for ex post detection of atypical transactions must not be automated if the nature, number and volume of transactions to be monitored do not require it. The NBB considers that this derogation should be applied with caution, and that the institution should demonstrate - both theoretically, ab initio, and later, on the basis of the experience gained from implementing the non-automated alternative system for ex post detection - that this derogation effectively allows efficient and discriminating ex post detection of atypical transactions that have not been detected ex ante. The NBB considers that the opinions of the senior manager and the AMLCO should be considered as decisive in the decision to adopt and maintain this alternative system. The NBB also expects the above demonstration to be in writing and to be provided to it immediately at its first request.

As the system for ex post detection of atypical transactions plays a crucial role in the ability of the financial institution to subject atypical transactions to the analysis required to determine whether they are suspect and, as a consequence, whether they must be reported to CTIF-CFI, the NBB expects financial institutions to take particular care in periodically monitoring the effectiveness of the system used, regardless of whether it is an automated system or a non-automated alternative system, and to address the deficiencies identified in this regard as soon as possible.

## 1.4. Procedure for reporting to the AMLCO

In all cases where an atypical fact or transaction is detected, whether in the context of an ex ante control or an ex post control, it is essential that it is reported as quickly as possible to the AMLCO, so that the latter can fulfil, before the deadline imposed by law, the duties assigned to him by Article 45 of the Anti-Money Laundering Law as regards the analysis of atypical facts or transactions or the reporting to CTIF-CFI. The mechanism for reporting to the AMLCO is ultimately aimed at allowing the financial institution to comply with its obligations regarding the reporting of suspicions to CTIF-CFI. However, it is recalled that, in principle, suspicion reports must be sent to CTIF-CFI before the transactions concerned are executed. Only when this is not possible can the report be sent to CTIF-CFI immediately after the execution of the transaction. Therefore the procedure for reporting atypical facts and transactions to the AMLCO must be highly efficient.

For this reason, the NBB expects financial institutions to lay down in their procedure that reportings must:

- i. be sent as soon as possible to the AMLCO;
- ii. include the reasons why the transaction concerned is considered atypical; and
- iii. be documented to the extent necessary to allow a pre-analysis and analysis to be conducted by the AMLCO.

As mentioned above, Articles 33, § 1, second paragraph, 34, § 3, second paragraph and 35, § 2, second paragraph of the Anti-Money Laundering Law provide that where financial institutions cannot fulfil their due diligence obligations, they must examine, in accordance with Article 46 of the Law, whether the causes of this inability are such as to raise ML/FT suspicions and whether CTIF-CFI should be notified. In order to satisfy this legal obligation, the procedure for reporting to the AMLCO must also be applied in these cases.

These reportings may be sent internally by email or via another channel. In urgent cases, atypical facts and transactions may be reported by phone. Such oral reportings must nevertheless be systematically confirmed, as soon as possible, in writing, and if necessary by email.

The NBB expects financial institutions to set up a system for archiving the various reports submitted in order to monitor the effectiveness and relevance of the reporting process. The internal procedures referred to in Article 8 of the Anti-Money Laundering Law must describe the practical procedures for submitting reports to the AMLCO, by drawing a distinction, where appropriate, according to the type of control exercised (ex ante or ex post).

The NBB also expects the staff training required by the Law (see the page "Training and education of staff") to ensure that persons who, in the performance of their duties, may have to submit such reports, are fully aware of this procedure.

For the steps that follow the transmission of a reporting to the AMLCO, see the page "Analysis of atypical transactions", which describes the procedure to be followed by the AMLCO for conducting the pre-analysis and subsequently, if applicable, the analysis.

## 1.5. Protection of persons who internally report facts or transactions they consider atypical

As mentioned above, the mechanisms for the detection of atypical facts and transactions and of cases in which the financial institution cannot fulfil its due diligence obligations are based inter alia on the attention and critical skills of the persons who are in contact with the customers and their transactions. In order for these mechanisms to be efficient, it is important that these persons do not feel fear of being penalised within the financial institution because they have reported such a transaction or situation to the AMLCO. They must also be protected from any threat or hostile action external to the financial institution, in particular where such threats or action are perpetrated by the customer concerned or by persons related to him.

According to Article 36 of the Anti-Money Laundering Law, financial institutions must take reasonable measures to ensure that their staff members, agents and, in case of electronic money institutions, distributors who report a transaction they consider atypical, are protected from being exposed to any threats or hostile action, including, within the institution, from any adverse or discriminatory employment actions.

Specifically, the NBB recommends that financial institutions put in place measures to ensure that the identity of persons who have reported atypical facts and transactions and of persons who have taken part in the collection and evaluation of related information is known within the financial institution and, a fortiori, outside the financial institution, only by persons for whom such information is necessary or useful for the performance of their duties in the field of AML/CFT.

## 2. Updating of the data or information and of the individual risk assessment

### 2.1. Updating of the data or information

A second implication of the ongoing due diligence obligation is that financial institutions must keep up to date the data or information they hold pursuant to their obligation to identify and verify the identity and their obligation to identify the characteristics of the customer as well as the purpose and nature of the business relationship or the occasional transaction.

This updating obligation is an important prerequisite for detecting atypical transactions: if the financial institution cannot rely on current information, the ongoing due diligence measures with respect to the transactions described above may not allow to identify the atypical character of some of them or, conversely, transactions could unnecessarily be treated as atypical whereas they would have been considered as not requiring special attention if the information held by the institution had been updated.

In principle, this updating obligation applies as soon as the relevant elements that are taken into account in the context of the individual risk assessment are modified. However, in complying with this obligation, a risk-based approach should be adopted. It follows that the measures taken by the financial institutions to fulfil this obligation should be proportional to the risk identified in the context of the individual risk assessment referred to in Article 19, § 2, first paragraph of the Anti-Money Laundering Law. However, it should be noted that the updating of data and information is of particular importance where elements relevant to the individual risk assessment appear to be no longer current. The financial institutions must also take into account this potentially higher level of ML/FT risk presented by a given situation in determining the updating measures to be taken.

Pursuant to Article 35, § 1, second paragraph of the Anti-Money Laundering Law, the update must cover all the data collected in the context of the initial identification, and not only part of this data. Similarly, the verification of the updated data may not be less comprehensive than that of the initial identification data.

The obligation of financial institutions to update the information they hold about their customers includes the obligation to implement measures to identify the persons among their customers whose individual situation has changed to such an extent that they fall within the scope of Articles 37 to 41 of the Anti-Money Laundering Law, which define cases in which special enhanced due diligence measures are required by law (see the page "Special cases of enhanced due diligence"). This is particularly the case for customers who have become politically exposed persons (PEPs), family members of PEPs or persons who are known to be closely associated with a PEP. See the page "Politically Exposed Persons" for more information on the enhanced due diligence measures required in case of identification of a PEP..

In addition to the requirements set out in Article 35, § 1, 2°, of the Anti-Money Laundering Law, financial institutions may consider it useful to periodically re-examine the information they hold to ensure that it is up to date. Such a periodic re-examination may be particularly indicated in cases of high risk. It should be noted, however, that this is a complementary precautionary measure which does not exempt the financial institution from updating the information it holds before the date of the next re-examination planned according to the internal procedures, if it knows or cannot be unaware that "*data relevant for the individual risk assessment referred to in Article 19 is modified*".

## 2.2. Updating of the individual risk assessment

As already mentioned, Article 35, § 1, fourth paragraph of the Anti-Money Laundering Law provides that updating the information collected may imply also updating the individual risk assessment and, where appropriate, adapting the extent or modalities of the due diligence measures implemented.

For example, significant changes in the management or beneficial ownership of customer companies, the activities or the socio-professional category of the customer, the establishment or severance of links with high-risk or low-tax or no-tax countries, the recent exercise of prominent public functions or, conversely, the termination since more than 12 months of the exercise of such functions, the extension of the use by the customer, within the framework of an existing business relationship, of products and services deemed to present higher risks according to the overall risk assessment or, conversely, the cessation of the use of these services, etc., can have a significant influence on the customer's risk profile and, consequently, on the nature and intensity of the due diligence measures to be implemented in respect of the transactions carried out.

It should be noted, however, that the updating of the individual risk assessment may be necessary due to "atypical facts" such as the receipt of information from credible external sources. This is the case when new events have occurred that may affect the customer's risk profile. This may be the case, in particular, where the financial institution receives an indictment from the judicial authorities or a request for information from CTIF-CFI concerning the business relationship with a customer or the transactions carried out by the latter (see point 1.1. above).

It is also recalled that under Article 22 of the Anti-Money Laundering Regulation of the NBB, a financial institution which has reported suspicions pursuant to Article 47 of the Anti-Money Laundering Law, should carry out an individual re-assessment of ML/FT risks, in accordance with Article 19, § 2, of the Law, taking account of the specific fact that a suspicion has been raised about the customer concerned, in order to decide whether to maintain the business relationship, in which case it should implement due diligence measures adapted to the re-assessed risks, or to end it (see in this regard the page "Reporting of suspicions"). The same is expected in case of receipt of an indictment from judicial authorities.

Finally, as a reminder, updating the overall risk assessment in accordance with Article 17 of the Anti-Money Laundering Law may also imply updating the individual risk assessment.

### 3. 3. Inability to exercise ongoing due diligence

Article 35, § 2 of the Anti-Money Laundering Law describes the consequences of the inability to fulfil the ongoing due diligence obligation.

As this obligation must be fulfilled throughout the business relationship, the Anti-Money Laundering Law distinguishes between future customers and existing customers.

#### 3.1. With regard to future customers

Apart from the cases in which the financial institution is unable to identify the persons involved in the business relationship or the occasional transaction and to verify their identity in due time (see the page "Non-compliance with the identification and identity verification obligations") or to gather the information necessary to understand the characteristics of the customer and the purpose and intended nature of the business relationship or transaction (see the page "Identification of the customer's characteristics and of the purpose and nature of the business relationship or the occasional transaction"), the law also prohibits to enter into a business relationship or to carry out a transaction on behalf of the customer where the financial institution has, in advance, reason to believe that it will not be able to meet its ongoing due diligence obligations with respect to the business relationship and the transactions of this potential customer.

In the case of occasional transactions, the impossibility to carry out the required careful examination of the transaction will generally result from the inability to identify the persons involved and to verify their identity and/or identify the customer's characteristics or the purpose and nature of the transaction.

In the case of business relationships the financial institution intends to establish, the prohibition applies if the financial institution has reasons to consider, from the outset, that it will not be able to comply with its future obligations to update the identification of the persons involved and the verification of their identity, to update the information it holds concerning the customer's characteristics or the purpose and nature of the business relationship, or to carefully examine the transactions carried out by the customer during the business relationship.

Any refusal to enter into a business relationship with a potential customer or to carry out an occasional transaction that he wishes to perform must be duly justified. This refusal may not be a means for the financial institution to discriminate against certain categories of customers (see the page "Due diligence requirements and compliance with other legislation").

#### 3.2. With regard to existing customers

Where the financial institution finds, in the course of a business relationship, that it can no longer satisfy its ongoing due diligence obligation with regard to the transactions carried out by the customer or update the data and information about the persons involved or the characteristics of the business relationship, it has a legal obligation to terminate this relationship. However, pursuant to Article 33, § 1, third paragraph of the Anti-Money Laundering Law, financial institutions may apply restrictive measures other than the termination of the business relationship in the specific cases detailed in Article 15 of the Anti-Money Laundering Regulation of the NBB:

- **in the case of life insurance contracts**, the unilateral termination of which is contrary to other mandatory legal or regulatory provisions or public policy provisions, the alternative restrictive measures to be applied

consist in refusing payment of any supplementary premiums by the policyholder, without prejudice to the consequences that legal or regulatory provisions attach to non-payment of a premium (Article 15, first paragraph, 1° of the Regulation);

- **in the case of loan contracts**, the unilateral termination of which would expose the obliged financial institution to a severe and disproportionate negative impact, the alternative restrictive measures to be applied consist in refusing any increase in the amount lent and in terminating the business relationship as soon as possible (Article 15, first paragraph, 2° of the Regulation). Examples of a severe and disproportionate negative impact are the impossibility, in practice, to obtain reimbursement of substantial amounts or the loss of the benefit of real or personal guarantees attaching to the loan. The financial institution must also seize the first opportunity available to terminate the loan without suffering the aforementioned negative impact.

The NBB considers that the decision to apply alternative restrictive measures must be substantiated in writing on a case-by-case basis:

- in the case of restrictive measures other than the termination of life insurance contracts, this substantiation must include a verification that the legislation in force does not authorise the insurance company to unilaterally terminate the contract;
- however, in the case of measures other than the termination of a loan, Article 15, first paragraph, 2° of the Anti-Money Laundering Regulation of the NBB subjects the authorisation to implement such measures to the condition that the unilateral termination of the loan would expose the obliged financial institution to a severe and disproportionate negative impact. The NBB therefore considers that the decision to apply these measures must be substantiated in writing on a case-by-case basis, and that this written statement must include an estimate of the negative impact to which such unilateral termination would expose the financial institution, in order to demonstrate its serious and disproportionate nature, and determine the date or future events that will allow the institution to terminate the business relationship as soon as possible without suffering the aforementioned severe and disproportionate negative impact.

In all these cases, the financial institution must also take the necessary measures to ensure that it does not enter into any other business relationship with the customer concerned and does not execute any occasional transaction on his behalf.

With regard to the business relationship which is subject to the alternative restrictive measures, the financial institution must also take enhanced due diligence measures, in accordance with Article 37, § 2 of the Anti-Money Laundering Law, which are proportionate to the level of re-assessed risk, in accordance with Article 19, § 2 of the Anti-Money Laundering Law, taking into account that this relationship has not been terminated (see the page "Special cases of enhanced due diligence". This enhanced due diligence must also enable the institution to ensure that the restrictive measures are effectively implemented and that the loans are terminated as soon as possible.

The modalities for implementing alternative restrictive measures must be specified in the internal procedures of the financial institution (see the page "Policies, procedures, processes and internal control measures").

### 3.3. Reporting to the AMLCO

In accordance with Article 46 of the Anti-Money Laundering Law, financial institutions must also verify whether it is necessary to inform CTIF-CFI of cases as referred to above in which the ongoing due diligence obligation could not be satisfied, where this inability can be an indication of ML/FT. This means that this inability should be recorded in writing within the financial institution and reported to the AMLCO. See chapters 1.1. and 1.3. above. The modalities of this recording in writing and of this reporting must be specified in the internal procedures of the financial institution (see the page "Policies, procedures, processes and internal control measures »).

## 4. Internal control measures

Financial institutions are expected to periodically verify that the internal procedures for exercising due diligence with regard to customers and transactions are consistently complied with and that the processes for implementing the ongoing due diligence obligations (examination of transactions and updating of information) are adequate.

The NBB therefore recommends that the internal audit function pay particular attention to:

- the adequacy of the indicators/criteria validated by the financial institution to enable atypical facts and transactions to be detected by persons who are in direct contact with customers or who are instructed with carrying out their transactions;
- the effectiveness of the system for ex ante detection of atypical facts and transactions, taking into account in particular the number of alerts generated;
- the effectiveness of the system for ex post detection of atypical facts and transactions and, in particular, the adequacy of the configuration of the automated monitoring system, taking into account in particular the number of alerts generated;
- the adequacy of the updating of the information held pursuant to the obligation to identify and verify the identity and the obligation to identify the customer's characteristics and the purpose and nature of the business relationship;
- the adequacy of the measures taken to protect persons who internally report a fact or transaction they consider atypical.

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



# Anti-Money Laundering Law of 18 September 2017 - Articles 35 and 36

## Art. 35

§ 1. Obligated entities shall, with regard to the business relationship, exercise ongoing due diligence proportionate to the risk level identified in accordance with Article 19, § 2, first subparagraph, which involves, among other things:

1° carefully examining the transactions carried out over the course of the business relationship as well as, where necessary, the origin of the funds, in order to verify whether these transactions are consistent with the customer's characteristics, with the nature and purpose of the business relationship or of the intended transaction, and with the customer's risk profile, in order to detect atypical transactions that should be subjected to an in-depth analysis in accordance with Article 45;

2° updating the data held in accordance with Sections 2 and 3, particularly when data relevant for the individual risk assessment referred to in Article 19 is modified.

The data referred to in the first paragraph, 2°, shall be updated and verified in accordance with Articles 26 to 29.

In the framework of updating the information they keep on their customers, obliged entities shall implement measures as referred to in Article 41, § 1, 1°, that enable them to identify which of their customers have become politically exposed persons, family members of politically exposed persons or persons who are known to be closely associated with politically exposed persons; where appropriate, a member of senior management shall decide whether or not to continue the business relationship, and the other enhanced due diligence measures laid down in Article 41, § 1, shall apply.

Without prejudice to Article 17, third subparagraph, updating the information in accordance with the third paragraph shall imply, where this is relevant, also updating the individual risk assessment referred to in Article 19, § 2, first paragraph, with regard to the customers concerned and, where appropriate, adapting the extent of the ongoing due diligence measures implemented.

§ 2. If obliged entities have reasons to consider that they will not be able to fulfil their obligation referred to in paragraph 1, they may neither establish a business relationship with or carry out a transaction for the customer concerned. Moreover, if they cannot fulfil that same obligation with regard to their existing customers, they shall terminate any already established business relationship or, where appropriate, apply the alternative restrictive measures referred to in Article 33, § 1, third subparagraph.

In the cases referred to in the first subparagraph, obliged entities shall examine, in accordance with Article 46, whether the causes of the inability to fulfil the obligation referred to in the first subparagraph could raise ML/FT suspicions and whether CTIF-CFI should be notified.

§ 3. Paragraph 2 shall not apply to the obliged entities referred to in Article 5, § 1, 23° to 28°, with the strict proviso that they ascertain the legal position of their customer or perform the task of defending or representing that customer in, or concerning, judicial proceedings, including providing advice on instituting or avoiding such proceedings.

## Art. 36

Each obliged entity shall ensure that its staff, agents and distributors who internally report a transaction they consider atypical within the meaning of Article 35, § 1, 1°, or who report that the entity is unable to fulfil the due diligence requirements referred to in Articles 33, § 1, 34, § 3 and 35, § 2, are protected from being exposed to threats or hostile action, and in particular from adverse or discriminatory employment actions.



# NBB anti-money laundering regulation of 21 November 2017 - Articles 15, 16 and 17

## Art. 15

If obliged financial institutions cannot fulfil their obligations to identify and verify the identity of a customer, or the customer's agents or beneficial owners within the time limits referred to in Articles 30 and 31 of the Law, or their obligations to keep these identification data up to date in accordance with the Law, they may apply restrictive measures as an alternative to ending the already established business relationship, as required pursuant to Article 33, § 1, 1st indent, of the Law, if it consists of:

1° a life insurance contract, unilateral termination of which is contrary to other mandatory legal or regulatory provisions or public policy provisions. In this case, the obliged financial institution may refuse payment of any supplementary premium by the policyholder, without prejudice to the consequences that the legal or regulatory provisions attach to non-payment of a premium;

2° a loan contract, unilateral termination of which would expose the obliged financial institution to a severe and disproportionate negative impact. In this case, the obliged financial institution shall refuse any increase in the amount lent and shall terminate the business relationship as soon as possible.

In the cases referred to in the 1st indent, obliged financial institutions shall apply, with regard to the business relationship, customer due diligence measures proportional to the level of re-assessed risk, in accordance with Article 19, § 2, of the Law, taking account of the fact that this business relationship has not been terminated. Moreover, obliged financial institutions shall refuse to enter into any other business relationship with the customer concerned and to carry out any occasional transaction on behalf of this customer.

## Art. 16

Obliged financial institutions shall set out in writing for their staff who are in direct contact with customers or instructed with carrying out their transactions:

1° the appropriate criteria enabling them to detect atypical transactions;

2° the procedure required to subject these transactions to a specific analysis under the responsibility of the AMLCO, in accordance with Article 45, § 1, of the Law, so as to determine whether these transactions may be suspected of being associated with money laundering or terrorist financing.

## Art. 17

Obliged financial institutions shall set up a monitoring system for detecting any atypical transactions which might not have been detected by their staff who are in direct contact with customers or instructed with carrying out their transactions.

This monitoring system must:

1° cover all customers' accounts and contracts and all their transactions;

2° be based on precise and relevant criteria fixed by each obliged financial institution taking particular account of the characteristics of its customers, the products, services or transactions that it offers, the countries or geographical areas concerned and the distribution channels that they use, and be sufficiently discriminating to make it possible to detect atypical transactions effectively;

3° allow these transactions to be detected rapidly;

4° be automated, unless the obliged financial institution can demonstrate that the nature, number and volume of transactions to be monitored do not require it;

5° be subject to an initial validation procedure and a regular re-examination of its relevance with a view to adapting it, if necessary, in accordance with the development of the customer base targeted by the obliged financial institution, the products, services or transactions that it offers, the countries or geographical areas concerned and the distribution channels that they use.

The criteria referred to in paragraph 2, 2nd indent, shall notably take into account the specific ML/FT risk associated with transactions carried out by customers whose acceptance has been subjected to stricter rules under the customer acceptance policy referred to in Title 3.

# Explanatory Memorandum to the Anti-Money-Laundering Law of 18 September 2017 - Articles 35 and 36

## Art. 35

Article 35, § 1 of the draft Law defines the obligation of ongoing due diligence. This constitutes the third component of the general due diligence obligations as well as the extension (i) to the obligation of identification and verification of the identity, and (ii) to the obligation of identification of the customer's characteristics and the nature and purpose of the business relationship.

The obligation of ongoing due diligence is currently referred to in Article 14, § 1, first indent of the Law of 11 January 1993, which is taken over by § 1 of this Article in the draft Law, subject to a few nuances.

As is the case with the two first components of the general due diligence obligations, the obligation of ongoing due diligence is subject to the risk-based approach: the intensity of the ongoing due diligence that the obliged entities are obliged to exercise must be proportionate to the level of risk identified as part of the individual risk assessment referred to in Article 19, § 2, first paragraph, of this draft Law, taking into account, where necessary, the update to this assessment.

The level of ongoing due diligence must also take into account the high level of risks associated with the situations referred to in Chapter 2 below.

§ 1, first indent of draft Article 35 specifies that the obligation of ongoing due diligence involves two aspects.

The first consists of carefully examining the transactions carried out over the course of the business relationship as well as, if necessary, the origin of the funds. This takes over Article 14, § 1, first paragraph of the Law of 11 January 1993. The purpose of this examination required by this provision is to verify whether these transactions are consistent with the customer's characteristics, with the nature and purpose of the business relationship or of the intended transaction, and with the customer's risk profile. This examination aims to detect atypical transactions that require special attention in accordance with draft Article 45.

These transactions may be considered atypical both for their objective characteristics and for the customer's characteristics. The first category encompasses abnormally complex transactions for an unusually high amount, as well as transactions which are intrinsically unusual with no apparent economic justification or legitimacy. The second category encompasses transactions that do not appear consistent with the customer's profile. By way of example, these could be transactions in cash for significant amounts that do not appear to be able to be explained by the customer's professional activity. Transactions may also be considered atypical because of the specific circumstances surrounding them. For example, this could be the case when a beneficiary of an electronic funds transfer seems to operate under the oversight of third parties when he/she proceeds with paying in cash for the amount of the transfer.

In practice, detecting atypical transactions rests in the first place on the attention and critical thinking of persons who, within the obliged entity, are in direct contact with the customers and their transactions, and who can exercise an *ex-ante* check of these transactions and detect, based on methods and criteria determined by internal procedures, transactions that should be considered atypical.

Where appropriate based on the characteristics of the obliged entity, and without prejudice to the real-time checks that need to be carried out, especially as part of the application of the European Regulation on funds transfers, the *ex-ante* check must be supplemented by an *ex-post* check of all the transactions with which the obliged entity has assisted in order to detect the atypical transactions that could not be detected with the *ex-ante* check. Where applicable, the effectiveness of this *ex-post* check requires it to be conducted using an automated system.

In this respect, we point out that under certain circumstances such as for example where the customer can directly initiate the transactions through the internet with no intervention by a member of staff, by an agent or by a distributor of the obliged entity, only this *ex-post* check is able to detect atypical transactions. The importance of its effectiveness is therefore heightened.

Just like all the due diligence obligations, the ongoing due diligence on transactions must be exercised through a risk-based approach. It follows that especially the nature, intensity and frequency of the due diligence measures applied to a customer's transactions, both as part of an *ex-ante* check and an *ex-post* check should be proportionate to the risk identified as part of the individual risk assessment associated with this customer (cf. Article 19, § 2, first paragraph).

In all cases where an atypical transaction is detected, a report should be sent to the AMLCO so that he/she may assume the responsibilities allocated by Article 45 of this draft Law (see below). For the sake of efficiency, these warnings should furthermore include a communication of the reasons for which the transaction concerned is considered atypical. This mechanism of reporting to the AMLCO must moreover take into account its aim in order to allow the obliged entity to meet its obligations of reporting of suspicions to the CTIF-CFI in accordance with Title 4, Chapter 2 of the draft Law (see below). It must therefore in particular take into account that in principle, reports of suspicions should be sent to the CTIF-CFI prior to executing the transactions concerned or, where this is not possible, immediately after their execution (see draft Article 51).

Each obliged entity should therefore define, in its internal procedures referred to in draft Article 8, and implement effective mechanisms adapted to its own characteristics with the purpose in part of submitting the transactions to appropriate checks (both *a priori* and *a posteriori* as the case may be) to detect atypical transactions and also to report as quickly as possible to the AMLCO any atypical transactions detected through the checks.

Where applicable, the supervisory authorities referred to in draft Article 85 may make use of the powers granted to them by Article 86 to specify, through circulars or other forms of guidelines or, where they deem it necessary, through a regulation, the methods for implementing these obligations.

The second aspect of ongoing due diligence consists of keeping updated the information gathered by the obliged entity in the fulfilment of its obligation of identification and verification of the identity, as well as the obligation of identification of the customer's characteristics and the nature and purpose of the business relationship. In this respect, it should be pointed out that the mere fact of documents being out of date is not in and of itself a trigger for the obligation of updating (for example at the time of expiry of the identity card). It is the fact that the information is out of date that is. However, the update must occur in particular when there is a change to the pertinent aspects taken into account as part of the individual risk assessment. In the Law of 11 January 1993, this obligation to update comes up in several Articles (especially Articles 7 and 8), which could seem to downplay its importance. The present draft Law clarifies that it does in reality constitute an important component of the obligation of ongoing due diligence. If up-to-date information is not used, the ongoing due diligence measures on transactions described above may not allow the atypical nature of some of them to be identified.

The obligation to update data and information must also give rise to a risk-based approach. It follows that the measures taken by the obliged entities to fulfil this obligation must be proportionate to the risk identified as part of the individual risk assessment referred to in Article 19, § 2, first paragraph. It should be emphasised that the update of the data and information is especially important when it seems that aspects pertinent to the individual risk assessment are no longer up to date, meaning that a renewed assessment could lead to the attribution of a higher risk level for the customer concerned (see the fourth paragraph below of the same Article 35, § 1). It is important that the obliged entities also take into account this potential increase in the level of risk to determine the updating measures they put in place.

During the update, the second paragraph of draft Article 35, § 1 specifies that there may not be less data gathered to identify the person than that gathered during the initial identification. In the same way, the verification of the updated data may not be less strict than that of the initial identification data. This is not expressly stated in the Directive but is inherent to its logic.

However, the obligation of the obliged entities of updating the information they keep on their customers, includes that of taking measures to enable them to identify, among their customers, those whom over the course of the business relationship have become PEPs, family members of PEPs or persons known to be close associates of PEPs (draft Article 35, § 1, third paragraph). In such a case, a member of a higher level of hierarchy must decide whether or not to maintain the business relationship, and the other enhanced due diligence measures provided for in Article 41 apply. This is a requirement from the FATF Recommendations.

As already stated below, draft Article 35, § 1, fourth paragraph provides that the updating of the information gathered may imply that it is necessary to proceed with updating the individual risk assessment and, where applicable, adapt the extent of the ongoing due diligence measures implemented. As a reminder, updating the overall risk assessment in accordance with Article 17 may also imply updating the individual risk assessment.

Draft Article 35, § 2, describes the consequences of the inability to fulfil the obligation of ongoing due diligence. Because this obligation must be fulfilled throughout the business relationship, this § 2 distinguishes between existing customers and future customers:

- *as regards existing customers:* if the obliged entity identifies that it can no longer fulfil the obligation of due diligence with regard to its existing customers, it shall terminate any already established business relationship or, where appropriate, apply the alternative restrictive measures referred to in Article 33, § 1, third sub-paragraph;
- *as regards future customers:* if the obliged entities have reasons to consider that they will be unable to comply with the obligation of due diligence during that business relationship, they may neither establish the business relationship nor carry out a transaction, especially a transaction through a bank account for that client. Refusal to establish a business relationship with a future customer (or to carry out a transaction) must be correctly justified. It may not serve as a means for the obliged entity to discriminate between certain categories of customers.

It should be noted that Article 14, § 4 of the Directive does not cover the inability to fulfil the general due diligence obligations referred to in Sections 2 and 3 of the present draft Law. It does not refer to the obligation of ongoing due diligence. It should however be reminded that the identification and verification of the identity of the persons concerned, and the understanding of the customer's characteristics and the envisaged nature and purpose of the business relationship or the transaction have the essential aim of enabling the exercise of ongoing due diligence to detect atypical transactions and ultimately report suspicious transactions to the CTIF-CFI. It therefore seems that the inability to exercise ongoing due diligence must have similar consequences to the inability to fulfil the two foregoing obligations with which they form a coherent whole.

The obliged entities must furthermore examine, in accordance with Article 46 of the draft Law, whether the CTIF-CFI needs to be notified of the cases in which the obligation of ongoing due diligence was unable to be fulfilled. This implies that the inability to fulfil the aforementioned obligation must be established within the obliged entity and must be reported to the AMLCO. The methods to establish and report this should be specified in the internal procedures referred to in draft Article 8.

Subject to meeting the conditions provided for, § 3 derogates from § 2 for lawyers, notaries, company auditors, auditors, audit firms, external chartered accountants, external tax consultants, registered external accountants and registered external tax accountants.

## Art. 36

The mechanisms for detecting and analysing suspicious transactions and cases in which the obliged entity is not able to fulfil its due diligence obligations rest in the first place on the attention and critical thinking of persons whom, within the obliged entity, are in first-line contact with the customers and their transactions. In order for these mechanisms to be effective, these persons must not experience any fear of being penalised within the obliged entity because they have reported such a transaction or such a situation to the AMLCO. They must also be protected from any threat or any hostile action external to the obliged entity and especially from those that could come from the customer concerned or the persons associated therewith. Draft Article 36 states that obliged entities must take reasonable measures to ensure the protection of their members of staff, agents or distributors who find themselves in this situation from threats or hostile action, including internal adverse or discriminatory employment actions.





# Special cases of enhanced due diligence

Home > Financial oversight > Combating money laundering and the financing of terrori...

**Explanatory Memorandum to the Anti-Money-Laundering Law of 18 September 2017**

- **General commentary on due diligence**

---

**Identity verification over the course of the business relationship: Comments and recommendations by the NBB**

**High-risk third countries**

**States with low or no taxes**

**Correspondent relationships**

**Politically exposed persons (PEPs)**

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



# Identity verification over the course of the business relationship and implementation of measures as an alternative to terminating a business relationship

Home > Financial oversight > Combating money laundering and the financing of terrori...

## Legal and regulatory framework

- Anti-Money Laundering Law: Article 37

## Explanatory Memorandum of the Anti-Money Laundering Law

- Article 37

## Comments and recommendations by the NBB

- Comments and recommendations

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



## Anti-Money Laundering Law of 18 September 2017 - Article 37

### Art. 37

§ 1. In the cases referred to in Article 31, both the measures taken for the purpose of verifying the identity of the persons referred to in Articles 21 to 24 and the transactions carried out in the context of the business relationship shall be subject to enhanced due diligence until the identity of all persons concerned has been verified. Any anomaly, including the inability to verify the identity of the aforementioned persons as soon as possible, shall be analysed and documented in a written report as laid down in Article 45.

§ 2. If they implement the alternative restrictive measures referred to in Articles 33, § 1, 34, § 3 and 35, § 2, obliged entities shall exercise enhanced due diligence with regard to the business relationships concerned.



# Explanatory Memorandum to the Anti-Money-Laundering Law of 18 September 2017- Article 37

## Art. 37

Paragraph 1 of this draft provision relates to the case in which the identity of the persons who need to be identified is verified over the course of the business relationship rather than when it begins (cf. Article 31). In this case, as regards the measures taken to verify the identity of the persons and the transactions executed as part of the business relationship, enhanced due diligence must be exercised until the identity of all persons involved has been verified. For every anomaly, including the impossibility of verifying the identity of the persons specified as quickly as possible, an analysis is carried out and an internal report is drawn up as referred to in Article 45. This obligation is taken over from Article 3 of the CBFA Regulations.

Paragraph 2 relates to cases where obliged entities cannot fulfil one of the general due diligence obligations and apply restrictive measures other than ending the business relationship, because unilateral termination of the business relationship by the obliged entity is prohibited by other mandatory statutory provisions or public policy provisions, or if such a unilateral termination would have a severe and disproportionate negative impact on the entity (cf. Articles 33, § 1, third subparagraph, 34, § 3 and 35, § 2): in such cases, obliged entities must exercise enhanced due diligence with regard to the business relationships concerned. This enhanced due diligence is, by definition, proportionate to the high risk that the case described entails.

# Identity verification over the course of the business relationship: Comments and recommendations by the NBB

Home > Financial oversight > Combating money laundering and the financing of terrori...

## Contents

- 1. Target situations
- 2. Enhanced due diligence measures
- 3. Reporting to the AMLCO
- 4. Internal control measures

## 1. Target situations

Article 37 of the Anti-Money Laundering Law requires financial institutions to adopt enhanced due diligence measures with regard to certain business relationships that have been established even though not all due diligence obligations were fulfilled, in the following cases:

1. when a financial institution has made use of the possibility of derogation provided for in Article 31 of the Anti-Money Laundering Law and **deferred verification of the identity of a customer** (or, where appropriate, of his agent(s) or beneficial owner(s)) with whom a business relationship has been established recently, in a situation provided for by its internal procedures in which it is essential not to interrupt the conduct of business. In that case, the business relationship and the transactions carried out during it should be subject to enhanced due diligence **until the identities of all the persons concerned have been verified**;
2. when a financial institution has **implemented one of the measures as an alternative to terminating the business relationship** that are authorised by the NBB in Article 15 of its Regulation:
  - either because the financial institution has made use of the possibility of derogation provided for in Article 31 of the Anti-Money Laundering Law and **deferred verification of the identity of a customer** (or, where appropriate of his agent(s) or beneficial owner(s)) with whom a business relationship has been established recently, in a situation provided for by its internal procedures in which it is essential not to interrupt the conduct of business, and because it is **unable to verify the identities of the persons involved as soon as possible after first contact with the customer** (case referred to in Article 33, § 1, of the Law);
  - or because it finds, during the business relationship, that it can **no longer fulfil its ongoing due diligence obligation** with regard to the transactions carried out by the customer or **update** the data and information pertaining to the persons involved or the characteristics of the relationship (case referred to in Article 35, § 2).

In these situations, since the Law in principle requires that the business relationship (which, by definition, has already been established) be terminated, financial institutions should adopt enhanced due diligence measures in addition to the measures applied as an alternative to ending the business relationship in accordance with Article 15 of the Anti-Money Laundering Regulation of the NBB.

## 2. Enhanced due diligence measures

The enhanced due diligence measures to be implemented pursuant to Article 37 of the Anti-Money Laundering Law should be proportionate with the reassessed risk level, in accordance with Article 19, § 2, of the Law. For more information on this subject, see the page “General commentary on cases of enhanced due diligence”, the content of which is taken from the Explanatory Memorandum of the Anti-Money Laundering Law. .

The NBB recommends determining the intensity of the due diligence measures to be implemented in the institution's internal procedures, depending on whether there are other factors indicative of high risk associated with the transaction or business relationship, in accordance with the individual risk assessment required by the aforementioned Article 19 of the Law (see the page “Individual risk assessment”). To that end, all characteristics of the transaction or business relationship should be taken into consideration, particularly its nature and purpose and the amounts involved.

Generally, pending verification of the identity of the persons involved, the specific framework of the business relationship should include a set of coherent measures which drastically limit the possibilities offered to the customer in the context of this business relationship during this period. For example, it could be envisaged deferring the settlement of the transactions, limiting the sources of funding for the account opened to a single other bank account opened in name of the customer with a credit institution established in the EEA or in an equivalent third country, etc.

If one of the measures as an alternative to terminating the business relationship referred to in Article 15 of the Anti-Money Laundering Regulation of the NBB is applied, the additional enhanced due diligence measures to be adopted should be determined taking into account that this relationship has not been ended. The enhanced due diligence measures should in particular enable the financial institution, in that case, to ensure that the restrictions imposed on the business relationship are actually implemented and complied with.

## 3. Reporting to the AMLCO

It should be highlighted that, as soon as there could be indications of ML/FT, (i) any anomaly in the functioning of a business relationship for which a financial institution has made use of the possibility of derogation referred to in Article 31 of the Anti-Money Laundering Law and deferred verification of the identities of the persons involved and, in the same situation, (ii) any anomaly in the verification process, including an inability to verify the identities of the persons concerned as soon as possible after first contact with the customer, as well as (iii) any inability to continue fulfilling the ongoing due diligence obligation during a business relationship or to update the information pertaining to the persons involved and the characteristics of the business relationship concerned, should be considered an “atypical fact” and be subject to a specific analysis and documented in an internal report under the responsibility of the AMLCO in accordance with Article 46 of the Law to determine whether a suspicion should be reported to CTIF-CFI (see Articles 37, § 1, and 35, § 2, second paragraph, of the Law).

This implies that the aforementioned anomalies or inability should first be established and reported to the AMLCO, the details of which should be specified in the internal procedures adopted by the financial institution pursuant to Article 8 of the Anti-Money Laundering Law (for more information on this subject, see the page “Policies, procedures, processes and internal control measures” and point 1.4 of the page “Ongoing due diligence and detection of atypical facts and transactions”).

## 4. Internal control measures

Financial institutions are expected to periodically and permanently monitor the adequacy of the organisational measures implemented to comply with the enhanced due diligence measures for the verification of the identity of the persons involved in a business relationship during the said relationship or for implementing measures as an alternative to ending a business relationship. In this respect, the NBB expects the internal audit function in particular to pay specific attention to the adequacy and effectiveness of the enhanced due diligence measures adopted by the financial institutions.

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



## High-risk third countries

Home > Financial oversight > Combating money laundering and the financing of terrori...

### Legal and regulatory framework

- Anti-Money Laundering Law: Article 38

### Explanatory Memorandum of the Anti-Money Laundering Law

- Article 38

### Other reference documents

- ESAs Risk Factor Guidelines dated 4 January 2018
- Commission Delegated Regulation (EU) 2016/1675 of 14 July 2016 on high-risk third countries (for the updated annex and methodology, see the website of the European Commission – financial crime section)
- See the Treasury website

### Comments and recommendations by the NBB

- Comments and recommendations

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



# Anti-Money Laundering Law of 18 September 2017 - Article 38

## Art. 38

Obligated entities shall apply enhanced customer due diligence measures in the context of their relationships with natural or legal persons or with legal arrangements such as trusts or fiducies that are established in a high-risk third country.

Obligated entities that have established branches or majority-owned subsidiaries in high-risk third countries may, based on an individual risk assessment, authorise them to not automatically apply increased customer due diligence measures, provided that they ensure that the branches and subsidiaries concerned fully comply with the group-wide policies and procedures, in accordance with Article 13.

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



# Explanatory Memorandum to the Anti-Money-Laundering Law of 18 September 2017 - Article 38

## Art. 38

Article 38 relates to the case in which the obliged entity has entered into a business relationship with natural or legal persons or with legal arrangements established in a high-risk third country. In accordance with Article 4, 6° of the draft Law, a third country is high-risk when it is identified under Article 9 of Directive 2015/849 by the European Commission as a country that shows strategic deficiencies in its national AML/CFT regimes that pose a significant threat to the European Union's financial system (see the list of third countries concerned in the annex to Commission Delegated Regulation (EU) 2016/1675 of 14 July 2016 supplementing Directive (EU) 2015/849 of the European Parliament and of the Council by identifying high-risk third countries with strategic deficiencies), or that entails a geographical risk deemed high by the Ministerial Committee for the coordination of the fight against the laundering of money of illicit origin, the National Security Council or the obliged entity itself.

It should be noted that a strict interpretation of Article 18 of the Directive could lead to the belief that the enhanced due diligence measures are only required for customers established in high-risk third countries and included as such in the European Commission's list; Article 18, paragraph 3 of the Directive, however, obliges the Member States and obliged entities to take into account in their risk assessment the criteria set out in Appendix III of the Directive, including the geographical risk. It therefore seems logical that the obligation of enhanced due diligence applies to all high-risk countries regardless of the origin of the identification. Consequently, the definition of "high-risk country" covers all these cases so that the enhanced due diligence measures established by law are applied in all these cases identically.

In these cases, which by definition entail a high risk, the obliged entities apply their general enhanced due diligence measures to their customers.

The second paragraph also adds a nuance where the obliged entities concerned have established branches or majority subsidiaries in high-risk third countries. In these cases, the obliged entities may, based on a specific risk assessment, allow these branches or majority subsidiaries not to automatically apply enhanced due diligence measures, on the condition that they ascertain that their branches and majority subsidiaries fully comply with the policies and procedures that apply at a group level in accordance with Article 13.

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**

# High-risk third countries: Comments and recommendations by the NBB

Home > Financial oversight > Combating money laundering and the financing of terrori...

## Contents

- 1. Target situations
- 2. Enhanced due diligence measures
- 3. Possibility of derogation: Belgian parent companies
- 4. Internal control measures

## 1. Target situations

Article 38 of the Anti-Money Laundering Law requires enhanced customer due diligence measures to be implemented by financial institutions which carry out transactions on behalf of or establish or maintain business relationships with natural or legal persons or legal arrangements such as trusts or fiducies that are established in a high-risk third country.

In accordance with Article 4, 9°, of the Anti-Money Laundering Law, “**high-risk third country**” refers to:

- a third country (i.e. a non-EEA country) which has been **identified by the European Commission** as having strategic deficiencies in its ML/FT regimes that pose significant threats to the financial system of the European Union: in this respect, see the list of countries concerned annexed to Delegated Regulation (EU) 2016/1675 of 14 July 2016, which is updated regularly on the basis of a methodology established by the Commission (see the financial crime section of the Commission’s website); or
- a third country **identified by (i) the FATF, (ii) the Ministerial Committee tasked with coordinating the fight against the laundering of money of illicit origin, (iii) the National Security Council or (iv) the obliged entity itself** as presenting a high geographic risk: in accordance with Article 19, § 2, of the Anti-Money Laundering Law, entities should perform their risk assessment taking into account the criteria indicative of a potentially higher risk that are specified in Annex III to the Anti-Money Laundering Law, including geographic risk factors (see the page “Individual risk assessment”). Please also refer to the ESAs Risk Factor Guidelines dated 4 January 2018 in particular.

For more information on countries identified as “high-risk” countries, see the Treasury website. The NBB stresses that the obligation to adopt enhanced customer due diligence measures applies to all these countries, regardless of whether they have been identified as a “high-risk third country” by the European Commission, the FATF, the Ministerial Committee tasked with coordinating the fight against the laundering of money of illicit origin, the National Security Council or the obliged entity, and regardless of the capacity of the person established there (customer, agent or beneficial owner).

## 2. Enhanced due diligence measures

In accordance with Article 19, § 2, of the Anti-Money Laundering Law, the special case of enhanced due diligence referred to in Article 38 of the Law still requires an individual risk assessment taking account of all risk factors associated with the business relationship or occasional transaction, to determine the appropriate intensity of the enhanced due diligence measures to be implemented to adequately manage and reduce these risks. For more information on this subject, see the page “General commentary on cases of enhanced due diligence”, the content of which is taken from the Explanatory Memorandum of the Anti-Money Laundering Law, and the page “Individual risk assessment”.

The NBB recommends determining the intensity of the due diligence measures to be implemented in the institution’s internal procedures, based not only on the reasons behind the decision made at the international, European or national level or by the institution itself to qualify a country as a “high-risk” country – since these reasons and, therefore, the measures taken on this basis may differ significantly from one country to the other – but also on the (non-)existence of other high-risk factors associated with the transaction or business relationship concerned. To that end, all characteristics of the transaction or business relationship should be taken into consideration, particularly its nature and purpose and the amounts involved. The enhanced due diligence measures should also be applied in conjunction with any measures involving financial embargoes or asset freezing which may have been taken against the same countries (for more information on this subject, see the page “Financial embargoes and asset freezing”).

When a decision is made at the international, European or national level or by the institution itself to qualify a territory as a “high-risk country”, it is typically followed (i) by a listing of all business relationships established by the financial institution which somehow involve natural or legal persons or legal arrangements established in the country concerned, (ii) by a new examination of the risk level presented by these relationships on the basis of the information available regarding the country concerned, and (iii) a formal decision by the senior management to maintain or terminate the relationship.

### 3. Possibility of derogation: Belgian parent companies

When a parent company governed by Belgian Law is at the head of a group as defined in Article 4, 22°, of the Anti-Money Laundering Law (see the page “Definitions”) which includes **a branch or subsidiary established in a high-risk third country**, this parent entity should, in principle, require the branch or subsidiary concerned to implement enhanced due diligence measures with regard to all its local customers pursuant to Article 13, § 3, second paragraph, of the Anti-Money Laundering Law. However, Article 38, second paragraph, of the Anti-Money Laundering Law provides that financial institutions may “*based on an individual risk assessment, authorise [these branches and subsidiaries] to not automatically apply increased customer due diligence measures, **provided that they ensure that the branches and subsidiaries concerned fully comply with the group-wide policies and procedures***”.

For the measures which the NBB recommends applying when making use of this possibility of derogation, see point 3.2 of the page “Belgian parent companies”.

Finally, in accordance with Article 14 of the Anti-Money Laundering Law, it is recalled that financial institutions may never open a branch or representative office or directly or indirectly acquire or create a subsidiary in one of the countries designated by the King pursuant to Article 54 of the Law. As yet, however, no Royal Decree has been adopted with regard to a third country.

### 4. Internal control measures

Financial institutions are expected to periodically and permanently monitor the adequacy of the organisational measures implemented to comply with enhanced due diligence obligations imposed by Article 38 of the Anti-Money Laundering Law, which notably aim to ensure that each institution has a comprehensive knowledge of all the countries identified as “high-risk” countries at the international, European or national level. The NBB expects the internal audit function in particular to pay specific attention to the adequacy and effectiveness of the enhanced due diligence measures accordingly adopted by the financial institutions.

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



## States with low or no taxes

Home > Financial oversight > Combating money laundering and the financing of terrori...

### Legal and regulatory framework

- Anti-Money Laundering Law: Article 39
- Income Tax Code 1992: Article 179 (implementing Article 307, § 1, seventh paragraph, of the Income Tax Code 1992)

### Explanatory Memorandum of the Anti-Money Laundering Law

- Article 39

### Other reference documents

- ESAs Risk Factor Guidelines dated 4 January 2018

### Comments and recommendations by the NBB

- Comments and recommendations

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



## Anti-Money Laundering Law of 18 September 2017 - Article 39

### Art. 39

Obligated entities shall apply increased due diligence measures, particularly taking into account the risk of laundering money stemming from serious fiscal fraud, whether organised or not, as referred to in Article 4, 23°, k):

1° with regard to transactions, including the reception of funds, that are somehow linked to a State with low or no taxes included in the list established by Royal Decree in accordance with Article 307, § 1, seventh subparagraph of the Income Tax Code 1992; and

2° with regard to business transactions that involve carrying out transactions, including the reception of funds, which are somehow linked to a State referred to in 1°, or that somehow involve natural or legal persons or legal arrangements such as trusts that are established in such a State or that are governed by the law of such a State.



# Explanatory Memorandum to the Anti-Money-Laundering Law of 18 September 2017 - Article 39

## Art. 39

Draft Article 39 provides for a specific obligation of enhanced due diligence, meaning that an in-depth investigation needs to be conducted into all transactions and business relationships with which links of any kind are identified with tax havens included in the list drawn up in accordance with the Income Tax Code. In these cases, the obliged entities must especially investigate whether there are any suspicions of money laundering and in such cases report these suspicions to the CTIF-CFI in accordance with draft Article 47.



# States with low or no taxes: Comments and recommendations by the NBB

Home > Financial oversight > Combating money laundering and the financing of terrori...

## 1. Target situations

Article 39 of the Anti-Money Laundering Law requires financial institutions to adopt enhanced due diligence measures, “particularly taking into account the risk of laundering money stemming from serious fiscal fraud, whether organised or not”, with regard to:

- any transactions, including the reception of funds, that are somehow linked to a State with low or no taxes;
- any business relationships that:
- involve carrying out transactions, including the reception of funds, which are somehow linked to a State with low or no taxes; or
- somehow involve natural or legal persons or legal arrangements such as trusts or fiducies that are established in a State with low or no taxes or that are governed by the law of such a State.

“**State with low or no taxes**” refers to one of the tax havens listed by a Royal Decree implementing Article 307, § 1, seventh paragraph, of the Income Tax Code 1992. This list of tax havens, which was inserted in Article 179 of the Income Tax Code 1992 in 2010 (by Royal Decree of 6 May 2010, published in the Belgian Official Gazette of 12 May 2010), was updated by Royal Decree of 1 March 2016 (published in the Belgian Official Gazette of 11 March 2016).

It contains approximately 30 States which have no corporate tax system or where the corporate income tax falls below a specific nominal rate (10 %).

**As this list may change in the future, the NBB recommends that financial institutions take the measures necessary to ensure that their knowledge of it is permanently up-to-date.**

The NBB also stresses that, while Article 39 of the Anti-Money Laundering Law requires the adoption of enhanced due diligence measures with regard to transactions and business relationships that are linked to one of the States with low or no taxes listed in the Income Tax Code 1992, this obligation is **without prejudice to the obligation to apply enhanced due diligence measures with regard to any transaction or business relationship posing a high ML/FT risk, in accordance with Article 19, § 2, of the Anti-Money Laundering Law. From the perspective of the risk of laundering proceeds from serious fiscal fraud, whether organised or not, this includes transactions and business relationships which, while they do not have a link with the countries referred to in Article 39 of the Law, have a similar link with a country posing analogous risks.** In this respect, see the page “Ongoing due diligence and detection of atypical facts and transactions”.

## 2. Enhanced due diligence measures

The specific enhanced due diligence obligation provided for in Article 39 of the Anti-Money Laundering Law requires all transactions and business relationships identified as being somehow linked to one of the tax havens listed by the King to be subjected to a thorough examination. Where appropriate, this thorough examination should enable the financial institution detecting such a link to determine whether, in accordance with Article 47 of the Law, a suspicion

should be reported to CTIF-CFI concerning the transaction or business relationship, “particularly taking into account the risk of laundering money stemming from serious fiscal fraud, whether organised or not,” posed by it as a result of this link.

However, the NBB notes that, pursuant to the principle laid down in Article 47, § 1, second paragraph, of the Anti-Money Laundering Law, a financial institution should deem an atypical transaction suspicious as soon as the analysis of this transaction leads it to consider that it knows, suspects or has reasonable grounds to suspect that the funds concerned have an illicit origin, **potentially serious fiscal fraud, without also having to determine whether that fiscal fraud actually meets the legal conditions to qualify as “serious fiscal fraud, whether organised or not”**. It is the responsibility of CTIF-CFI, to which this suspicious transaction should be reported, to perform a more thorough analysis to discover whether there is underlying serious fiscal fraud. For more information on this subject, see point 2.1. of the page “Analysis of atypical facts and transactions”, and in particular the section dedicated to the laundering of money stemming from serious fiscal fraud, whether organised or not.

Furthermore, it should be noted that the enhanced due diligence measures to be implemented pursuant to Article 39 of the Anti-Money Laundering Law should be proportionate with the risk level assessed in accordance with Article 19, § 2, of the Law. For more information on this subject, see the page “General commentary on cases of enhanced due diligence”, the content of which is taken from the Explanatory Memorandum of the Anti-Money Laundering Law. The NBB consequently recommends determining the intensity of the due diligence measures to be implemented in the institution’s internal procedures, depending on whether there are other factors indicative of high risk associated with the transaction or business relationship concerned, in accordance with the individual risk assessment required by the aforementioned Article 19 of the Law (see the page “Individual risk assessment”). To that end, all characteristics of the transaction or business relationship should be taken into consideration, particularly its nature and purpose and the amounts involved.

Generally, the specific framework of a transaction or business relationship identified as being linked to a tax haven comprises **the adoption of measures aimed at determining, with an increased level of certainty,**

- the origin of the funds involved in the transaction concerned;
- and the identities of all persons involved in the business relationship concerned, regardless of whether they are natural or legal persons or legal arrangements such as trusts or fiducies and, in particular, the identities of the beneficial owners of these persons.

Indeed, in order to detect transactions or facts that could be linked to the laundering of proceeds of serious fiscal fraud, financial institutions should be fully aware of the identities of the natural persons who ultimately own or control the companies or legal arrangements with which they establish business relationships.

Article 23 of the Money-Laundering Law describes the obligation to identify the beneficial owners of customers that are companies or legal arrangements as a performance obligation; conversely, given that the obliged entity generally is not in direct contact with the beneficial owners, the obligation to verify their identity is legally defined as a best-effort obligation.

However, the obligations to identify and verify the identity of the parties involved in the business relationship are not merely administrative obligations: they must enable the financial institution to completely and effectively fulfil its due diligence obligations and, in particular, its ongoing due diligence obligations with regard to the business relationship, in order to perform a thorough analysis of the atypical transactions detected, so it can be determined whether there is a suspicion of money laundering and whether, as a result, the obligation to report suspicions to CTIF-CFI applies.

It should also be noted that, pursuant to Article 33, § 1, of the Anti-Money Laundering Law, when a financial institution can no longer fulfil its obligations to identify and verify the identity of the beneficial owners of a customer within the time limit required, it may neither establish nor maintain a business relationship with this customer.

### 3. Reporting to the AMLCO

It should be highlighted that, as soon as there could be an indication of ML/FT, any link identified between a (pre-existing or intended) transaction or business relationship and a tax haven may have to be considered atypical and should be subject to a specific analysis and documented in an internal report under the responsibility of the AMLCO, in accordance with Article 46 of the Law, to determine whether this link could lead to a suspicion of ML/FT and should therefore be reported to CTIF-CFI.

This implies that such a link should first be established and reported to the AMLCO. The internal procedures adopted by the financial institution pursuant to Article 8 of the Anti-Money Laundering Law should specify the cases in which the transaction concerned should be considered atypical based on this link as well as the procedures to be used for reporting these cases to the AMLCO (for more information on this subject, see the page “Policies, procedures, processes and internal control measures” and point 1.4 of the page “Ongoing due diligence and detection of atypical facts and transactions”).

## 4. Internal control measures

Financial institutions are expected to periodically and permanently monitor the adequacy of the organisational measures implemented to comply with the enhanced due diligence measures for transactions and business relationships linked to a tax haven.

In this respect, the NBB expects the internal audit function in particular to pay specific attention to the adequacy and effectiveness of the measures implemented by the institution concerned to:

- have permanent up-to-date knowledge of the list of countries considered “States with low or no taxes” within the meaning of Article 39 of the Anti-Money Laundering Law;
- identify any potential link between a transaction or business relationship and one of those tax havens;

fulfil the enhanced due diligence obligation required with regard to the transactions or business relationships for which such a link has been identified.

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



# Correspondent relationships

Home > Financial oversight > Combating money laundering and the financing of terrori...

## Legal and regulatory framework

- Anti-Money Laundering Law: Article 40

## Explanatory Memorandum of the Anti-Money Laundering Law

- Article 40

## Other reference documents

- ESA guidelines of 4 January 2018 on risk factors
- BCBS Guidelines dated June 2017 on Sound management of risks related to money laundering and financing of terrorism (see Annex 2)
- FATF Guidance dated 21 October 2016 on Correspondent Banking Services

## Comments and recommendations by the NBB

- Comments and recommendations

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



# Anti-Money Laundering Law of 18 September 2017 - Article 40

## Art. 40

§ 1. Obligated entities referred to in Article 5, § 1, 1°, 3° and 4°, that establish cross-border correspondent relationships with a respondent institution from a third country shall, in addition to the customer due diligence measures laid down in Chapter 1, take the following measures:

1° gather sufficient information about the respondent institution to understand fully the nature of the respondent's business and to determine from publicly available information the reputation of the institution and the quality of the supervision it is subject to;

2° assess the respondent institution's AML/CFT controls;

3° obtain approval from senior management before establishing new correspondent relationships;

4° document the respective responsibilities of each institution;

5° with respect to payable-through accounts, be satisfied that the respondent institution has verified the identity of, and performed ongoing due diligence on, the customers having direct access to accounts of the correspondent institution, and that it is able to provide relevant customer due diligence data to the correspondent institution, upon request.

§ 2. Obligated entities may neither establish nor continue a correspondent relationship with a shell bank, a credit or financial institution within the meaning of Article 3(1) and (2) of Directive 2015/849, or a credit or financial institution governed by the law of a third country, that is known to allow its accounts to be used by a shell bank.



# Explanatory Memorandum to the Anti-Money-Laundering Law of 18 September 2017 - Article 40

## Art. 40

Paragraph 1 of this draft provision relates to the case where a financial institution, as referred to in Article 5, § 1, 4° enters into cross-border correspondent relationships with a respondent institution from a third country.

By way of reminder, Article 4, 34° determines that a correspondent relationship involves the following:

- the provision of banking services by an obliged entity as referred to in Article 5, § 1, 1°, 3° and 4° (“correspondent institution”) to another institution (“respondent institution”) which may include, *inter alia*, providing a current or other liability account (for example, a term deposit account) and related services, such as cash management, international funds transfers, cheque clearing, payable-through accounts (i.e. accounts opened in the name of the respondent institution and to which the customers of this latter have direct access to execute their transactions) and foreign exchange services.
- business relationships which are similar in nature to those referred to in a) between the obliged entities referred to in Article 5, § 1, 1°, 3° and 4° (“correspondent institution”) and financial institutions within the meaning of Article 3 (2) of Directive 2015/849 (“respondent institution”) and which may include, in particular, carrying out securities transactions or funds transfers.

The case referred to here is that in which the correspondent institution is Belgian and the respondent institution is established outside the EEA.

Where cross-border correspondent relationships are entered into with such a respondent institution, the obliged entity must take general due diligence measures vis-à-vis the customers specified in Chapter 1, and also:

- gather sufficient information about the respondent institution to understand fully the nature of its business and to determine from publicly available information the reputation of the institution and the quality of supervision to which it is subject;
- assess the respondent institution’s AML/CFT controls;
- obtain approval from senior management before establishing new correspondent relationships;
- document the respective responsibilities of each institution;
- with respect to payable-through accounts, be satisfied that the respondent institution has verified the identity of, and performed ongoing due diligence on, the customers having direct access to accounts of the correspondent institution, and that it is able to provide relevant customer due diligence to the correspondent institution, upon request.

This provision transposes Article 19 of the Directive. The enhanced due diligence measures described therein are drawn from Article 12, § 4, of the Law of 11 January 1993, with the nuance that the draft Law determines that the member who must authorise the correspondent relationship must belong to a high level of hierarchy, while the Law of 11 January 1993 determines that the level of hierarchy must be “appropriate”; in practice, this “appropriate level of hierarchy” was also in principle always a “high level”. By way of reminder, in Article 4, 31°, “senior management” is defined as: “an officer or employee with sufficient knowledge of the institution’s money laundering and terrorist financing risk exposure and sufficient seniority to take decisions affecting its risk exposure, without necessarily being a member of the legal management body”;

To facilitate readability, Article 40 collates in one single Article all provisions relating to correspondent relationships. As a result, Article 40, § 2 also transposes Article 24 of the Directive and prohibits obliged entities from entering into or maintaining a correspondent relationship with a shell bank or with a credit institution or financial institution within

the meaning of Article 3, 1) and 2) of Directive 2015/849, known to allow a shell bank to use its accounts. By way of reminder, Article 4, 37° of the draft Law defines a “shell bank” as “a credit institution or an institution that carries out activities equivalent to those as referred to in Annex I of Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC, incorporated under the law of a Member State in which it has no physical presence, involving meaningful mind and management, and which is unaffiliated with a regulated financial group”. Article 40, § 2 of the draft Law, which takes over Article 12, § 4, second paragraph of the Law of 11 January 1993, does not provide for a special obligation to report suspicious transactions if a shell bank asks to enter into a business relationship with an obliged entity (which therefore has the obligation to refuse), because Article 47 already lays down a generally binding obligation to report suspicious transactions.



# Correspondent relationships: Comments and recommendations by the NBB

Home > Financial oversight > Combating money laundering and the financing of terrori...

## Contents

- 1. Concept of correspondent relationship
- 2. Correspondent relationship with a customer established in Belgium or in another EEA Member State
- 3. Correspondent relationship with a customer governed by the law of a third country
- 4. Correspondent relationship with a shell bank
- 5. Internal control measures

## 1. Concept of correspondent relationship

This page concerns correspondent relationships and relationships posing similar risks established by financial institutions.

For the definition of the concept of “correspondent relationship”, please refer to Article 4, 34°, of the Anti-Money Laundering Law (see the page “Definitions”).

## 2. Correspondent relationship with a customer established in Belgium or in another EEA Member State

In the past, Article 11, § 1, 1°, of the Law of 11 January 1993 authorised the implementation of simplified due diligence measures in case of correspondent relationships with customers or correspondent relationships where the beneficial owner was a credit or financial institution as referred to in Article 2 of Directive 2005/60/EC that was established in Belgium or in another EEA country, or an equivalent institution established in a third country imposing obligations and checks equivalent to those set out in Directive 2005/60/EC.

Pursuant to the risk-based approach and in accordance with Article 19, § 2, of the Anti-Money Laundering Law, any financial institution establishing a correspondent relationship or a relationship posing similar risks **with a respondent institution based in Belgium or in another EEA Member State** should henceforth assess the ML/FT risk level posed by the relationship concerned in order to determine the appropriate intensity of the due diligence measures to be implemented to adequately manage and reduce these risks. For further information on this subject, see the page “Individual risk assessment” and, in particular as regards the risk factors to be taken into consideration in the context of such an assessment, the documents mentioned in the section “Other reference documents” of the previous page.

It follows from the above and from the variety in the types of correspondent relationships that when, for instance, a high ML/FT risk level is found to be associated with a cross-border relationship established with a customer governed by the law of another EEA Member State, the correspondent financial institution should **apply enhanced due diligence measures** commensurate with the risk level thus identified. Conversely, a business relationship with a customer could lead to the identification of a low risk level based on the existence of low risk criteria such as those listed in the documents included in the section “Other reference documents”.

The NBB recommends determining in the institution's internal procedures the intensity of the due diligence measures to be implemented as a result of the assessment of the risks associated with the correspondent relationship or the relationship posing similar risks, taking into account all characteristics of the said relationship and of the transactions performed. When the relationship is found to be associated with a high ML/FT risk, which requires the implementation of enhanced due diligence measures, the internal procedures can provide for the adoption of measures similar to those included in Article 40, § 1, of the Anti-Money Laundering Law (see point 3 below).

Finally, the NBB stresses that each financial institution establishing a correspondent relationship with a customer established in Belgium or on the territory of another EEA Member State must verify, **first and foremost and regardless of the risk level associated with the relationship concerned**, that its customer is not a fictitious institution or an institution which is known to agree to establishing relationships with or carrying out transactions for fictitious institutions. This obligation flows logically from the prohibition referred to in Article 40, § 2, of the Anti-Money Laundering Law on establishing or continuing a correspondent relationship with a shell bank (see point 4 below).

### 3. Correspondent relationship with a customer governed by the law of a third country

**Where a financial institution referred to in Article 5, § 1, 1°, 3° or 4°, of the Anti-Money Laundering Law** establishes a cross-border correspondent relationship **with a respondent institution governed by the law of a third country**, Article 40 of the Law requires it to **apply enhanced due diligence measures in all cases**. For more information on the enhanced due diligence measures to be implemented, see Article 40, § 1, of the Anti-Money Laundering Law and the comments in the Explanatory Memorandum of this Article.

Implementing the enhanced due diligence measures provided for in Article 40, § 1, of the Anti-Money Laundering Law does not, however, exempt the correspondent institution from assessing the ML/FT risks associated with the relationship concerned. The enhanced due diligence measures to be implemented pursuant to the aforementioned Article 40 should be proportionate with the reassessed risk level, in accordance with Article 19, § 2, of the Law. For more information on this subject, see the page "General commentary on cases of enhanced due diligence", the content of which is taken from the Explanatory Memorandum of the Anti-Money Laundering Law.

Likewise, pursuant to the risk-based approach and to Article 19, § 2, of the Anti-Money Laundering Law, **any financial institution other than those referred to in Article 4, 1°, 3° or 4°, of the same Law** that establishes a relationship posing similar risks as a correspondent relationship **with a respondent institution governed by the law of a third country** should assess the ML/FT risk level posed by the relationship concerned in order to determine the appropriate intensity of the due diligence measures to be implemented. For further information on this subject, see the page "Individual risk assessment" and, in particular as regards the risk factors to be taken into consideration in the context of such an assessment, the documents mentioned in the section "Other reference documents" of the previous page. It follows from the above that, when a high ML/FT level is found to be associated with a cross-border relationship established with a customer governed by the law of a third country, the correspondent financial institution should **apply enhanced due diligence measures** commensurate with the risk level thus identified.

The NBB recommends determining the intensity of the due diligence measures to be implemented in the institution's internal procedures, depending on whether there are other factors indicative of high risk associated with the transaction or correspondent relationship concerned, in accordance with the individual risk assessment required by the aforementioned Article 19 of the Law (see the page "Individual risk assessment"). For this purpose, all characteristics of the said relationship and of the transactions performed should be taken into account. Finally, the NBB stresses that each financial institution establishing a correspondent relationship with a customer established in a third country must verify **first and foremost** that its customer is not a fictitious institution or an institution which is known to agree to establishing relationships with or carrying out transactions for fictitious institutions. This obligation flows logically from the prohibition referred to in Article 40, § 2, of the Anti-Money Laundering Law on establishing or continuing a correspondent relationship with a shell bank (see point 4 below).

## 4. Correspondent relationship with a shell bank

Article 40, § 2, of the Anti-Money Laundering Law prohibits financial institutions from establishing or continuing a correspondent relationship with a shell bank or with a credit or financial institution within the meaning of Article 3(1) and (2) of Directive 2015/849 that is known to allow its accounts to be used by a shell bank.

For the definition of the concept of “shell bank”, please refer to Article 4, 37°, of the Anti-Money Laundering Law (see the page “Definitions”).

Article 40, § 2, of the Law does not contain any obligation to address a specific suspicion report to CTIF-CFI when a shell bank wishes to enter into a business relationship with a financial institution that is subject to the Anti-Money Laundering Law (and is therefore obliged to refuse), as this situation falls under the general obligation to report suspicions as laid down in Article 47 of the Law.

## 5. Internal control measures

Financial institutions are expected to periodically and permanently monitor the adequacy of the organisational measures implemented to comply with the due diligence measures with regard to respondent institutions with which a correspondent relationship or a relationship posing similar risks has been established. The NBB expects the internal audit function in particular to pay specific attention to the adequacy and effectiveness of the enhanced due diligence measures adopted when the correspondent relationship concerned has a high risk level, where appropriate because the respondent institution is governed by the law of a third country.

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



# Politically exposed persons (PEPs)

Home > Financial oversight > Combating money laundering and the financing of terrori...

## Legal and regulatory framework

- Anti-Money Laundering Law: Article 41

## Explanatory Memorandum of the Anti-Money Laundering Law

- Article 41

## Other reference documents

- ESAs Risk Factor Guidelines dated 4 January 2018
- BCBS Guidelines dated June 2017 on Sound management of risks related to money laundering and financing of terrorism (see Annex 4)
- FATF Guidance dated 27 June 2013 on Politically Exposed Persons

## Comments and recommendations by the NBB

- Comments and recommendations

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**

# Politically exposed persons (PEPs): Comments and recommendations by the NBB

Home > Financial oversight > Combating money laundering and the financing of terrori...

## Contents

- 1. Persons concerned
- 2. Implementation of the risk-based approach for PEPs
- 3. System for determining whether the customer is a PEP
- 4. Enhanced due diligence measures
- 5. Internal control measures

In accordance with Article 41 of the Anti-Money Laundering Law, financial institutions should take enhanced due diligence measure when they carry out occasional transactions on behalf of or establish business relationships with politically exposed persons (“PEPs”), family members of such persons or persons known to be close associates of such persons. Included below are comments and recommendations made by the NBB regarding the persons referred to in this legal provision (see point 1), the implementation of the risk-based approach for PEPs (see point 2), the system to be implemented for identifying PEPs (see point 3), the enhanced due diligence measures to be taken (see point 4) and the internal control measures to be applied (see point 5).

## 1. Persons concerned

The enhanced due diligence provided for in Article 41 of the Anti-Money Laundering Law applies to three categories of persons: (i) PEPs, (ii) family members of PEPs, and (iii) persons known to be close associates of PEPs. The Anti-Money Laundering Law specifies criteria determining under what conditions a person should be considered a PEP because of the prominent public functions he/she holds or has held him-/herself, because he/she is a close relative of a person who holds or has held such functions, or because of the fact that he/she is known to be a close associate of a person who holds or has held such functions.

### 1.1. PEPs

PEPs are persons residing in Belgium or abroad who are exposed to particular risks because of the prominent public (political, judicial or administrative) functions they hold or have held.

More specifically, the term PEP is defined in Article 4, 28°, of the Anti-Money Laundering Law as a natural person who is or who has been entrusted with prominent public functions (not middle-ranking or more junior officials) and, in particular (non-exhaustive list):

1. heads of State, heads of government, ministers and deputy or assistant ministers;
2. members of parliament or of similar legislative bodies;
3. members of the governing bodies of political parties;
4. members of supreme courts, of constitutional courts or of other high-level judicial bodies, including administrative judicial bodies, the decisions of which are not subject to further appeal, except in exceptional circumstances;
5. members of courts of auditors or of the boards of central banks;

6. ambassadors, consuls, *chargés d'affaires* and high-ranking officers in the armed forces;
7. members of the administrative, management or supervisory bodies of State-owned enterprises;
8. directors, deputy directors and members of the board or persons in an equivalent function of an international organisation. International organisations are defined in Article 4, 32°, of the Law as associations of means or interests established by means of an international agreement between States, with joint bodies if necessary, with legal personality and subject to a legal system which is different from the one of its members.

While the Law of 11 January 1993 limited the notion of PEPs to foreign residents, the new anti-Money Laundering Law includes PEPs **residing in Belgium**. As a result, there is no longer a distinction between PEPs residing in Belgium, in an EEA Member State or in a third country. It should also be noted that the notion of PEPs refers to **important** public functions and not to middle-ranking or more junior officials.

## 1.2. Persons holding comparable prominent public functions

In contrast to the Law of 11 January 1993, the list of public functions included in the new Anti-Money Laundering Law is open-ended. For example, financial institutions could be led to conclude that persons holding prominent public functions comparable to those listed in Article 4, 28°, of the Money-Laundering Law should be considered PEPs. To that end, financial institutions should assess the risk level associated with these persons as a result of the functions that are effectively held by them and which present a degree of risk exposure comparable to that of the functions listed in Article 4, 28°, of the Law. For instance, although public functions performed at the regional or local level are not included in the legal listing of "important public functions", it cannot be excluded that they generate comparable risks, particularly in view of the size of the regional or local entity within which these public functions are performed, of the prevalence of the corruption that is generally known to affect the jurisdiction concerned, of the inadequacy of the anti-corruption measures implemented in this jurisdiction, etc.

Financial institutions should therefore, on the one hand, specify in their AML/CFTP policy (customer acceptance section) how they interpret "comparable prominent public functions", taking particular account of the nature and scale of the risks, notably the risk of money laundering of proceeds of corruption, that could be linked to the business relationships with the persons holding such functions. It should be noted, for example, that prominent public functions performed at the local or regional level are not included in the legal definition of PEPs, which means the function of mayor is not considered a prominent public function. However, depending on the size of the city concerned and of the budgets managed, the function of mayor of this city could present risks of the same nature and the same scale as the function of head of government. It could therefore be advisable to qualify such a prominent public function performed at the local level as a "comparable prominent public function".

On the other hand, in the context of the individual risk assessment according to Article 19 of the Anti-Money Laundering Law (see the page "Individual risk assessment"), financial institutions should also assess the risks linked to the performance of these comparable functions on a case-by-case basis, to determine whether their risk level requires the enhanced due diligence measures listed in Article 41 of the Law to be implemented.

## 1.3. Family members of PEPs

"Family members" are defined in Article 4, 29°, of the Anti-Money Laundering Law as:

- the spouse or a person considered to be equivalent to a spouse;
- the children and their spouses, or persons considered to be equivalent to a spouse;
- the parents.

## 1.4. Persons known to be close associates of PEPs

"Persons known to be close associates" are defined in Article 4, 30°, of the Anti-Money Laundering Law as:

- natural persons who have joint beneficial ownership of a legal entity or legal arrangement with a PEP or who are known to have any other close business relations with such a person;
- natural persons who have sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the de facto benefit of a PEP.

## 1.5. Cessation of a public function

Article 41, § 3, of the Anti-Money Laundering Law specifies that where a PEP is **no longer entrusted with a prominent public function** by an EEA Member State, a third country or an international organisation, financial institutions shall, for at least twelve months, take into account the continuing risk posed by that person and apply appropriate and risk-sensitive measures until such time as that person poses no further risk specific to PEPs. Whether this person poses no further risk should be determined through a new individual risk assessment performed by the financial institution in accordance with Article 19 of the Law. Thus, after the aforementioned twelve months have passed, there are several possible situations. For example, financial institutions may decide to stop applying enhanced PEP due diligence measures following this new assessment. Conversely, they may decide to continue to apply these enhanced due diligence measures in certain cases, even though the person has not held a public function for more than a year, if the ML/FT risk still seems high. In these cases, they can decide to perform a new individual risk assessment at a later moment, for example after another year or after six months.

## 2. Implementation of the risk-based approach for PEPs

The specific measures prescribed by Article 41 of the Anti-Money Laundering Law should be applied in conjunction with the general principle of the risk-based approach imposed by Articles 7, 16 and 19 of the Law.

A customer, his agent or one of his beneficial owners being identified as a PEP, as a family member of a PEP or as a person known to be a close associate of a PEP, as described in Article 41, does not exempt the financial institution from performing the individual risk assessment required by Article 19 of the Anti-Money Laundering Law or from taking this assessment into account to determine the appropriate due diligence measures to be implemented. It follows, in particular, that this individual risk assessment should also be taken into consideration to determine the intensity of the measures taken in accordance with Article 41 and, where appropriate, to supplement them when necessary to account for other identified risk factors.

## 3. System for determining whether the customer is a PEP

Article 41 of the Anti-Money Laundering Law stipulates that financial institutions should have “appropriate risk management systems, including appropriate risk-based procedures, to determine whether the customer, an agent of the customer or the beneficial owner of the customer is or has become a politically exposed person”. To be able to fully implement the obligations laid down in § 2 of the same Article 41 of the Law as well, these systems should also enable life insurance companies to identify cases where a beneficiary of a life insurance policy and/or, where appropriate, a beneficial owner of the beneficiary of such a policy is a PEP.

As regards enhanced PEP due diligence, the primary obligation for financial institutions is to adopt a procedure and a system that enable them to detect transactions or business relationships in the context of which one or multiple persons meeting the criteria to be qualified as PEP are involved in one of the capacities listed above. This system must make it possible to detect such transactions or business relationships while occasional transactions are being carried out or at the start of a business relationship, but it should also allow to detect business relationships during which one or multiple persons involved in one of the capacities listed above obtained the status of PEP.

### 3.1. Detection at the start of the relationship

The NBB expects financial institutions:

- a. to lay down, in their AML/CFTP policy (customer acceptance section), the main principles of the methodology to be applied to determine whether a customer, his agent, the beneficiary of a life insurance policy or a beneficial owner is a PEP (see the page “Policies, procedures, processes and internal control measures”);
- b. to determine whether their customers meet the definition of PEP by **comparing** their data **with reliable sources of information**, by using their **forms** for requesting the execution of a transaction or the establishment of a relationship or, in the case of life insurance, by using the precontractual documents to be completed by customers, or by any other means. In this regard, they may provide that customers should be asked contractually at the start of a business relationship to identify themselves as a PEP or ask questions to

ensure that the person in question is not a PEP (direct questions to obtain a spontaneous identification as PEP and/or indirect questions when there is no such spontaneous identification). However, these questions must proportionate to the purposes of the Anti-Money Laundering Law and the information received may only be used for the sole purpose of implementing the Law, to avoid having this information gathering constitute an excessive intrusion into customers' private lives; and

- c. to define, in their **procedure** relating to customer and transaction due diligence measures (section "identification and verification of the identity of customers, agents and beneficial owners), the special rules to be followed, depending on the level of ML/FT risks associated with the products or services for which they were called on by the customer, with the distribution channel used and with the geographical areas concerned, to check the information provided by the customer against certain reliable sources of information and ensure that the customer does not belong to the category of PEPs. In this respect, financial institutions are expected to take all information available to them into account in their analysis and to state in their procedures that customers should be asked specific additional questions when the **sources of information** consulted seem to indicate, contrary to the information provided by the customers, that they themselves or another person involved in the transaction or business relationship has the status of PEP.

### 3.2. Detection during the business relationship

The NBB draws the attention of the financial institutions to the fact that the enhanced due diligence obligations listed in Article 41 of the Anti-Money Laundering Law also apply when a customer, his agent, the beneficiary of a life insurance policy or a beneficial owner obtains the status of PEP during the business relationship. Moreover, these obligations also apply to existing business relationships (which were established before the entry into force of the new Anti-Money Laundering Law), in this respect also considering the expansion of the notion of PEPs, particularly to include persons residing in Belgium.

For example, in the framework of **updating the information** they hold about their customers, their agents, the beneficiaries of life insurance policies and the beneficial owners (see the page "Ongoing due diligence"), financial institutions are expected to implement risk-proportionate measures that enable them to identify which of their customers have become PEPs, either because they hold new public functions or because the legal definition of PEPs has been modified, and which of them have become family members of PEPs or persons known to be close associates of them.

When a PEP is identified as such during the business relationship, the financial institution's internal procedures should stipulate that the decision to maintain the business relationship should be made by the management committee or by the person authorised to do so (see below). If this decision is positive, the other enhanced due diligence measures described hereinafter apply (see Article 35, § 1, paragraph 3, of the Anti-Money Laundering Law).

## 4. Enhanced due diligence measures

In addition to the system for identifying PEPs, Article 41 of the Anti-Money Laundering Law provides for three specific enhanced due diligence measures. These measures apply as soon the financial institution establishes business relationships with or carries out occasional transactions on behalf of PEPs, family members of PEPs or persons known to be close associates of PEPs in whatever capacity (customer, agent, beneficial owner, etc.).

Financial institutions should specifically:

1. obtain **senior management** approval for establishing or continuing business relationships with PEPs or carrying out an occasional transaction on behalf of a PEP;
2. take adequate measures **to establish the source of the wealth and of the funds** that are involved in the business relationship or transaction with such persons;
3. subject the **business relationship to enhanced scrutiny**.

Article 41, § 2, of the Anti-Money Laundering Law addresses the particular case in which the beneficiaries of a **life insurance** policy and/or, where appropriate, the beneficial owner of the beneficiary of such a policy are or have become PEPs, family members of PEPs or persons known to be close associates of PEPs. In this case, obliged entities should, in addition to implementing ordinary customer due diligence measures:

1. inform senior management before pay-out of insurance benefits;
2. subject the entire business relationship with the policyholder to ongoing enhanced scrutiny.

#### 4.1. Senior management approval for establishing or continuing a business relationship with PEPs or carrying out an occasional transaction on behalf of a PEP

In accordance with Article 41 of the Anti-Money Laundering Law, when a PEP has been identified, financial institutions should provide for measures that make it possible to obtain senior management approval to establish or continue this business relationship with or to perform an occasional transaction on behalf of this PEP.

In practice, the NBB expects financial institutions:

- a. to lay down, in their AML/CFTP **policy** (customer acceptance section) the main principles to be followed with regard to the hierarchical level required for approval for establishing or continuing a business relationship with PEPs or carrying out occasional transactions on behalf of PEPs; and
- b. to define, in their **procedure** for customer and transaction due diligence measures (section on identification and verification of the identity of customers, agents and beneficial owners), the criteria to determine the specific hierarchical level which is competent to decide to establish or continue a business relationship with PEPs or to accept to carry out an occasional transaction on behalf of a PEP. These criteria may be based on a combination of risk factors associated with the profile of the PEP concerned and the risk factors inherent to the nature of the business relationship or the transaction to be concluded.

The NBB considers that the terms of the decision-making process for accepting or continuing a business relationship with a PEP should be determined **on the basis of the individual risk assessment** performed in accordance with Article 19 of the Anti-Money Laundering Law. These terms should in particular provide for the designation of the person or the body empowered with decision-making authority and organise the participation of the AMLCO in the decision-making process.

When the individual risk assessment leads to the identification of particularly high risks, in particular due to the fact that the status of PEP is combined with other factors indicative of high risk (for example because of links between the PEP concerned and countries with high ML/FT risks or a high risk of corruption), the nature of the ML/FT risks incurred by the financial institutions fully justifies having the **management committee** or, where appropriate, the senior management of the financial institution validate the establishment of a business relationship with or the performance of an occasional transaction on behalf of the PEP concerned. When the risks identified are less high, the internal procedures can allocate decision-making authority to persons or bodies of a lower hierarchical level. However, the financial institution must be able to justify this hierarchical level based on the ML/FT risk level assessed. In any case, this hierarchical level must be higher than that of the persons with decision-making authority regarding customers without PEP status.

For risk management purposes, the **NBB also recommends** that financial institutions provide, in their internal procedures, that **the AMLCO and/or of the person responsible for the compliance function must be involved** in the process for accepting or continuing a business relationship with a PEP or for accepting an occasional transaction on behalf of a PEP. This involvement may also be determined on the basis of the individual risk assessment performed pursuant to Article 19 of the Anti-Money Laundering Law. The NBB will take particular care to ensure that financial institutions at least provide that the AMLCO should participate actively and play a determining role in the decision-making process when the risks identified are particularly high, notably because of the presence of other factors indicative of high risk.

Moreover, where the financial institution belongs to a financial **group**, an exchange of information is required when necessary to implement the group policy. Taking the sensitivity of information on personal data into account, the flow of information on these customers within the group should take place at an appropriate hierarchical level and include the AMLCOs and the persons responsible for the compliance functions of the relevant entities of the group. The NBB considers that, among the information to be shared within a group, it is useful to include information on the customers identified as PEPs, in order to enable the financial institutions' management bodies to have suitable insight into all business relationships of these PEP customers.

#### 4.2. Determining the source of the wealth and the funds involved

In accordance with Article 41 of the Anti-Money Laundering Law, financial institutions having business relationships with PEPs should take appropriate measures to establish the source of these customers' wealth and of the funds involved in the business relationship with or transaction on behalf of such persons.

To be able to determine the source of the wealth and funds involved in the business relationship with PEPs, financial institutions must **either** obtain information directly from the customer, especially evidence that can be used to determine the source of the wealth and the funds, **or** have access to information that is publicly available, in particular on the internet, and that can be considered reliable.

The NBB recommends determining the intensity of the due diligence measures to be implemented depending on whether there are other factors indicative of high risk associated with the transaction or business relationship, in accordance with the individual risk assessment required by Article 19 of the Anti-Money Laundering Law (see the page "Individual risk assessment"). To that end, all characteristics of the transaction or business relationship should be taken into consideration, particularly its nature and purpose and the amounts involved. In this respect, the risk factors associated with the geographical areas concerned are of particular importance. For example, financial institutions must pay particular attention to well-known cases of corruption or organised crime in the country where the public function is performed, and to countries publicly known to have widespread corruption based on information published by credible governmental or non-governmental organisations or by major national or international media outlets.

In this regard, the NBB expects financial institutions to specify, in their customer and transaction due diligence procedures (section 'identification and verification of the identity of customers, agents and beneficial owners' and section 'ongoing due diligence'), which measures are required to determine the source of the wealth and funds involved in the business relationship, properly taking into account all risk factors determining the customer's profile as well as the business relationship or transaction to be concluded.

### 4.3. Enhanced scrutiny of the business relationship

In accordance with Article 41 of the Anti-Money Laundering Law, financial institutions having business relationships with PEPs should subject these relationships to enhanced scrutiny. For the specific measures required to scrutinise the customer's transactions, please refer to the page "General commentary on cases of enhanced due diligence".

As with the measures needed to determine the source of the customer's wealth and of the funds involved in the transaction or business relationship (see above), the intensity of the enhanced due diligence measures with regard to the customer's transactions should be established on the basis of the individual risk assessment, taking into consideration all risk factors determining the customer's risk profile.

## 5. Internal control measures

Financial institutions are expected to periodically and permanently monitor the adequacy of the organisational measures implemented to comply with the identity and enhanced due diligence obligations with regard to PEPs. In this respect, the NBB expects the internal audit function in particular to pay specific attention to the adequacy of the measures for identifying PEPs and to the effectiveness of the enhanced due diligence measures implemented by the financial institutions.

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



# Anti-Money Laundering Law of 18 September 2017 - Article 41

## Art. 41

§ 1. Obligated entities that carry out transactions or establish business relationships with politically exposed persons, family members of politically exposed persons or persons who are known to be closely associated with politically exposed persons shall, in addition to the customer due diligence measures laid down in Chapter 1, take the following measures:

1° without prejudice to Article 8, have in place appropriate risk management systems, including appropriate risk-based procedures, to determine whether the customer, an agent of the customer or the beneficial owner of the customer is or has become a politically exposed person;

2° apply the following measures in cases of business relationships with politically exposed persons:

- a) obtain senior management approval for establishing or continuing business relationships with such persons;
- b) take adequate measures to establish the source of the wealth and of the funds that are involved in business relationships or transactions with such persons;
- c) subject the business relationship to enhanced scrutiny.

§ 2. Without prejudice to paragraph 1, if the beneficiaries of a life insurance policy and/or, where appropriate, the beneficial owner of the beneficiary of such a policy are or have become politically exposed persons, family members of politically prominent persons or persons who are known to be closely associated with politically exposed persons, obliged entities shall, in addition to the customer due diligence measures laid down in Chapter 1, take the following measures:

1° inform senior management before pay-out of insurance benefits;

2° subject the entire business relationship with the policyholder to ongoing enhanced scrutiny.

§ 3. Where a politically exposed person is no longer entrusted with a prominent public function by a Member State, a third country or an international organisation, obliged entities shall, for at least twelve months, take into account the continuing risk posed by that person and apply appropriate and risk-sensitive measures until such time as that person poses no further risk specific to politically exposed persons.



# Explanatory Memorandum to the Anti-Money-Laundering Law of 18 September 2017 - Article 41

## Art. 41

Paragraph 1 of this draft Article refers to cases in which obliged entities execute transactions or enter into business relationships with politically exposed persons (PEPs), family members of these persons or persons known to be close associates.

Enhanced due diligence measures are required in all cases where a PEP is involved, in any way whatsoever, in a business relationship. While § 1 refers to cases in which the customer, authorised agent or beneficial owner of the customer is a PEP, § 2 refers to cases in which the beneficiary of a life insurance policy or a beneficial owner of the latter can be qualified as a PEP.

In all these cases, the obliged entity must conduct the general due diligence measures provided for in Chapter 1, but is also required to:

- have appropriate risk-management systems, including risk-based procedures, to determine whether the customer or the customer's beneficial owner is or has become a PEP; this obligation applies without prejudice to Article 8;
- obtain consent from senior management to embark on or maintain business relationships with PEPs;
- take appropriate measures to establish the source of the wealth and funds involved in the business relationships or transactions with such persons;
- exercise enhanced supervision on the business relationship.

These enhanced due diligence measures are taken over from Article 12, § 3, sixth paragraph of the Law of 11 December 1993.

It should be noted that the enhanced due diligence measures are required in accordance with Directive 2015/849 as soon as an obliged entity executes transactions or enters into business relationships in which PEPs are involved, irrespective of whether they reside in Belgium or abroad. This is new compared to the Law of 11 January 1993, which only referred to PEPs residing abroad. There is therefore no distinction made between PEPs residing in Belgium, in a Member State or in a third country, which is in line with the Recommendations of the FATF.

We also note that the obliged entities must take measures, when updating the information they keep on their customers, that enable them to identify, among their customers, those who over the course of the business relationship have become PEPs, family members of PEPs or persons known to be close associates of PEPs; in such a case, the management must decide whether the business relationship should or should not be pursued, and whether the other enhanced due diligence measures apply (see draft Article 35, § 1, third paragraph).

It should equally be noted that the meaning of the term 'PEP' is defined in Article 4, 28° of the draft Law. According to this definition, a PEP is a natural person who is or who has been entrusted with prominent public functions. These include the following persons:

- heads of State, heads of government, ministers and assistant ministers; (the term "minister" also includes "deputy ministers" as referred to in the Directive);
- members of parliament or of similar legislative bodies;
- members of the governing bodies of political parties (this category is not included in the Law of 11 January 1993);

- members of supreme courts, of constitutional courts or of other high-level judicial bodies, including administrative judicial bodies, the decisions of which are not subject to further appeal, except in exceptional circumstances;
- members of courts of auditors or of the boards of central banks;
- ambassadors, consuls, *chargés d'affaires* and high-ranking officers in the armed forces;
- members of the administrative, management or supervisory bodies of State-owned enterprises;
- directors, deputy directors and members of the board or persons in an equivalent function of an international organisation (this category is not expressly included in the Law of 11 January 1993; however, this does not constitute a new category given that the Law of 11 January 1993 specifies that the roles exercised on a European and international level also come under the various categories of PEPs). International organisations are defined in Article 4, 32° of the draft text as an association of means or interests established by means of an international agreement between States, with joint bodies if necessary, with legal personality and subject to a legal system which is different from that of its members.

Middle-ranking or more junior roles do not come under the public functions referred to in points a) to h).

Whilst Article 12, § 2 of the Law of 11 January 1993 provides a full list of PEPs, the list in the present draft Law is an open list, in accordance with Article 3, 9) of the Directive.

The definition of family members provided in draft Article 4, 29°, remains unchanged from the definition in the Law of 11 January 1993. The following come under this definition:

- the spouse or a person considered to be equivalent to a spouse;
- the children and their spouses, or persons considered to be equivalent to a spouse;
- the parents.

The same applies to the definition of “persons known to be close associates” (see Article 4, 30°), which still covers the following persons:

- natural persons who are known to have joint beneficial ownership of a legal entity or legal arrangement, or are known to have any other close business relationships with a PEP;
- natural persons who have sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the *de facto* benefit of a PEP.

Draft Article 41, § 2, refers to the special case in which the beneficiaries of a life insurance policy and/or, where applicable, the beneficial owner of the beneficiary of such a policy are or have become PEPs, family members of PEPs or persons known to be close associates of PEPs. In such a case, obliged entities must, in addition to the due diligence measures stipulated in Chapter 1, also:

- 1° inform senior management before pay-out of insurance benefits;
- 2° subject the entire business relationship with the policy-holder to ongoing enhanced scrutiny.

This § 2 partially transposes Article 21 of the Directive. The words “family members of PEPs or persons known to be close associates of PEP” are added in the draft text to transpose Article 23 of the Directive too, and the wording of point 2° has been amended to take into account the comments of the Council of State.

Draft Article 41, § 3 specifies that, when a PEP is no longer entrusted with a prominent public function by a Member State or a third country or by an international organisation, obliged entities must, for at least twelve months, take into account the continuing risk posed by that person and apply appropriate and risk-sensitive measures until such time as that person poses no further risk specific to a PEP. The fact that the person poses no further risk must be established based on a specific risk assessment by the obliged entity.



# Due diligence requirements and compliance with other legislation

Home > Financial oversight > Combating money laundering and the financing of terrori...

## Contents

- 1. Combating discrimination
- 2. Protection of personal data
- 3. Basic banking services
- 4. Access by payment institutions to credit institutions' payment account services

---

The NBB insists that in implementing their organisational and operational AML/CFT obligations, financial institutions should take into account the impact of, inter alia, the legislation mentioned below.

## 1. Combating discrimination

Financial institutions should take into account the impacts of the anti-discrimination legislation: see <https://www.unia.be/en/law-recommendations/legislation>.

The NBB emphasises in particular that the customer acceptance policy should be defined in accordance with the provisions of the anti-discrimination legislation.

## 2. Protection of personal data

Financial institutions should take into account the impacts of the privacy legislation: see <https://www.dataprotectionauthority.be/legislation-and-standards>.

Financial institutions should ensure that their customer acceptance policies and internal procedures are compatible with the applicable provisions of Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (Regulation usually referred to as the General Data Protection Regulation or GDPR), taking into account the specific relevant provisions of Articles 64 and 65 of the Anti-Money Laundering Law.

As regards the application of the general rules on data protection, see the recommendations made in this respect by the Data Protection Authority. For the application of these rules in the specific context of AML/CFT, see the opinion of the Privacy Protection Committee of 24 May 2017 on the draft Anti-Money Laundering Law, which forms part of the preparatory work for that Law (see: <https://www.autoriteprotectiondonnees.be>).

The implementation of the Anti-Money Laundering Law requires the processing of personal data. This includes processing operations which are required to enable financial institutions to comply with their legal AML/CFT obligations, and processing operations performed pursuant to the European Regulation on transfers of funds and to national and international financial sanctions measures.

These processing operations are aimed in particular at implementing monitoring procedures adapted to the ML/FT risks throughout the business relationship and to assist in monitoring, detecting and examining transactions carried out by customers involving sums likely to be derived from a criminal activity falling under the concept of money laundering, to participate in the financing of terrorism or to detect funds and economic resources subject to a freezing or sanction measure.

The data processed relate in particular to the identification and verification of the identity of the customer and, where applicable, his agents and beneficial owners, the operation of the account, financial transactions or products subscribed to. They also include the information referred to in Article 34, § 1 of the Anti-Money Laundering Law which is necessary for implementing the customer acceptance policy, for fulfilling the ongoing due diligence obligations with regard to business relationships and transactions, and for complying with the specific enhanced due diligence obligations.

The specific conditions to be satisfied when processing these data are set out in Article 64 of the Anti-Money Laundering Law. In particular, it should be noted that these data may only be processed for the specific purposes for which they are collected and may under no circumstances be used for commercial purposes.

The rights of the persons whose personal data are held and processed for AML/CFT purposes are specified in Article 65 of the Anti-Money Laundering Law, which derogates from the general rules on the basis that the participation of financial institutions in AML/CFT is a public interest task.

### 3. Basic banking services

Financial institutions should take into account the impacts of the legislation on basic banking services. Their customer acceptance policies and internal procedures should ensure compliance with this legislation. Reference is made in this respect to Book VII, Title 3, Chapter 8, of the Code of Economic Law.

### 4. Access by payment institutions to credit institutions' payment account services

Credit institutions should ensure that their customer acceptance policies and internal procedures are compatible with Article VII 55/12 of the Code of Economic Law, which grants payment institutions objective, non-discriminatory and proportionate access to credit institutions' payment account services.

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



# Analysis of atypical transactions and reporting of suspicions

[Home](#) > [Financial oversight](#) > [Combating money laundering and the financing of terrori...](#)

**Analysis of atypical facts and transactions**

**Reporting of suspicions**

**Prohibition of disclosure**

**Protection of reporting entities**

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



# Analysis of atypical facts and transactions

Home > Financial oversight > Combating money laundering and the financing of terrori...

## Legal and regulatory framework

- Anti-Money Laundering Law: Articles 45 and 46
- Anti-Money Laundering Regulation of the NBB: Articles 16 to 18

## Explanatory Memorandum of the Anti-Money Laundering Law

- Articles 45 and 46

## Other reference documents

- CTIF-CFI's information note of 26 October 2017 regarding the disclosure of information to CTIF-CFI

## Comments and recommendations by the NBB

- Comments and recommendations

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**

# Analysis of atypical facts and transactions: Comments and recommendations by the NBB

Home > Financial oversight > Combating money laundering and the financing of terrori...

## Contents

- 1. Preliminary analysis of the reportings generated by the system for detecting atypical facts and transactions
- 2. Analysis of atypical facts and transactions by the AMLCO
- 3. Resources and internal control measures

If the mechanisms used for exercising due diligence with respect to transactions and business relationships report an atypical fact or transaction, the financial institution is expected to first pre-analyse the said reporting to ensure that it is justified (see point 1 below). Financial institutions must also have a system for analysing the facts or transactions whose atypical nature has thus been confirmed, in order to establish, where appropriate on the basis of a wider range of information, whether the financial institution must consider that it knows, suspects or has reasonable grounds to suspect that the funds, transaction or fact are related to money laundering or terrorist financing (see point 2 below). The system for analysing atypical facts and transactions must also be subjected to internal control measures (see point 3 below).

## 1. Preliminary analysis of the reportings generated by the system for detecting atypical facts and transactions

As specified on the page “Ongoing due diligence and detection of atypical transactions”, the system for detecting atypical facts and transactions is based on 2 elements: (i) detection by the persons who are in direct contact with customers or instructed with carrying out their transactions and (ii) an additional automated monitoring system.

Where this appears indicated in light of the characteristics of the reporting, taking into account in particular the complexity of the transaction or fact concerned, the number of participants, the amounts involved, etc., or because of serious doubts as to the validity of the information on which the reporting is based, the Bank recommends to conduct a preliminary analysis in order to verify that the information directly available to the financial institution does not contradict the atypical nature of the fact or transaction reported. This preliminary analysis allows to make a first assessment of the circumstances surrounding the transaction that has led to the reporting, in order to ensure the relevance of this reporting.

As a rule, the NBB recommends that this preliminary analysis be carried out by **the AMLCO or a member of his team**. However, inter alia for reasons of proportionality, the NBB allows this task to be carried out by an “**AML correspondent**” of another service provided that he is subject to dual reporting lines: on the one hand to the AMLCO or the person responsible for the Compliance function, for his tasks relating to the preliminary analysis of reportings, and on the other hand to another operational department, for his other tasks and functions. In all cases, the persons who carry out the preliminary analysis of the reportings must receive their instructions in this regard from the AMLCO under whose supervision they carry out these tasks. They must have adequate AML/CFTP experience and skills, have received adequate AML/CFTP training and have access to the information necessary to perform their tasks. In addition, financial institutions are expected to ensure that the person(s) carrying out this preliminary analysis has(have) sufficient human and technical resources to validate the reportings. If insufficient resources are allocated to this task, it may be impossible to analyse the reportings generated in a timely manner, which, in turn,

may cause harmful delays in submitting validated reportings to the AMLCO for analysis, or, conversely, lead to an excessive number of files being submitted to the AMLCO, including files based on incorrect information, which may reduce the effectiveness of the capacity of the latter to conduct an in-depth analysis.

The preliminary analysis, which consists in examining the information directly available concerning the context of the facts or transactions that have led to the reporting, may lead to **either** a duly justified closing of the case without further action in case of a 'false alert', **or** to submission of the file to the AMLCO for further analysis. The result of this preliminary analysis must **be documented on the basis of a simple and if possible structured justification** (such as "*false alert because...*" or "*Reporting requiring further analysis because...*") in order to facilitate an ex post control.

If the file is submitted to the AMLCO, the person or persons instructed with conducting this preliminary analysis must immediately cooperate fully and help him collect, if necessary, as much available information as possible concerning the customer, the fact or transaction concerned or the context.

## 2. Analysis of atypical facts and transactions by the AMLCO

### 2.1. Purpose of the analysis - Determination of the suspicion of money laundering or terrorist financing

If the relevance of the reporting is validated as indicated above, the financial institution must ensure that the atypical fact or transaction concerned is analysed in sufficient depth, also taking into account its context, to determine whether the financial institution should consider that it "*knows, suspects or has reasonable grounds to suspect*" that the funds, transaction or fact concerned are related to money laundering or terrorist financing.

The determination of suspicion must be the result of an intellectual process and the conclusion of a documented analysis. It cannot be carried out by automated systems alone but requires human intervention based on the analysis of atypical facts and transactions and their circumstances, to decide whether these atypical facts or transactions are suspected of being related to ML/FT and must therefore be reported to CTIF-CFI or, conversely, that their analysis allows to rule out such suspicions and close the case without further action.

This analysis must be conducted taking full account of the legal definition of money laundering and terrorist financing.

#### 2.1.1 Suspicions of money laundering

##### A. General principles

Article 2 of the Anti-Money Laundering Law defines money laundering by listing acts (conversion, transfer, concealment, etc.) relating to funds stemming from criminal activities and aimed essentially at evading or enabling to evade the legal consequences of unlawful acts.

The predicate money laundering offences are numerous. They are listed exhaustively in Article 4, 23° of the Anti-Money Laundering Law, which defines them as "any kind of involvement in the commission of an offence related to:

- a. terrorism or terrorist financing;
- b. organised crime;
- c. illicit drug trafficking;
- d. illicit trafficking in goods, merchandise and weapons, including anti-personnel mines and/or submunitions;
- e. smuggling in human beings;
- f. trafficking in human beings;
- g. exploitation of prostitution;
- h. illicit use in animals of hormonal substances or illegal trade in such substances;
- i. illicit trafficking in human organs or tissues;
- j. fraud detrimental to the financial interests of the European Union;
- k. serious fiscal fraud, whether organised or not;
- l. social fraud;
- m. embezzlement by public officials and corruption;

- n. serious environmental crime;
- o. counterfeiting currency or bank notes;
- p. counterfeiting products;
- q. piracy;
- r. stock market-related offence;
- s. an improper public offering of securities;
- t. the provision of banking services, financial services, insurance services or funds transfer services, or currency trading, or any other regulated activity, without having the required licence for these activities or meeting the conditions to carry out these activities;
- u. fraud;
- v. breach of trust;
- w. misappropriation of corporate assets;
- x. hostage-taking;
- y. theft;
- z. extortion;
- aa. the state of bankruptcy;
- ab. computer fraud."

However, Article 47, § 1, second paragraph, of the Anti-Money Laundering Law specifies **that the financial institutions are not required to identify the offence underlying the suspected money laundering activity**. *A fortiori*, they are not required to verify that the constituent components of the criminal offences concerned are present, nor gather evidence of them. If their analysis of the atypical transactions and facts leads them to know, suspect or have grounds to suspect that these transactions or facts are related to any of the offences listed, the atypical fact or transaction concerned must be qualified as suspicious. In most cases, the reporting entities cannot know precisely which are the offences underlying the suspected money laundering activity. It is up to CTIF-CFI to conduct an in-depth analysis in order to find the link between the funds concerned, the suspicious transaction or the facts reported and one of the forms of offences referred to in the Law. In this respect, CTIF-CFI plays a sorting/filtering role and enriches the reportings sent to it, thus avoiding that the offices of the prosecutor are overloaded with irrelevant reportings. This does not prevent the reporting entities from referring to any predicate offence when they know, suspect or have reasonable grounds to suspect that the laundered funds stem from any of the criminal activities mentioned in Article 4, 23°, of the Anti-Money Laundering Law.

The terms "suspect" or "have reasonable grounds to suspect" indicate that the financial institution must qualify the funds involved, the transaction or the fact concerned as suspicious if the analysis of the information collected in accordance with the due diligence obligations for the purpose of conducting the analysis, leads to a suspicion ("suspect") or includes elements that do not reasonably allow it to dispel the doubt ("have reasonable grounds to suspect") as to the lawful origin of the amounts or of the transaction or as to their economic, legal or tax justification.

## **B. Individual cases of money laundering**

### *§1. Money laundering stemming from serious fiscal fraud, whether organised or not*

It should be recalled, pursuant to the principle set out in Article 47, § 1, second paragraph, of the Anti-Money Laundering Law, that a financial institution must qualify an atypical transaction as suspicious if the analysis of this transaction leads it to consider that it knows, suspects or has reasonable grounds to suspect that the funds concerned have an illicit origin that may consist in any of the forms of crime listed in the Law, including serious fiscal fraud, without having to determine which of these crimes has been committed (see above).

The Bank therefore considers that funds and transactions relating to funds of which the financial institution knows, suspects or has grounds to suspect that they could stem from fiscal fraud, must be qualified as suspicious since the financial institution cannot reasonably exclude, on the basis of the information in its possession, that a serious fiscal fraud has been committed. The suspicion that a serious fiscal fraud may have been committed or the existence of reasonable grounds to suspect so, are sufficient to qualify the transaction as suspicious. This may be the case in particular if the suspicion of fiscal fraud is combined, either with a large amount of funds involved, or with an amount that is abnormal in view of the customer's activities or financial situation, or with a suspicion of forging of documents or use of false documents.

However, this does not imply in any way that the financial institution must be certain or must have evidence that the suspected fiscal fraud actually meets the legal conditions to be qualified as "serious, whether organised or not". It is up to CTIF-CFI, to which this suspicious transaction must be reported, to determine, on the basis of a more detailed analysis, whether or not there is predicate serious fiscal fraud.

It is also pointed out that, in order to promote the detection of atypical transactions that may be related to money laundering stemming from serious fiscal fraud, Article 39 of the Anti-Money Laundering Law requires enhanced due diligence measures with regard to transactions, business relationships or persons involved that are in any way linked to a no-tax or low-tax State included in the list established by Royal Decree in accordance with Article 307, § 1, seventh paragraph, of the Income Tax Code 1992. In this respect, see the page "States with low or no taxes".

See also the page "Ongoing due diligence and detection of atypical transactions" for a list of indicators of atypical transactions that may lead to suspicions of serious fiscal fraud.

### *§2. Money laundering stemming from social fraud and computer fraud*

In the Anti-Money Laundering Law, social fraud and computer fraud have been added to the list of predicate offences.

The notion of social fraud includes, for example, undeclared work, misappropriation of benefits, non-compliance with the regulations relating to the occupation of foreign workers, etc.

Although the concept of "computer fraud" may already be covered by the notion of fraud, the Anti-Money Laundering Law uses this concept to refer to attempts to obtain, for its perpetrator or others, an illegal economic advantage by breaching a computer system, by modifying or deleting the data stored, processed or transmitted by a computer system, or by modifying by any technological means the normal use of data in a computer system.

The NBB urges financial institutions to consult CTIF-CFI's activity reports on these subjects.

### 2.1.2. Suspicions of terrorist financing

The NBB draws the attention of financial institutions in particular to the fact that the analysis of atypical transactions and facts must also enable the financial institution to determine whether it "**knows, suspects or has reasonable grounds to suspect**" that the funds, transaction or fact concerned are related to terrorist financing. Article 3 of the Anti-Money Laundering Law defines terrorist financing as the provision or collection of funds or other assets, by any means, directly or indirectly, with the intention that they be used or in the knowledge that they are to be used, in full or in part, by a terrorist organisation or by a terrorist acting alone, even without any link to a specific terrorist act.

Financial institutions must therefore verify the consistency of the origin and/or destination of funds relating to one or more transactions with the up-to-date knowledge of their customers. They should exercise enhanced due diligence with regard to transfers of funds (credit transfers and money remittances) from or to geographical areas considered to be at risk with regard to terrorism or terrorist financing or with regard to transactions carried out in these areas.

Financial institutions are reminded of the need for their AML/CFTP policies to integrate the risks associated with the countries/territories from which or to which the funds are transferred. They must be alert to transactions carried out by their customer in "sensitive" countries, but also to those carried out in countries which, to their knowledge, are not in any way linked to their customer, as some countries may be used as transit countries to hide the final country of destination or the origin of the funds. Particular attention must also be paid to patterns showing that one and the same person makes multiple transfers of funds over a short period of time to beneficiaries in high-risk geographical areas or, conversely, that one and the same person receives a large number of transfers of funds initiated by different persons.

The due diligence measures must however be taken in various domains in order to address the changing nature of terrorist financing. Indeed, recent events show that transactions are carried out in all countries, without there being any link with conflict areas or with the business relationship.

Changes in a customer's attitude or in the functioning of the business relationship also require specific attention.

### 2.1.3. Suspicions of financing of the proliferation of weapons of mass destruction

The analysis of atypical transactions and facts must also enable the financial institutions to comply with the provisions of European Law imposing restrictive measures against certain countries in order to fight against the proliferation of weapons of mass destruction and its financing, and in particular with the obligation to report to CTIF-CFI any transaction involving funds for which there are reasonable grounds to suspect that they could be linked to the financing of weapons of mass destruction-related activities or programmes.

The Bank considers that a specific analysis of atypical transactions and facts is required where the characteristics of the funds, in particular their origin and destination, the nature and characteristics of the transactions or of the persons involved in the transaction or business relationship, including the customer, his agents, his beneficial owners or the counterparties to the transactions, have links with the countries concerned or with persons or entities known to be involved in the proliferation of weapons of mass destruction.

It must be stressed that, in the same way as for the fight against ML or TF, there is no need for the financial institution to be certain or to have evidence that a transaction or funds can be related to the financing of the proliferation of weapons of mass destruction, to consider that this is the case: the fact that there are reasonable grounds to suspect this, is sufficient.

## 2.2. Responsibilities of the AMLCO

One of the AMLCO's main operational responsibilities is to conduct the above analysis of detected atypical facts and transactions in order to determine whether or not there is a suspicion of ML/FT or whether or not there are reasonable grounds for this suspicion, and whether the facts, funds or transactions concerned should therefore be reported to CTIF-CFI in accordance with Article 47 et seq. of the Anti-Money Laundering Law.

In order to be able to fulfil this responsibility, the AMLCO must have easy access to all information held by the financial institution that is relevant to its analysis.

Contrary to the preliminary analysis described in point 1 above, the analysis to be carried out by the AMLCO pursuant to Article 45 of the Anti-Money Laundering Law may not be limited to the mere validation of the information directly related to the atypical transaction or fact.

The AMLCO is expected to carry out an in-depth analysis of **all the information that has been collected as part of the process of detecting atypical facts or transactions and their preliminary analysis**, i.e. (i) reportings from either persons who are in direct contact with customers or who are instructed with carrying out their transactions, or the automated monitoring system and (ii) all the information collected and documented as part of the preliminary analysis.

This initial information is usually insufficient to decide whether or not the funds, the transaction or fact should be qualified as suspicious. The analysis of atypical transactions and facts by the AMLCO should generally be more thorough and rely on a wider range of information to support the decision. The NBB therefore expects the AMLCO to **appropriately expand the range of information on which he bases his analysis, depending on the circumstances and needs**.

To this end he must, for the purpose of his analysis, collect the information available within the financial institution concerning the customer, his risk profile, the business relationship with him - including an overview of the transactions he has carried out over a sufficient period of time, depending on the circumstances - and any relevant background information. However, it is important that the AMLCO be able to collect all the information held by the financial institution, regardless of the service or department of the financial institution that holds it, if it is relevant to properly assess whether or not the atypical transactions or facts considered are suspicious.

Depending on the circumstances, this analysis may also require the reconciliation of the transactions of the customer concerned with those of other customers with whom he appears to have a financial relationship.

In addition to the abovementioned searches for information in the institution's internal databases, the analysis of the facts or transactions concerned may require **measures complementary** to those already taken in the context of the ongoing due diligence (see Articles 19 to 41 of the Anti-Money Laundering Law). Such additional measures may include, in particular:

- asking additional information or supporting documents from the customer himself;
- initiating procedures to share information within the group for the purpose of combating ML/FT (see Organisation and internal control within groups), in order to obtain, in particular, information held by other

entities of the group on the transactions or business relationships of that customer with these other entities of the group, their knowledge of that customer, and even, where applicable, their possible suspicions regarding the customer or any reportings of suspicions concerning the customer that they would have addressed to the financial intelligence unit in their country of establishment;

- consulting public sources of information, in particular on the internet,
- etc.

Attention should be drawn to Article 45 of the Anti-Money Laundering Law, which provides that as part of this analysis, the AMLCO (or members of his team acting under his authority) must examine, as far as possible, the **background** and **purpose of the transactions**, particularly in the case of complex transactions and transactions of unusually large amounts or transactions which are part of unusual patterns of transactions that have no apparent economic or lawful purpose.

As to the **purpose of the transactions**, financial institutions must try to gain insight into, for example, a legal arrangement, the interdependence of companies or financial movements between different persons. The institution carries out the analysis on the basis of all the information which is at its disposal or to which it has access (search of the beneficial owner, purpose of the transactions concerned, operation of the accounts, etc.).

The scope of the searches and the depth of the analysis may be determined on the basis of the characteristics and importance of the cases examined, but must be sufficient to prevent transactions or facts either from being qualified as suspicious without taking into account important information that was available within the financial institution and that was clearly of such a nature as to remove the suspicion or, conversely, to prevent them from being closed without further action because no account has been taken of information that is nevertheless available, and which, together with the analysis, would constitute reasonable grounds to suspect a link with ML or FT.

As the decision to qualify a transaction or fact as suspicious must result from the analysis described above, financial institutions may not automatically qualify certain transactions or facts as suspicious solely on the basis of predefined objective indicators, without carrying out the required analysis.

Thus, transactions may not be automatically qualified as suspicious without an analysis having been conducted to justify the suspicion, where this suspicion is solely based on:

- a mere assumption concerning the activity of the customer, his address or his country of residence or registration;
- a transaction of a large amount which has been fixed a priori and, more generally, without establishing that it is unusually large taking into account the profile of the business relationship or, in the case of occasional customers, the transactions usually carried out by the institution;
- difficulties between the financial institution concerned and its customer or the latter's conduct, in particular in a personal interview;
- the opening of a judicial inquiry or a request for information from, for example, CTIF-CFI or an administrative or judicial authority;
- etc.

On the other hand, such indicators appear to be particularly useful in identifying atypical facts or transactions that should be submitted to the AMLCO for analysis.

For example, unusual behaviour by a customer generally does not in itself suffice to establish, without further analysis, a link between his transactions or acts and money laundering or terrorist financing. It may however be a relevant indication to qualify his transactions or acts (including attempted transactions) as atypical, and may thus give rise to an analysis by the AMLCO to determine whether there is a suspicion of ML/FT. In this respect, it is recalled that the internal procedures relating to the *Due diligence with regard to the business relationships and transactions* must include in particular appropriate criteria allowing persons who are in direct contact with customers or carrying out their transactions, to detect atypical transactions and facts (see Article 16, 1°, of the Anti-Money Laundering Regulation of the NBB). In this respect, see the page "Policies, procedures, processes and internal control measures: comments and recommendations".

Similarly, the fact that the financial institution is informed of the opening of a judicial inquiry into a customer, or the fact that it has received a request for information from, for example, CTIF-CFI or an administrative or judicial authority, does not suffice to automatically consider the transactions carried out by his customer as suspicious without the AMLCO having analysed these transactions to determine whether there are suspicions of ML/FT. Likewise, the observation that the assets of a customer, his agent or beneficial owner are frozen is not sufficient in

itself to consider all the transactions of the customer concerned as suspicious, but must lead the financial institution to re-examine the business relationship in greater detail to determine whether certain transactions may be suspected of being linked to terrorist financing.

However, if the AMLCO, after analysing the transactions carried out by a customer, suspects that they are related to ML/FT, the fact that the financial institution has been informed of the opening of a judicial inquiry or even of criminal proceedings against a customer does not exempt it from reporting the suspicious transactions.

For further information see the page "Reporting of suspicions" and the information on that page about reportings made in good faith.

### 2.3. Result and documentation of the analysis conducted by the AMLCO in a written report

The analysis of the atypical fact or transaction may lead to the case being closed without further action, or to the fact, the funds or the transaction being qualified as suspicious. In both cases, the decision rests with the AMLCO (without the intervention of the senior officer responsible for AML/CFTP).

Since the purpose of this analysis is to determine whether or not suspicious facts, funds or transactions should be reported to CTIF-CFI in accordance with Article 47 of the Anti-Money Laundering Law, financial institutions must ensure that their AMLCO is able to analyse the reportings addressed to them with the required due diligence to ensure that the reporting deadlines set out in Article 51 of the Law can be met (see the page "Reporting of suspicions"). The AMLCO must give priority to the analyses of atypical transactions presenting the most alarming characteristics, in particular in terms of the amounts involved and the nature and likelihood of a possible link with the ML/FT.

Whenever atypical facts or transactions are submitted to the AMLCO for analysis, the latter must document the results of the analysis in a **written internal report**. In particular, this internal analysis report should make it possible to understand the reasons why the AMLCO has concluded that either there is or there is not a suspicion of ML/FT, to justify his decisions a posteriori and to monitor the effectiveness and relevance of the decision-making process.

In accordance with Article 47, § 1, 1°, of the Anti-Money Laundering Law, neither the analysis of the AMLCO nor the written analysis report must however identify the offence underlying the suspicious transaction (see above).

## 3. Resources and internal control measures

The analysis of atypical facts and transactions as described above to determine whether or not there are suspicions of ML/FT, which must be carried out before suspicious transactions, funds or facts are reported to CTIF-CFI, is a key element of the mechanism to prevent ML/FT that financial institutions are legally required to have.

It is recalled that Article 18 of the Anti-Money Laundering Regulation of the NBB also provides that financial institutions should adopt appropriate procedures enabling them to analyse atypical transactions as soon as possible (see the page "Policies, procedures, processes and internal control measures").

The NBB also expects financial institutions to provide their AMLCO with the necessary human and technical resources to enable them to carry out this analysis effectively and to adequately follow it up within the deadlines set out by the Law.

Generally, financial institutions are expected to periodically and continuously monitor the effective exercise of AML/CFTP-related tasks by all persons responsible for such tasks within the institution. This also includes all the AMLCO's tasks and responsibilities, in particular his task to analyse atypical transactions. In this respect, see point 3 on the page "Policies, procedures, processes and internal control measures".

With regard in particular to the supervision of the system for analysing atypical facts and transactions that is implemented by the AMLCO, the NBB urges the **internal audit function** to pay particular attention to:

- the effectiveness of the preliminary analysis and analysis of atypical transactions by the AMLCO;

- the adequacy of the work carried out by the AMLCO to collect information as part of his task to analyse atypical transactions;
- the sufficiency of the human and technical resources allocated to the AMLCO to analyse atypical facts and transactions.

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



# Anti-Money Laundering Law of 18 September 2017 - Articles 45 and 46

## Art. 45

§ 1. Obligated entities shall perform a specific analysis, under the responsibility of the person appointed in accordance with Article 9, § 2, of the atypical transactions identified pursuant to Article 35, § 1, 1°, in order to determine whether these transactions can be suspected of being linked to money laundering or terrorist financing. In particular, they shall examine, as far as reasonably possible, the background and purpose of any complex and unusually large transactions, as well as any unusual patterns of transactions that have no apparent economic or lawful purpose.

To this end, they shall implement any measures that are necessary in addition to those referred to in Articles 19 to 41.

§ 2. Obligated entities shall draw up a written report on the analysis performed pursuant to § 1.

This report shall be drawn up under the responsibility of the persons referred to in Article 9, § 2, who shall provide adequate follow-up pursuant to the obligations described in this Title.

## Art. 46

In the cases referred to in Articles 33, § 1, 34, § 3 and 35, § 2, obligated entities shall perform a specific analysis of these situations under the responsibility of the person designated in accordance with Article 9, § 2, to determine whether the causes of the inability to fulfil the due diligence requirements could raise ML/FT suspicions and whether the CTIF-CFI should be notified, in accordance with Articles 47 to 54.

Obligated entities shall draw up a written report on the analysis performed pursuant to the first paragraph. This report shall be drawn up under the responsibility of the persons referred to in Article 9, § 2, who shall provide adequate follow-up pursuant to the obligations described in this Title.



## NBB anti-money laundering regulation of 21 November 2017 - Articles 16 and 18

### Art. 16

Obligated financial institutions shall set out in writing for their staff who are in direct contact with customers or instructed with carrying out their transactions:

1° the appropriate criteria enabling them to detect atypical transactions;

2° the procedure required to subject these transactions to a specific analysis under the responsibility of the AMLCO, in accordance with Article 45, § 1, of the Law, so as to determine whether these transactions may be suspected of being associated with money laundering or terrorist financing

### Art. 18

Pursuant to Article 9, §§ 1 and 2, of the Law, obliged financial institutions shall adopt appropriate procedures, for carrying out as soon as possible, depending on the circumstances, an analysis of the atypical transactions in order to determine, pursuant to Article 45 of the Law, whether the CTIF-CFI should be notified of the suspicions in accordance with Article 47 of the Law.



# Explanatory Memorandum to the Anti-Money-Laundering Law of 18 September 2017 - Articles 45 and 46

## Art. 45

One of the essential operational responsibilities of the anti-money-laundering compliance officer (AMLCO) designated in accordance with Article 9, § 2, of the draft Law consists of analysing atypical transactions detected during the ongoing due diligence (cf. draft Article 35, § 1, 1°). The objective of this analysis consists of determining if there is a suspicion of ML/TF or not, or reasonable motives for such a suspicion, and whether this gives rise to reporting the transaction concerned to the CTIF-CFI in accordance with draft Articles 47 et seq.

Where the AMLCO (or the persons acting under his/her authority) proceed(s) with this analysis, he/she must examine, as much as possible, the context and purpose of the transactions, in particular in the case of complex transactions for unusually high amounts or in the context of unusual processes with no apparent economic justification or legitimacy.

To proceed with this analysis of atypical transactions, the AMLCO shall firstly look into the results of the ongoing due diligence (cf. above). Nevertheless, the information he/she possesses in this respect may be insufficient to enable him/her to decide whether there is a suspicion of ML/TF. In this case, the second indent of § 1 imposes that the obliged entity must take (at the initiative of its AMLCO) the measures additional to those already applied as part of the ongoing due diligence and which appear necessary to be able to appreciate whether these transactions or activities seem suspicious or not. This provision transposes Article 18, § 2, 2nd sentence of the Directive that in this case requires specific enhanced due diligence which differs from the ongoing due diligence — where applicable increased — required under Articles 35 to 41 of this draft Law.

In all cases in which an atypical transaction is subjected to the analysis of the AMLCO, he/she must document the results of his/her analysis in a written internal report. This internal analysis report must in particular enable an understanding to be gleaned of the motives for which the AMLCO has decided that there is or is not a suspicion of ML/TF. However, because by virtue of Article 47, § 1, 1° it is not necessary for the report of a suspicion to identify the predicate criminal activity, it is equally not required that the analysis by the AMLCO and the written report that documents it identify this underlying criminality to conclude that the transaction concerned is suspect. However, it should be emphasised that such an internal report must be written whatever the decision made as to whether or not there is a suspicion of ML/TF and certainly as regards whether or not to report a suspicion to the CTIF-CFI. This report's purpose is mainly to allow the decisions made by the AMLCO to be justified ex post and to allow the effectiveness and pertinence of the decision-making process to be monitored.

## Art. 46

Whilst draft Article 45 concerns the case in which the transactions carried out or desired by a customer are qualified as atypical, Article 46 similarly regulates the cases in which, for whatever reason, the obliged entity is unable to fulfil its obligation:

- to identify or verify the identity of persons or legal arrangements involved in the business relationship or transaction (cf. draft Article 33);
- to identify the characteristics of the customer and the nature and purpose of the business relationship or occasional transaction (cf. draft Article 34, § 3); or

- to exercise ongoing due diligence on the business relationship (cf. draft Article 35, § 2).

In these cases, additional to the prohibition of entering into or maintaining the business relationship or carrying out the occasional transaction concerned, the obliged entity must examine, under the responsibility of its AMLCO, whether the causes of being unable to fulfil the obligations of due diligence are of a nature to give rise to a suspicion of ML/TF. This assumes that the obliged entity draws up and applies a mechanism of alerts to the AMLCO similar to that set out hereinabove as regards atypical transactions.

Just as is the case with the analysis of atypical transactions, that of the situations in which the obliged entity is unable to meet the obligations listed above should be the subject of a written report, whatever the decision made as regards the suspicious nature, or not, of the situation analysed and, consequently, as regards its communication, or not, to the CTIF-CFI.



# Reporting of suspicions

Home > Financial oversight > Combating money laundering and the financing of terrori...

## Legal and regulatory framework

- Anti-Money Laundering Law: Articles 47 to 54
- Anti-Money Laundering Regulation of the NBB: Article 22

## Explanatory Memorandum of the Anti-Money Laundering Law

- Articles 47 to 54

## Other reference documents

- CTIF-CFI's information note of 26 October 2017 regarding the disclosure of information to CTIF-CFI

## Comments and recommendations by the NBB

- Comments and recommendations

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



# Reporting of suspicions: Comments and recommendations by the NBB

Home > Financial oversight > Combating money laundering and the financing of terrori...

## Contents

- 1. Situations requiring the reporting of a suspicion to CTIF-CFI
- 2. Arrangements for reporting to CTIF-CFI
- 3. Consequences of reporting suspicions
- 4. Internal control measures

---

One of the most important AML/CFTP obligations for financial institutions is the fact they have to report a suspicion to CTIF-CFI when they know, suspect or have reasonable grounds to suspect that funds, transactions or a fact of which they are aware are linked to ML/FT. Summarised below are the situations requiring the reporting of a suspicion (see point 1), the practical arrangements for reporting to CTIF-CFI (see point 2), the consequences of reporting suspicions (see point 3) and the relevant internal control measures to be implemented (see point 4).

## 1. Situations requiring the reporting of a suspicion to CTIF-CFI

### 1.1. Reporting ML/FT suspicions following the analysis of atypical facts or transactions

In accordance with Article 47, § 1, of the Anti-Money Laundering Law, financial institutions must report to CTIF-CFI when they know, suspect or have reasonable grounds to suspect that the following are linked to ML or to FT:

- **funds** held by their customers, regardless of the amount;
- **transactions** carried out or ordered by their customers; or
- **facts**, including attempted transactions, which they are aware of.

Reporting to CTIF-CFI is required when the analysis described on the page “Analysis of atypical facts and transactions” concludes that an atypical transaction, the relevant funds or the atypical facts concerned are suspicious.

### 1.2. Other situations requiring the reporting of suspicions

Article 47, § 3, of the Anti-Money Laundering Law empowers the King to determine, by Royal Decree deliberated in the Council of Ministers and adopted upon the advice of CTIF-CFI, situations in which funds, transactions and facts should in any case be reported to CTIF-CFI without requiring an analysis by the AMLCO to conclude that there is a suspicion of ML/FT.

Likewise, Article 54, § 1, of the Anti-Money Laundering Law empowers the King to extend the obligation to report to CTIF-CFI to funds, transactions or facts pertaining to natural or legal persons that are linked to jurisdictions whose legislation is considered insufficient or whose practices are deemed to impede the fight against ML/FT, without requiring these funds, transactions or facts to be analysed in order to confirm a suspected link with ML/FT.

However, no Royal Decree implementing these two provisions of the Law has been adopted as of yet.

The provisions of European Law imposing restrictive measures against certain countries in order to fight against the proliferation of weapons of mass destruction and its financing also provide for an obligation directly applicable to financial institutions to immediately notify their Financial Information Unit (FIU), in Belgium CTIF-CFI, of any situations in which there are reasonable grounds to suspect that funds or transactions could be linked to the financing of the proliferation of weapons of mass destruction. Such cases of obligatory reporting to CTIF-CFI are currently listed in Article 23(1), points (e) and (f) of Council Regulation (EU) 2017/1509 of 30 August 2017 concerning restrictive measures against the Democratic People's Republic of Korea and repealing Regulation (EC) No 329/2007.

For an overview of and comments on all possible situations in which a reporting should be submitted to CTIF-CFI, the NBB urges financial institutions to consult CTIF-CFI's information note of 26 October 2017 regarding the disclosure of information to CTIF-CFI.

## 2. Arrangements for reporting to CTIF-CFI

### 2.1. Territorial scope of the obligation to report suspicions to CTIF-CFI

The obligation to report to CTIF-CFI applies to all financial institutions governed by Belgian Law, to the branches established in Belgium and to the central contact points of European payment or electronic money institutions that have independent agents or distributors in Belgium for all their activities in Belgium.

Moreover, Article 47, § 2, of the Anti-Money Laundering Law stipulates that when the financial institution operates in another EEA Member State without having any establishment there, suspicions regarding transactions carried out under the freedom to provide services in relation to customers established in that other Member State should also be reported to CTIF-CFI (as the FIU of the home country).

However, when a financial institution carries out activities on the territory of another EEA Member State through a subsidiary, a branch or another form of establishment (particularly agents or, in the case of electronic money institutions, distributors representing the institution in that Member State) this establishment on the territory of the other Member State is not subject to the Belgian Anti-Money Laundering Law but to the anti-money laundering legislation of its host country. Suspicious facts and transactions detected locally in accordance with this legislation should therefore be reported to the FIU of the host country. Neither the establishment on the territory of this host country nor its Belgian parent company can or may fulfil its legal reporting obligation correctly by reporting to CTIF-CFI with regard to the same facts or transactions. For this subject, please also refer to the page "Scope" and to the comments and recommendations formulated by the Bank on the page "Belgian parent companies" (chapter 3: Application of local legislation by branches and subsidiaries established abroad). These clarifications are without prejudice to the fact that information should be shared within groups whenever necessary (see the page "Belgian parent companies", chapter 2, section 2.3.1 Internal information sharing procedure of the group) or that a Belgian establishment should take into account the suspicious facts or transactions detected by another entity in its group in order to adequately analyse the atypical facts or transactions which were detected by this Belgian establishment and are linked to the same persons (see the page "Analysis of atypical facts and transactions", section 2.2. Responsibilities of the AMLCO).

### 2.2. Reporting entities

In accordance with article 49 of the Anti-Money Laundering Law, financial institutions governed by Belgian Law and branches established in Belgium by financial institutions governed by foreign law (by the law of another EEA Member State or of a third country) should in principle report and submit information to CTIF-CFI through their **AMLCO**. However, the AMLCO may delegate this responsibility to members of his service, who perform this task

under his supervision and direct responsibility. Furthermore, any manager, employee or representative of the financial institution or branch concerned should personally submit information to CTIF-CFI whenever the usual procedure through the AMLCO cannot be followed. This could be the case, for instance, when the AMLCO is unavailable to do so himself in a timely manner or when the persons in the obliged entities seem to be involved in a money laundering or terrorist financing activity and would impede the submission of information through the usual procedures.

European payment or electronic money institutions that have independent agents or distributors in Belgium who meet the criteria included in the page “Belgian central contact points of European payment institutions and electronic money institutions” should in principle report and submit information to CTIF-CFI through the **designated central contact point**.

## 2.3. Reporting procedures

Article 50 of the Anti-Money Laundering Law specifies that the information referred to in Articles 47, 48 and 66 should be submitted in writing or electronically according to the procedures laid down by CTIF-CFI. These procedures are currently included in CTIF-CFI's information note of 26 October 2017 regarding the disclosure of information to CTIF-CFI.

In practice, the NBB recommends that financial institutions report their suspicions through the secure ORIS site launched by CTIF-CFI on 1 September 2006. For this purpose, the reporting entity receives one or multiple secure access codes under the responsibility of the AMLCO, which are then distributed internally without requiring CTIF-CFI to know the identity of the employee who submits the reporting. This way, the reporting is submitted in the name and on behalf of the reporting entity. Additionally, this system enables reporting entities to automate a part of the reporting process.

## 2.4. Content of the reporting

La déclaration de soupçons doit au moins contenir les informations suivantes :

- the reporting entity's identification information and business contact details;
- the identification information of the customer and, where appropriate, of the beneficial owner who is the subject of the reporting as well as, where a business relationship has been established with the customer, the purpose and nature of this relationship;
- the description of the transaction and the elements of analysis which led to the reporting;
- the time limit for carrying out the transaction if this has not been done yet.

Financial institutions shall take care not to submit incomplete reportings which do not allow to ascertain the facts underlying the suspicion.

The description of the transaction and the elements of analysis which led to the reporting should mention noteworthy flows and/or the most significant amounts as well as the persons involved in these flows.

Where appropriate, the reporting of suspicions shall be accompanied by all other documents that are useful to CTIF-CFI (particularly bank statements, if possible in an electronically accessible format, documents related to the opening of an account or the signing of an insurance contract, etc.).

The NBB notes that it is essential that reportings of suspicions be drawn up correctly, regardless of the arrangements for submitting them. A clear, concise and accurate presentation of the information in the reporting is of particular importance for the efficiency of the AML/CFTP policy.

## 2.5. When to submit the reporting to CTIF-CFI

### 2.5.1. Principle of reporting before carrying out the transaction

In accordance with Article 51 of the Anti-Money Laundering Law, suspicions should generally be reported to CTIF-CFI before the transaction is carried out, where appropriate indicating the time limit within which it should be carried out.

However, the reporting can occur immediately after carrying out the transaction in the following two cases:

- when it is not possible to delay carrying out the transaction due to its nature;
- when delaying the transaction could prevent prosecution of the persons benefiting from the money laundering.

The first derogation applies when the transaction is instantaneous. Such is the case with a manual foreign exchange transaction whereby currencies are exchanged immediately, or with a transaction that is carried out directly by the customer himself without any intervention from an employee of the financial institution, for instance by using a home banking or mobile application. This derogation can also apply when the transaction must be carried out within a very short time limit, which hinders a systematic a priori detection. This is the case, for example, with transactions of the banking sector, the investment and payment services sector and, more exceptionally, the insurance sector, which must be carried out immediately. In their AML/CFTP procedures, the institutions shall clarify for which transactions reportings must take place before or after the former have been carried out.

The second derogation also applies if delaying the transaction could prevent prosecution of the persons benefiting from the money-laundering, in particular if there are reasons to fear that delaying the transaction could alert the customer and encourage him to take immediate measures to hide his funds, which are suspected of having illicit origins, from the investigations of CTIF-CFI or of the judicial authorities.

In both cases, these derogations must be implemented strictly and CTIF-CFI should be informed of the reason why it could not be notified before the transaction was carried out.

### 2.5.2. Time limit for reporting after carrying out the transaction

After carrying out a transaction meeting the conditions set out in Article 51 of the Anti-Money Laundering Law, the reporting should be submitted "immediately" to CTIF-CFI. This provision introduces an obligation to act promptly, requiring each financial institution to ensure, regardless of its organisation and at any stage of its process leading, where appropriate, to a reporting, that the necessary steps are taken as quickly as possible. For instance, financial institutions shall ensure that they do not spend more time than strictly necessary on the investigations and analysis following the reporting of an atypical fact or transaction.

## 2.6. Additional reportings and requests for information by CTIF-CFI

Article 48 of the Anti-Money Laundering Law stipulates that financial entities are obliged to follow up on the requests for additional information submitted to them by CTIF-CFI within the time limits set by it.

Furthermore, any information that could invalidate, confirm or modify the information included in a reporting of suspicions should be reported immediately to CTIF-CFI, regardless of the amount and a fortiori if a customer carries out new suspicious transactions. When a first reporting of suspicions is followed by multiple transactions which should be brought to the attention of CTIF-CFI, the reporting entity may, for the sake of efficiency, bundle multiple transactions in a single additional reporting which pertains to a specific period of transactions determined on a case-by-case basis. In such a case, the additional reporting shall specify the procedure for bundling the transactions reported. If necessary, multiple additional reportings of suspicions may be submitted by the same obliged entity.

## 3. Consequences of reporting suspicions

The main consequences of reporting a suspicion to CTIF-CFI are:

1. prohibition of disclosure;
2. protection of reporting entities;
3. obligation to carry out an individual re-assessment of the customer's ML/FT risks; and

#### 4. obligation to retain documents related to the reportings submitted.

For the first two consequences, please refer to the pages “Prohibition of disclosure” and “Protection of reporting entities”.

The third consequence mentioned above results from Article 22 of the Anti-Money Laundering Regulation of the NBB, which stipulates that when an obliged financial institution wishes to report suspicions pursuant to Article 47 of the Anti-Money Laundering Law, it shall carry out an individual re-assessment of ML/FT risks, in accordance with Article 19, § 2, of the Law, taking account of the specific fact that a suspicion has been raised about the customer concerned. On the basis of this re-assessment and its customer acceptance policy, the financial institution shall decide whether to maintain the business relationship subject to the implementation of due diligence measures adapted to such re-assessed risks, or whether to terminate it. The NBB highlights the fact that this must be an individual decision taken on the basis of the individual assessment of all available information on the customer and the business relationship with the customer. It considers that a decision in principle to systematically terminate business relationships when a suspicion has been reported to CTIF-CFI would not comply with Article 22 of the Anti-Money Laundering Regulation and would moreover lead to the customer being informed indirectly and implicitly of the fact that a suspicion against him has been reported to CTIF-CFI.

As regards the fourth consequence, documents on the transactions carried out by the financial institutions shall be retained for a period of ten years following the termination of the business relationship concerned. When applied to the reporting of suspicions, this retention obligation pertains to the copy of the reporting of suspicions and, where appropriate, of the accompanying documents as well as to the acknowledgement of receipt of the reporting by CTIF-CFI. For further information on this subject, see the page “Retention and protection of data and documents”.

## 4. Internal control measures

Financial institutions are expected to periodically and permanently monitor the adequacy of the organisational measures implemented to comply with the legal obligation to report suspicions to CTIF-CFI. In this respect, the NBB expects financial institutions in particular to monitor their time limits for reporting suspicions.

Additionally, the NBB urges the internal audit function to pay particular attention to:

- the adequacy of the policy implemented by the AMLCO for reporting suspicions, for submitting additional reportings and for responding to requests for information by CTIF-CFI;
- the adequacy of the time limits for reporting suspicions, in order to avoid late reporting of suspicions by the financial institution;
- compliance with the instructions of CTIF-CFI regarding the arrangements for reporting suspicious transactions and regarding the information to be included in the reporting; and
- compliance with the consequences of reporting a suspicious transaction to CTIF-CFI.



# Anti-Money Laundering Law of 18 September 2017 - Articles 47 to 54

## Art. 47

§ 1 The obliged entities shall report to CTIF-CFI, when they know, suspect or have reasonable grounds to suspect:

1° that funds, regardless of the amount, are related to money laundering or terrorist financing;

2° that transactions or attempted transactions are related to money laundering or terrorist financing. This obligation also applies when the customer decides not to carry out the intended transaction;

3° other than the cases referred to in 1° and 2°, that a fact of which they know, is related to money laundering and terrorist financing.

The obligation to report to CTIF-CI in accordance with 1° to 3°, does not entail that the obliged entity must identify the predicate money laundering offence.

§ 2. The obliged entities also report to CTIF-CFI suspicious funds, transactions or attempted transactions and facts, referred to in paragraph 1, of which they know as part of activities carried out by them in another Member State without having a subsidiary, branch or other type of establishment through agents or distributors representing them there.

§ 3. The obliged entities report to CTIF-CFI funds, transactions and facts determined by the King, by Decree deliberated in the Council of Ministers, upon the advice of CTIF-CFI.

§ 4. The obliged entities report to CTIF-CFI, in accordance with paragraphs 1 to 3, within the periods referred to in Article 51.

## Art. 48

The obliged entities respond to the requests for additional information sent by CTIF-CFI, in accordance with Article 81, within the periods determined by CTIF-CFI.

## Art. 49

In principle any information or intelligence referred to in Article 47 and 48 is reported to CTIF-CFI by the person(s) designated pursuant to Article 9, § 2.

Any manager, employee, agent or distributor of a obliged entity referred to in Article 5, § 1, 1° to 22°, and 29° to 33°, as well as any employee or representative of an obliged entity referred to in Article 5, § 1, 23° to 28°, who is an obliged entity himself, shall nevertheless personally report the relevant information or intelligence to CTIF-CFI each time when they procedure referred to in the first subparagraph cannot be followed.

## Art. 50

The information and intelligence referred to in Articles 47, 48, and 66, § 2, third subparagraph, is reported to CTIF-CFI in writing or electronically, in accordance with its terms.

The King may, upon the advice of CTIF-CFI, determine by Decree, a list of obliged entities for which the reporting of information and intelligence referred to in the first subparagraph, is done exclusively online.

## Art. 51

§ 1. The information relating to a transaction, referred to in Article 47, § 1, 2°, and §§ 2 and 3, is reported to CTIF-CFI prior to carrying out the transaction. Where appropriate, the period of time is mentioned during which the transaction must be carried out.

In case the obliged entities are unable to inform CTIF-CFI prior to carrying out the transaction, either because it is not possible to delay carrying out the transaction due to its nature, or because doing so could prevent prosecution of the individuals benefiting from this transaction, they shall report this transaction to CTIF-CFI immediately after carrying out the transaction.

In such a case, the reason why it was not possible to inform CTIF-CFI beforehand should be indicated.

§ 2 When the obliged entities know, suspect or have reasonable grounds to suspect that the funds or a fact, referred to in Article 47, § 1, 1° and 3°, and § 2, are linked to money laundering or terrorist financing, or when they become aware of funds or facts referred to in Article 47, § 3, they immediately report this to CTIF-CFI.

## Art. 52

[By way of derogation from Articles 47 and 49], lawyers who, while carrying out the activities listed in Article 5, § 1, 28°, are faced with funds, transactions to be carried out or facts referred to in Article 47 are obliged to immediately inform the President of the bar association to which they belong.

*First subparagraph modified by Article 112 of the Law of 30 July 2018 – Belgian Official Gazette of 10 August 2018*

The President of the bar association shall verify compliance with the conditions referred to in Article 5, § 1, 28°, and 53. Where appropriate, he shall transmit the information unfiltered to CTIF-CFI.

## Art. 53

By way of derogation from Articles 47, 48 and 54 the persons referred to in Article 5, § 1, 23° to 28°, shall not transmit this information and intelligence referred to in these Articles if it was received from or obtained on one of their clients in the course of ascertaining that client's legal position or performing their task of defending or representing that client in, or concerning judicial proceedings, including giving advice on instituting or avoiding proceedings, whether such information is received or obtained before, during or after such proceedings, unless they take part in the money laundering or terrorist financing activities themselves or provide legal advice for money laundering or terrorist financing purposes, or if they know their client requests advice for money laundering or terrorist financing purposes.

## Art. 54

§ 1. The King may, by Decree deliberated in the Council of Ministers upon the advice of CTIF-CFI extend the reporting obligation to funds, transactions and facts involving natural or legal persons domiciled, registered or located in a country or jurisdiction whose legislation is considered insufficient or whose practices are deemed to impede the fight against money laundering and terrorist financing by the national risk assessment referred to in Article 68, or by a competent international or European consultative and coordinating authority.

He may determine the type of such facts, funds and transactions as well as their minimum amount which is most appropriate to mitigate the risks linked to these countries or jurisdictions.

§ 2. When the national risk assessment referred to in Article 68 identifies a country or a jurisdiction whose legislation is considered insufficient whose practices are deemed to impede the fight against ML/TF the King may, by Decree deliberated in the Council of Ministers and without prejudice to paragraph 1 determine other countermeasures proportionate to the high money laundering or terrorist financing risks of the country or jurisdiction involved.



## NBB anti-money laundering regulation of 21 November 2017 - Article 22

### Art. 22

When an obliged financial institution wishes to report suspicions pursuant to Article 47 of the Law, it shall carry out an individual re-assessment of ML/FT risks, in accordance with Article 19, § 2, of the Law, taking account of the specific fact that a suspicion has been raised about the customer concerned. It shall decide, on the basis of this re-assessment and the customer acceptance policy referred to in Title 3, whether to maintain the business relationship subject to the implementation of due diligence measures adapted to such re-assessed risks, or whether to terminate it.



# Explanatory Memorandum to the Anti-Money-Laundering Law of 18 September 2017- Articles 47 to 54

## Art. 47

The draft Article transposes Article 33, § 1, first paragraph, a) and second paragraph of Directive 2015/849 concerning the obliged entities' obligation to report suspicions to the competent FIU.

The draft Article takes over and consolidates, with no changes of a substantive nature, the obligation of reporting suspicions already provided for in Articles 23 to 26 of the Law of 11 January 1993 without maintaining the provisions of Article 26, § 2, second paragraph of the aforementioned Law, for casinos that benefited, via Royal Decree, from a list of transactions to automatically report to the CTIF-CFI, given that the possibility for the King to introduce an objective reporting obligation is extended to all the obliged entities in § 3 of the draft Article.

In its opinion, the Council of State considers that § 3 confers on the King a very broad power, the purpose of which should be better regulated by the new Law and all the more so because professional secrecy could be at issue here. This power had already been conferred with no further specific regulation in the law by virtue of Article 26, § 2, second indent of the said Law, for casinos.

It is extremely difficult to precisely determine the funds, transactions and acts for which an objective and therefore systematic report could be required. It should be underlined that the reporting obligation is essentially a reporting obligation that is subjective and the outcome of an intellectual process, and that the objective reporting obligation would only be invoked in very specific circumstances for financial transactions showing a high risk of money laundering or terrorist financing without prejudicing the professional secrecy that some non-financial professions subject to the draft Law may invoke by virtue of the draft law vis-à-vis the CTIF-CFI.

This measure could also be required as one of the counter-measures to mitigate the risks of money laundering or terrorist financing as specified in Recommendation 19 of the FATF, as well as Article 54 of the draft Law.

For the purposes of clarification, the methods for these obligations are contained and detailed in draft Articles 50 et seq. (reporting in writing, time of reporting etc.).

As is already the case today, by virtue of Articles 23 to 26 of the Law of 11 January 1993, and as required by Article 33, § 1, first paragraph, a) and second paragraph of Directive 2015/849, the obligation to report to the CTIF-CFI also covers funds, regardless of the amount involved, where it is known, suspected or there are reasonable grounds to suspect that they are related to money laundering, i.e. that they are the proceeds of criminal activity, or terrorist financing, as well as suspicious transactions including attempted suspicious transactions. If the funds themselves that are involved in the transaction or the business relationship could give rise to suspicion (for example because their origin cannot be identified with sufficient certainty, or because of their size for the customer's characteristics), the suspicion may also be created by transactions carried out using the funds which, in and of themselves, have not given rise to suspicions as indicated above. As a result, for example, the suspicion can result from a series of transactions which taken separately had not aroused suspicion and relating to funds that had not aroused suspicion but which, because of their juxtaposition or concomitance nevertheless appear likely to be involved in ML/TF. The obligation to report to the CTIF-CFI is also triggered by knowledge of a fact that could constitute an indication of ML/TF. As regards "knowledge of a fact", it is no longer the execution of a transaction in particular that is referred to but rather facts in a more general sense that could arise for example from the intervention of the judicial authorities or be revealed by the media. The suspicion may also arise in this case from the behaviour of the customer (unusual lack of interest in the financial conditions proposed, physical surveillance of the customer by a third party, etc.).

In order to dissipate any doubts on the matter, the draft Article now expressly emphasises that it is not up to the obliged entities to determine any criminal activity underlying the suspected money laundering. As a result, for example, as soon as an obliged entity suspects that funds are of an illicit origin that could constitute tax fraud, this obliged entity must send a report to the CTIF-CFI without needing to first determine whether or not this tax fraud is in fact serious. Consequently, maintaining Article 28 of the Law of 11 January 1993 which specifically referred to suspicions of money laundering stemming from serious tax fraud, whether organised or not, is no longer appropriate.

As can be read in Recital 37 of Directive 2015/849, all Member States must set up an FIU to collect and analyse the information they receive “with the aim of establishing links between suspicious transactions and underlying criminal activity in order to prevent and combat money laundering and terrorist financing”.

The fact that it does not fall to reporting entities to identify the predicate criminal activity is also confirmed in Article 37 of Directive 2015/849 which reads as follows: “Disclosure of information in good faith by an obliged entity or by an employee or director of such an obliged entity in accordance with Articles 33 and 34 shall not constitute a breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, and shall not involve the obliged entity or its directors or employees in liability of any kind even in circumstances where they were not precisely aware of the underlying criminal activity and regardless of whether illegal activity actually occurred”.

In the majority of cases, reporting entities are not in a position to be aware of the criminal activity underlying the suspected money laundering. It is up to the CTIF-CFI to find out, by way of an in-depth analysis, the link between the funds concerned, the suspicious transaction or the facts reported and one of the forms of criminality referred to by the Law (Senate, 1323/1, S.O. 1994-1995, p. 5 and Senate, 1335/1 and 1336/1, S.O. 1997-1998, p. 18).

The preventive system, which gives a more restrictive definition of money laundering than the criminal approach has always conferred to the CTIF-CFI and not to reporting entities, the task of filtering between reports relating to serious criminality justifying the collaboration of the financial and non-financial sector and those considered less of a threat to social and economic order. By playing its filtering role, the CTIF-CFI prevents the public prosecutor's office from being encumbered by irrelevant reports (Parliamentary documents, Chamber of Representatives 1992-1993, 689/2, p. 3; A. De Nauw, *Les métamorphoses administratives du droit pénal de l'entreprise*, Gand, Mys & Breesch, 1994, p. 135).

This does not prevent reporting entities being able to refer to one or another underlying crime if they are aware or suspect, or they have reasonable grounds to suspect that the money laundered is the proceeds of one or another criminal activity mentioned in Article 4, 23° of the draft Law.

As this has always been the case in the Law of 11 January 1993, the slightest suspicion suffices for the reporting obligation to apply. This is the case if the professional is unable to rule out that the transaction or the fact he/she is aware of is linked to money laundering or terrorist financing (Explanatory Memorandum, Parliamentary documents, Chamber of Representatives, 1997-1998, 1335/1, p. 18). Money laundering under the draft Law consists of, as it did in the past, acts (conversion, transfer, concealment, etc.) relating to funds that are the proceeds of criminal activity. The slightest suspicion of the illicit origin or destination of funds that the professional must handle (conversion, transfer, concealment, etc.) or of a transaction or series of transactions that seem suspicious suffices to trigger the obligation to report the suspicion.

Obliged entities are clearly expected to report a suspicion if they have not obtained, from the information and documents gathered from the customer or available in the customer's file, assurance as to the legality of the funds or the transaction, or as regards its economic, legal or fiscal justification.

Whereas Article 33, § 1, a) of Directive 2015/849 imposes a reporting obligation “where the obliged entity knows, suspects or has reasonable grounds to suspect that funds [...]”, the Law of 11 January 1993 only used the terms “know or suspect”, because it has been considered at the time that the notion of “reasonable grounds to suspect” is implicitly included in the notion of “suspicion”, as it could be aroused by the slightest indication, whether subjective or objective. After all, even though suspicion refers to a subjective notion, it does not mean that it cannot be based on objective criteria (J. Spreutels, *La Cellule de traitement des informations financières et la prévention du blanchiment de capitaux en Belgique*, Bruylant, Bruxelles, 2003, p. 103). The draft Article, by from now on making express reference to “reasonable grounds to suspect” ensures compliance with Directive 2015/849 and above all more effectiveness in the system. Although this change does not in any way change the obligations as regards reporting

suspicious which remain subjective in the sense described above, this change enables the supervisory authority to sanction obliged entities that have not made a declaration even though they were in possession of facts that should reasonably have led it to suspect money laundering or terrorist financing.

The draft Article transposes Article 33, § 2 of Directive 2015/849 which clearly provides that reports of suspicions should be sent to the FIU of the Member State on the territory of which the obliged entity that sends the information is established. The reports of suspicions must therefore be sent to the FIU of the Member State where the obliged entity has its registered office, its subsidiary, its branch or any other form of establishment through agents or distributors representing it.

Where the obliged entity acts in another Member State without an establishment, suspicions concerning transactions carried out under the freedom to provide services in relation to customers established in this other Member State are equally sent to the FIU of the home country of the obliged entity, which is the FIU of the State in which the obliged entity is established, and not the host country, which is the State in which the obliged entity operates without an establishment.

Article 22, § 2 of the third Directive lacked legal clarity on the subject by requiring “establishments and persons” subject to this Directive to send the information to the FIU “of the Member State in whose territory the institution or person forwarding the information is situated”.

In the Jyske Bank judgment issued by the Court of Justice of the European Union on 25 April 2013 (Case C-212/11 Jyske Bank Gibraltar Ltd v Administración del Estado), the Spanish government maintained that these terms gave it the right to require credit institutions (in this case Jyske Bank) carrying on their activities in Spain without being established there to send their reports of suspicions to the Spanish FIU, which is the FIU of the host country, given that the transactions were carried out on its territory. Directive 2015/849 and the draft Law put an end to this ambiguity.

The draft Article maintains, but extends the possibility for the King to introduce objective reporting obligations for all the obliged entities.

## Art. 48

The draft Article transposes Article 33, § 1, first paragraph, a), second part, and b) of Directive 2015/849 which provides that obliged entities are obliged to cooperate fully with the FIU “by promptly providing the FIU, directly or indirectly, at its request, with all necessary information in accordance with the procedures established by the applicable law”.

The draft Article confirms the obligation, which already existed by virtue of Article 33 of the Law of 11 January 1993, to respond, within the periods determined by the CTIF-CFI, to requests for additional information sent by the CTIF-CFI. The specific powers of the CTIF-CFI on the subject will be detailed as follows in draft Article 81.

## Art. 49

The draft Article transposes Article 33, § 2 of Directive 2015/849 which identifies the person appointed for sending the information to the FIU. The draft Article to a large extent takes over the provisions of Article 29 of the Law of 11 January 1993.

It is usually the AMLCO who reports and passes on information to the CTIF-CFI.

However, all employees and representatives of the entity in question personally proceed with the transmission of information to the CTIF-CFI any time that the normal procedure via the AMLCO is unable to be followed.

This could be the case for example if the AMLCO cannot be reached in good time, or where the directors of the obliged entities seem involved in a money laundering or terrorist financing activity and would hinder the transmission of the information (Parliamentary documents, Senate, 1991-1992, 468-1, p. 18).

For non-financial professions subject to professional secrecy within the meaning of Article 458 of the Criminal Code referred to in Article 5, § 1, 23° to 28° of the draft Law, it is expressly provided for, as is already the case in the Law of 11 January 1993, that it is the responsibility of the professional (company auditor, auditor, external accountant, external tax consultant, registered external accountant, registered external tax accountant, notary, bailiff or lawyer) to proceed with the reporting and therefore not of an employee if the AMLCO is unable to proceed with the reporting. However, this report does not necessarily have to come from the title-holder in charge of the file as long as it comes from a member of the firm that holds the title of the profession concerned.

For these aforementioned non-financial professions, where the AMLCO is unable to fulfil his/her obligation, the employees of these professionals may not personally proceed with this transmission.

This is not authorised given the specific characteristics of these professions which are subject to professional secrecy. In a judgment of 23 January 2008, the Constitutional Court considered that this possibility would pose a threat to a lawyer's professional secrecy and it has now eliminated the reference to lawyers in Article 18, second paragraph of the Law of 11 January 1993, amended by Article 30, 2° of the Law of 12 January 2004.

Given the complexity of the obliged entities' obligations under this Law, it is now stipulated that every subjected entity, without exception, is required to designate an AMLCO.

## Art. 50

The draft Article specifies, as was already the case under the Law of 11 January 1993, that the information and intelligence referred to in draft Articles 47, 48 and 66 should be reported in writing or electronically in accordance with the terms defined by the CTIF-CFI.

These terms are currently contained in the CTIF-CFI guideline of December 2013 addressed to reporting entities. This guideline will be adapted to the new Law without making any substantive changes as to the terms for transmitting information.

The draft Article also specifies that the King may make it obligatory for reports of suspicions to be transmitted online.

An online reporting system was launched on 1 September 2006. This system, which was named ORIS, allows reporting entities to report transactions and facts via a secure website. The reporting entity receives, under the responsibility of the AMLCO, one or more secure access codes, which are subsequently distributed internally, without the CTIF-CFI having to know the identity of the reporting employee. The reporting is done in the name and on behalf of the reporting entity. The system also allows reporting entities to automate part of the reporting process. The CTIF-CFI hopes that more and more reporting entities will use this online reporting system. Its use can now also be made mandatory by Royal Decree.

## Art. 51

The draft Article transposes Article 35 of Directive 2015/849 by placing the emphasis on the period of time for reporting to the CTIF-CFI.

As in the past, as a general rule, the CTIF-CFI must be sent the report of the suspicion before the transaction is executed with an indication, where applicable, of the deadline by which it must be executed. The draft Article also puts all the obliged entities on an equal footing because neither Directive 2015/849 nor the FATF make any distinction between the obliged entities based on their obligation to report to the CTIF-CFI.

As has always been the case for financial professions, now non-financial professions faced with transactions requiring handling funds (receipt of funds, transfer into an account, etc.) will have to report suspicions to the CTIF-CFI before executing the transaction.

As was the case in the past, there is an exception to the general rule, which can be used whenever justified. The report may be proceeded with immediately after the execution of the transaction either because it is not possible to delay carrying out the transaction due to its nature, or because doing so could prevent the prosecution of the individuals benefiting from this transaction. "These terms in particular refer to the hypothesis of very high sums being

deposited at the counter of an agency of which the depositor is not a customer, in conditions which are of a nature so as to give rise to a doubt as to the origin of the funds presented. In this case, it is preferable for the purposes of the subsequent investigation that the deposit may be accepted forthwith by the entities or persons, with the proviso that they immediately inform the unit, rather than see this money disappear again with the risk of definitively losing trace of these funds of a potentially illicit origin" (Parliamentary documents, Chamber of Representatives, 1991-1992, 468/1, p. 16).

Finally, based on the draft Article, the obliged entities must furthermore immediately report to the CTIF-CFI:

- funds which they know, suspect or have reasonable grounds to suspect are linked to money laundering or terrorist financing: these are funds they know or suspect are of illicit origin but for which they do not execute any transactions (cf. draft Article 47, § 1, 1° and § 2 and Article 33, § 1, a) of the Directive);
- all the facts they are aware of and which they know, suspect or have reasonable grounds to suspect are linked to money laundering or terrorist financing (cf. draft Article 47, § 1, 3° and § 2); as well as
- funds and facts determined by the King (cf. draft Article 47, § 3).

## Art. 52

Draft Article 11 of the draft Law transposes Article 34, § 1 of Directive 2015/849 and takes over, with no changes of a substantive nature, the current provisions of Article 26, § 3, first and third paragraphs of the Law of 11 January 1993, on the subject of lawyers.

By virtue of the draft Article, lawyers who, while carrying out the activities listed in draft Article 5, § 1, 28°, are faced with funds, transactions to be carried out or facts such as those referred to in Article 47 are obliged to immediately inform the President of the bar association to which they belong.

The President of the bar association verifies compliance with the conditions referred to in draft Article 5, § 1, 28°, and 53. He/she must verify that the lawyer is acting within the scope of the law before deciding to transmit the information to the CTIF-CFI. His/her assessment does not relate to the suspicion communicated by the lawyer. If the conditions of application are adhered to, the President of the bar association will decide to transmit the information received from the lawyer to the CTIF-CFI unfiltered under the terms determined by the CTIF-CFI.

Through the Law of 12 January 2004 amending the Law of 11 January 1993 on preventing use of the financial system for purposes of money laundering, the Law of 22 March 1993 on the legal status and supervision of credit institutions and the Law of 6 April 1995 on the legal status and supervision of investment firms, intermediaries and investment advisers, the Belgian legislator had already taken into account, like European law-makers, of the specific characteristics of the profession of lawyer. Neither Directive 2015/849 nor this Law make amendments to the acts already referred to by the preceding Directives as regards lawyers.

In its judgment No 10/2008 of 23 January 2008, the Constitutional Court interpreted the extent of lawyers' obligations to inform and cooperate with the CTIF-CFI by virtue of the Law of 11 January 1993. These interpretations still apply.

By way of the judgment of 26 June 2007 issued in case C-305/05, the Court of Justice of the European Union, following a preliminary question asked by interlocutory judgment No 126/2005 of 13 June 2005 by the Constitutional Court, said that the fundamental right to a fair trial is not contravened by the obligation of lawyers to inform and cooperate with the authorities responsible for combating money laundering, taking into account the limits to these obligations imposed or permitted by Directive 91/308/EEC as amended by Directive 2001/97/EC.

In this respect, the Constitutional Court provides, in its judgment No 10/2008 of 23 January 2008 that the information known by lawyers in the exercise of the activities essential to their profession, including on the subjects listed in Article 3, 5° of the Law of 11 January 1993, taken over in Article 5, § 1, 28° of the draft Law, i.e. assistance and defence in court of the customer, as well as legal advice, even outside any judicial proceedings, remain covered by professional secrecy. They may therefore not be reported to the CTIF-CFI. However, on the subjects listed in Article 3, 5° of the Law of 11 January, taken over in Article 5, § 1, 28° of the draft Law, where lawyers exercise an activity

outside the specific remit of defence, representation in court or legal advice, they are subject to the obligation to communicate to the CTIF-CFI any pertinent information within the meaning of the Law of 11 January 1993, as well as of the draft Law, that they are aware of.

The Constitutional Court defines the activity of legal advice as the activity “of informing customers on the current state of the legislation applicable to his/her personal situation or the transaction that they plan to carry out, or of advising on the way in which to carry out this transaction within the legal framework”.

In its judgment No 10/2008 of 23 January 2008, the Constitutional Court also considers that the intervention of the President of the bar association is necessary where the CTIF-CFI wishes to obtain additional information from lawyers who have reported a suspicion to their President of the bar association. The Constitutional Court explains that the intervention of the President of the bar association in the transmission of information by lawyers to the CTIF-CFI is an essential guarantee, both for the lawyers and for the customers, which makes it possible to ensure that no threat will be posed to professional secrecy except in cases strictly provided for by the Law. The President of the bar association has the role of checking that the legal conditions of application of the obligation of communication are indeed fulfilled and, if he/she identifies that this is not the case, he/she must abstain from sending the information communicated. If it is, he/she shall pass on the information.

The Constitutional Court clearly refers to the case in which the lawyer has already reported a suspicion through his/her President of the bar association. It also specifies that this same filter must exist where, after this first contact is established, more detailed information is requested from the lawyer who filed the report.

Consequently, this does not prejudice the right of the CTIF-CFI to ask the lawyer directly for additional information where this lawyer is not the author of the initial report, but is involved in a report of a suspicion received from another reporting entity. In this case, the lawyer questioned is of course not prohibited from responding to the CTIF-CFI through the President of his/her bar association, which is at the same time compliant with the legal provision and the interpretation of the Constitutional Court.

## Art. 53

The draft Article transposes Article 34, § 2 of Directive 2015/849 and takes over, with no changes of a substantive nature, the current provisions of Article 26, § 1, second paragraph and § 3, second paragraph of the Law of 11 January 1993.

The draft Article reconfirms the professional secrecy that notaries, bailiffs, accounting professions, and lawyers may invoke as regards their obligation to report suspicions and their obligation to respond to the additional information requested by the CTIF-CFI, as well as the fact that this professional secrecy is not absolute.

In this respect, Recitals 9 and 10 of Directive 2015/849 provide that: “(9) Legal professionals, as defined by the Member States, should be subject to this Directive when participating in financial or corporate transactions, including when providing tax advice, where there is the greatest risk of the services of those legal professionals being misused for the purpose of laundering the proceeds of criminal activity or for the purpose of terrorist financing. There should, however, be exemptions from any obligation to report information obtained before, during or after judicial proceedings, or in the course of ascertaining the legal position of a client. Therefore, legal advice should remain subject to the obligation of professional secrecy, except where the legal professional is taking part in money laundering or terrorist financing, the legal advice is provided for the purposes of money laundering or terrorist financing, or the legal professional knows that the client is seeking legal advice for the purposes of money laundering or terrorist financing.

As was the case in the past, these professions do not transmit this information when such information was received from, or obtained on, one of their clients, in the course of ascertaining the legal position of their client, unless they take part in the money laundering or terrorist financing activities or provide legal advice for money laundering or terrorist financing purposes, or they know that their client requests legal advice for these purposes.

In the latter three cases, the obligation to report and the obligation to transmit additional information are legitimate.

However, the Constitutional Court had also specified in its judgment No 10/2008 of 23 January 2008, that lawyers who, having made the effort to dissuade a customer from carrying out or participating in a money laundering or terrorist financing transaction he/she is aware is illegal, find that they have failed in this endeavour, are obliged, if

they find themselves in a case in which the obligation of communication applies, to transmit the information they are aware of to the President of the bar association, who will in turn transmit it to the CTIF-CFI. In this case, the lawyer concerned may not continue to act on behalf of the customer concerned and must put an end to the relationship that links him/her to the latter. There is therefore no longer a question of a relationship of trust between the lawyer and his/her customer. The same interpretation applies to the other non-financial professions referred to.

## Art. 54

The draft Article takes over the content of Article 27 of the Law of 11 January 1993 by giving the power to the King to extend the reporting obligation of obliged entities to funds, transactions and facts involving natural or legal persons domiciled, registered or located in a country or jurisdiction whose legislation is considered insufficient or whose practices are deemed to impede AML/CFT through the national risk assessment referred to in draft Article 68 or by a competent international or European consultative and coordinating authority.

The draft Article also takes into account consequences of the application of Recommendation 19 by the FATF concerning "higher-risk countries" as well as the application of the European Commission's power as regards its policy on third countries by virtue of Article 9 of Directive 2015/849.

The competent international or European consultative and coordinating authority, in particular refers to the FATF, the Council of Europe – MONEYVAL and the European Commission by virtue of Article 9 of Directive 2015/849.

Based on this Recommendation, the countries should be able to apply adapted counter-measures where the FATF asks them to do so. The countries should also agree to apply the counter-measures independently of any call by the FATF to do so. These counter-measures should be effective and proportionate to the risks. The draft Article also refers to introducing this royal prerogative.

In the interpretive notes to Recommendation 19, the FATF cites examples of counter-measures that could be taken by countries, which include the following measures, as well as any other measure with a similar effect in terms of risk mitigation:

- Requiring financial institutions to apply specific elements of enhanced due diligence.
- Introducing enhanced relevant reporting mechanisms or systematic reporting of financial transactions.
- Refusing the establishment of subsidiaries or branches or representative offices of financial institutions from the country concerned, or otherwise taking into account the fact that the relevant financial institution is from a country that does not have adequate AML/CFT systems.
- Prohibiting financial institutions from establishing branches or representative offices in the country concerned, or otherwise taking into account the fact that the relevant financial institution is from a country that does not have adequate AML/CFT systems.
- Limiting business relationships or financial transactions with the identified country or persons in that country.
- Prohibiting financial institutions from relying on third parties located in the country concerned to conduct elements of the CDD process.
- Requiring financial institutions to review and amend, or if necessary terminate, correspondent relationships with financial institutions in the country concerned.
- Requiring further supervisory examination and/or external audit requirements for branches and subsidiaries of financial institutions based in the country concerned.
- Requiring further external audit requirements for financial groups with respect to any of their branches and subsidiaries located in the country concerned.

The second paragraph of the draft Article grants the power to the King, independently of any call from a competent international or European consultative and coordinating authority as required under FATF Recommendation 19, to determine other counter-measures proportionate to the high risk of ML/TF of the country or territory concerned.



## Prohibition of disclosure

Home > Financial oversight > Combating money laundering and the financing of terrori...

### Legal and regulatory framework

- Anti-Money Laundering Law: Articles 55 and 56

### Explanatory Memorandum of the Anti-Money Laundering Law

- Articles 55 and 56

### Other reference documents

- CTIF-CFI's information note of 26 October 2017 regarding the disclosure of information to CTIF-CFI

## Comments and recommendations by the NBB

Financial institutions should exercise the greatest discretion with regard to the information they submit to CTIF-CFI as well as to the ongoing or potential analyses of facts or transactions that could be linked to money laundering or terrorist financing.

### 1. Principle of the prohibition of disclosure

In accordance with Article 55 of the Anti-Money Laundering Law, financial institutions may under no circumstances provide the customer concerned or third parties with information that is being, will be or has been submitted to CTIF-CFI in accordance with Articles 47 (**reporting of suspicions**), 48 (**additional information**) and 54 (reportings concerning a transaction linked to a high-risk country) of the Anti-Money Laundering Law, or inform them that a **money laundering or terrorist financing analysis** is being, or may be carried out. The prohibition against informing the customer or third parties that a money laundering or terrorist financing analysis is ongoing or may be started, covers both the internal analyses performed by the obliged entity's AMLCO to determine in particular if a reporting should be submitted to CTIF-CFI, and the external analyses performed by CTIF-CFI or the judicial authorities to determine whether there are serious indications of ML/FT.

The NBB expects financial institutions to **comply strictly** with this prohibition of disclosure in light of the objectives pursued by it. On the one hand, confidentiality of reportings of suspicious transactions is essential to enable the judicial authorities to apprehend and seize the assets of the perpetrators of the money laundering or terrorist financing offences. On the other hand, prohibiting the disclosure of information to third parties also aims to preserve the reputation of the persons concerned as long as no criminal sanction has been issued by the judicial authorities

as a result of these reportings of suspicions. Moreover, a violation of this confidentiality obligation with the aim of enabling the perpetrator of the money laundering or terrorist financing offence to avoid the consequences of a reporting that has been or will be submitted, could, depending on the circumstances, constitute an act of complicity in money laundering or terrorist financing.

In practice, the prohibition of disclosure implies that where an atypical transaction has been detected, it is preferable to avoid, as far as possible, contacting the customer concerned, in order to avoid any risk of unintentional disclosure; contact with the customer should be limited to cases where the analysis of the transaction actually requires such contact in order to form an opinion as to the possible existence of a suspicion and may in no case reveal that the additional information requested aims to determine whether a suspicion should be reported to CTIF-CFI.

In accordance with paragraph 2 of § 1 of Article 55, read in conjunction with Article 56, § 2, 2°, of the Anti-Money Laundering Law, the prohibition of disclosure also applies to the reporting of this information by Belgian financial institutions to their branches and subsidiaries established in a third country if no adequate measures have been taken to ensure that these branches or subsidiaries effectively apply a group policy in compliance with Directive 2015/849.

Given the importance of this prohibition of disclosure, the NBB expects financial institutions to specifically draw the attention of their managers and employees to the obligation to comply strictly with this prohibition and to limit access to this information to the persons who need it for the performance of their functions.

Furthermore, the NBB considers that if a financial institution finds that the prohibition of disclosure has been or might have been violated within the institution, it should examine the facts and their circumstances as quickly as possible in order to determine which proportionate and dissuasive measures should be taken against the person concerned. The NBB moreover expects these facts to be reported to itself and to CTIF-CFI without delay.

## 2. Exceptions

### 2.1. For competent authorities

In accordance with § 1 of Article 56 of the Anti-Money Laundering Law, the prohibition of disclosure does not apply to notifications from the financial institutions **to the NBB** in its capacity as competent supervisory authority, nor to disclosures **for law enforcement purposes**.

For instance, when exercising its supervisory powers both on- and off-site, the NBB is authorised to ask financial institutions to provide it in particular with the reports of the analyses of atypical facts and transactions and the accompanying documents, a copy of their reportings of suspicions to CTIF-CFI, the content of these reportings and their follow-up, notably the new individual risk assessment and the decision taken on this basis in accordance with Article 22 of the Anti-Money Laundering Regulation.

Likewise, the reporting entity may not invoke the confidentiality attached to the reporting of suspicions to the CTIF-CFI to refuse cooperation in criminal investigations that potentially result from the reporting of suspicions and pertain to the persons who are the subject of this reporting or to their transactions.

### 2.2. Information sharing within groups

Pursuant to Article 56, § 2, 1°, of the Anti-Money Laundering Law, financial institutions are authorised to share information covered by the prohibition of disclosure mentioned in § 1 with other financial institutions belonging to the same group, including the branches of these financial institutions, that are established on the territory of the European Economic Area.

On the basis of Article 56, § 2, 2°, of the Anti-Money Laundering Law, the same information may only be shared with financial institutions' branches or majority-owned subsidiaries that are located in third countries provided that those branches and subsidiaries fully comply with the group-wide policies and procedures, including procedures for sharing information within the group, in accordance with Article 45 of Directive 2015/849, and that the group-wide policies and procedures comply with the requirements laid down in this Directive.

These derogations from the prohibition on disclosing reportings of suspicious transactions aim to strengthen the effectiveness of the ML/FT prevention mechanisms within groups. The NBB therefore considers that financial institutions should make use of these derogations whenever that is useful and necessary for AML/CFT purposes to provide other entities belonging to the same group with relevant information on customers and their transactions, on

potential indications of ML/FT, on the analysis of atypical transactions or on reportings of suspicious transactions. Conversely, financial institutions should also make use of the communication channels provided for in their group policies to request equivalent information held by other entities of the group when this information could strengthen the effectiveness of the detection or analysis of atypical transactions and of the reporting of suspicious transactions to CTIF-CFI. However, these exchanges of information should comply with strict procedures which should notably limit access to this information to the persons whose AML/CFT tasks and functions justify access. In this respect, please also refer to the page “Retention and protection of data and documents”.

### 2.3. Information sharing with another financial institution not belonging to the same group

Article 56, § 2, 3°, of the Anti-Money Laundering Law authorises financial institutions to inform other financial institutions not belonging to the same group that a transaction carried out by a customer has been the subject of a reporting of suspicions to CTIF-CFI, when the financial institution receiving this information is involved in the same transaction with the same customer.

This authorisation is conditional upon the recipient being subject to equivalent AML/CFT legislation and only using the information for this sole purpose, on the one hand, and on the recipient being subject to equivalent obligations of professional secrecy and personal data protection, on the other.

As with the authorisation to exchange information within groups (see above), the main objective of this provision is to promote the effectiveness of AML/CFT. However, taking into account that the exchange of information is, in this case, not regulated by a single group policy, the NBB considers that it falls upon the financial institution reporting to CTIF-CFI a suspicious transaction involving another financial institution, to decide on a case-by-case basis whether it would be useful in light of the objectives pursued to inform this other financial institution thereof, and whether this institution is able to provide sufficient guarantees that it will comply with the conditions mentioned above. This decision falls within the competence of the AMLCO.

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



# Anti-Money Laundering Law of 18 September 2017 - Articles 55 and 56

## Art. 55

§ 1. Obligated entities, their directors, employees, agents and distributors, as well as the President of the bar association in the cases referred to in Article 52, shall not disclose to the customer concerned or to other third persons the fact that information is being, will be or has been transmitted to CTIF-CFI in accordance with Article 47, 48, 54 or 66, § 2, third subparagraph, or that a money laundering or terrorist financing analysis is being, or may be, carried out.

The prohibition referred to in the first subparagraph is also applicable to the communications of information or intelligence referred therein to branches of obliged entities established in third countries.

§ 2. When a natural person belonging to one of the categories of obliged entities referred to in Article 5, § 1, 23° to 28°, seeks to dissuade a client from engaging in illegal activity, that shall not constitute disclosure within the meaning of paragraph 1.

## Art. 56

§ 1. The prohibition referred to in Article 55 does not apply to the disclosure to supervisory authorities in accordance with Article 85, nor to disclosure for law enforcement purposes.

§ 2. The prohibition referred to in Article 55 shall not apply to disclosure of information:

1° between credit or financial institutions referred to in Article 2, paragraph 1, items 1 and 2, of Directive 215/849, established in a Member State when these institutions belong to the same group;

2° between the institutions referred to in 1°, their branches and majority-owned subsidiaries located in third countries, provided that those branches and majority-owned subsidiaries fully comply with the group-wide policies and procedures, including procedures for sharing information within the group, in accordance with Article 45 of Directive 2015/849, and that the group-wide policies and procedures comply with the requirements laid down in this Directive;

3° between the institutions referred to in 1° and between these institutions and equivalent institutions established in third countries whose requirements are equivalent to those laid down in Directive 2015/849 when these institutions act for the same customer and for the same transaction, provided that the information exchanged relates to that customer or that transaction, that it is used exclusively for the prevention of money laundering or terrorist financing, and that the institution receiving the information is subject to obligations equivalent to those laid down in Directive 2015/849 with regard to professional secrecy and personal data protection;

4° between the persons referred to in Article 2, paragraph 1, item 3, a) and b), of Directive 2015/849 or between these persons and persons carrying out the same profession in third countries which impose requirements equivalent to those laid down in Directive 2015/849:

a) who carry out their professional activities, whether as employees or not, within the same legal person or a larger structure to which the person belongs and which shares common ownership, management or compliance control.

b) when acting for the same customer and for the same transaction, provided that the information exchanged relates to that customer or that transaction, that it is used exclusively for the prevention of money laundering or terrorist financing, and that the recipient of the information is subject to requirements equivalent to those laid down in Directive 2015/849 with regard to professional secrecy and personal data protection.



# Explanatory Memorandum to the Anti-Money-Laundering Law of 18 September 2017 - Articles 55 and 56

## Art. 55

The draft Article closely mirrors the provisions concerning confidentiality of the report of suspicion as currently contained in Article 30, § 1, first paragraph of the Law of 11 January 1993, as well as the derogation from this prohibition as referred to in Article 30, § 1, second paragraph of the aforementioned Law in particular, and transposes Article 39, §§ 1 and 6 of Directive 2015/849 as well as FATF Recommendation 21, b).

The reference in the draft Article to the prohibition of letting the customer or third parties know that an analysis for money laundering or terrorist financing is underway or could be commenced, also covers internal analyses by the AMLCO of the obliged entity in order in particular to determine if a report should be filed with the CTIF-CFI, as well as the external analyses by the CTIF-CFI to determine if there are serious indications of ML/TF.

In the second paragraph of § 1 of the draft Article, it is stipulated that the prohibition of disclosure also applies to the communications of information or intelligence referred to for branches of entities established in third countries. The draft Article should be read along with Article 56, § 2, 2° of the draft Law which provides for an exception to the principle of prohibition where the branch or subsidiary in the third country effectively applies the group policy and it has been ensured that it is compliant with the Directive. Although with subsidiaries, § 1, first paragraph of the draft Article may be referred to because they have a separate legal personality to that of their parent company and are therefore third parties to it, this is not valid for branches as they do not have a separate legal personality to that of their 'parent company' and are therefore not legally third parties to it. Consequently, the prohibition of informing third parties does not apply between the parent company and the branch. For the exception to the prohibition of disclosure as provided for in Article 56, § 2, 2° of the draft Law to make sense, and submit communications between parent companies and branches of third countries to certain conditions, a prohibition in principle therefore needed to be provided for to be able to make an exception with conditions.

Where a notary, company auditor, auditor, external accountant, external tax consultant, registered accountant or registered tax accountant or even a lawyer makes an effort to dissuade a customer from taking part in an illegal activity, this is not disclosure within the meaning of the first paragraph of the draft Article.

## Art. 56

The draft Article closely follows the derogations from the prohibition of "tipping off" as contained in Article 30, §§ 2 and 3 of the Law of 11 January 1993 and transposes Article 39, §§ 2 to 5 of Directive 2015/849 as well as its Article 45, § 8.

In order to protect the reporting entity, it may neither reveal to the customer concerned nor to third parties that information and intelligence is being, will be or has been transmitted to the CTIF-CFI or that a money laundering or terrorist financing analysis is being or may be carried out.

The draft Article reconfirms that the prohibition does not apply to the communications addressed to the competent supervisory authorities or to disclosure for law enforcement purposes. This last exception confirms that the secrecy attached to the reporting of a suspicion transmitted to the CTIF-CFI may not be invoked by the reporting entity to refuse to cooperate with legal investigations, whether they arise from the reporting of the suspicion or not, and concerning the persons or their transactions to which this report refers.

Dispensing with the prohibition of “tipping off” from the third day of opposition by the CTIF-CFI as contained in Article 30, § 2 of the Law of 11 January 1993 is contrary to Article 39, § 1 of Directive 2015/849 and FATF Recommendation 21. This is why this is deleted from the draft Article.

Point 1° to 3° of § 2 of the draft Article refers to exceptions to the prohibition of disclosure that apply between credit institutions and financial institutions that belong to the same group, whose branches and subsidiaries are mainly located in third countries, and between these establishments when they do not belong to the same group.

Point 4°, a) of § 2 of the draft Article refers to lawyers, notaries, company auditors, auditors and audit firms, external chartered accountants, external tax consultants, registered external accountants and registered tax accountants governed by the European Union or a third country who carry out their professional activities, whether as employees or not, within the same legal person or a larger structure to which the person belongs and which shares common ownership, management or compliance control. In this way, it is possible for these professionals who carry out their activities within a cross-border structure to share information on the reports they have made to their national FIU.

Point 4°, b) of § 2 of the draft Article refers to lawyers, notaries, company auditors, auditors and audit firms, external chartered accountants, external tax consultants, registered external accountants and registered tax accountants governed by the European Union or located in a third country without belonging to the same larger structure and where they intervene concerning the same customer and the same transaction. In this way, as was the case in the past, it is possible for example for a notary and for a lawyer intervening in the same transaction and for the same customer to share information about the declaration that one of them has made to the FIU. If the information must be shared with a person established in country outside the EEA, it must fulfil requirements and have supervision equivalent to that required by Directive 2015/849.



# Protection of reporting entities

Home > Financial oversight > Combating money laundering and the financing of terrori...

## Legal and regulatory framework

- Anti-Money Laundering Law: Articles 57 to 59

## Explanatory Memorandum of the Anti-Money Laundering Law

- Articles 57 to 59

## Other reference documents

- CTIF-CFI's information note of 26 October 2017 regarding the disclosure of information to CTIF-CFI

## Comments and recommendations by the NBB

### 1. Protection of and exemption from liability for reporting entities

Article 57 of the Anti-Money Laundering Law provides on the one hand that the disclosure of information in good faith to CTIF-CFI shall not constitute a breach of any restriction on disclosure of information imposed by contract and shall not lead to any adverse or discriminatory employment action. On the other hand, immunity remains intact even if the reporting entity was not precisely and clearly aware of the predicate criminal activity, and even if it appears a posteriori that no illegal activity is related to the transaction that was reported to CTIF-CFI.

Thus, for example, if a financial institution suspected or had reasonable grounds to suspect that the funds are of illicit origin, which may involve tax fraud, it may not be held liable by the customer for not having determined previously that it concerned a case of serious fiscal fraud.

It should be specified however that the reporting must be considered to have been made in good faith. This means that the reporting may not have been carried out with the intention of harming the customer and that it may not be based on information that the entity knew was incorrect. Good faith also implies that the obliged entity has not committed any manifest breach of the obligation of careful examination provided for in Article 35, § 1, 1° of the Anti-Money Laundering Law, or of its obligation to analyse atypical transactions, in accordance with Article 45, § 1 of that Law. Good faith implies, in particular, that it cannot be considered that the reporting financial institution should have known or, in any case, could not have been unaware that the transactions for which suspicions were reported, were not related to money laundering or terrorist financing. This presupposes that, in their examination of the transaction

concerned, the AMLCOs of the financial institutions take appropriate account of all relevant information relating to the customer, the business relationship and the transaction held by the financial institution. See in this regard the page “Analysis of atypical facts and transactions”.

## 2. Anonymity of reporting entities

Article 58 of the Anti-Money Laundering Law aims to protect the reporting entities against threats or hostile actions. Thus, it is legally prohibited for the Public Prosecutors, investigating judges, foreign services that are counterparts of CTIF-CFI, OLAF, the Prosecutor at a labour tribunal, SIRS-SIOD, the Minister of Finance, State Security Service, the General Intelligence and Security Service of the Armed Forces and OCAM-OCAD to obtain a copy of the suspicious transaction reports, even when CTIF-CFI provides them with information.

In practice, when CTIF-CFI receives information, it cross-references it with information transmitted or requested from the authorities, institutions and obliged entities that the law allows it to question. Consequently, if the file is transmitted to the Public Prosecutor's Office or to the authorities mentioned above, it is based on multiple sources of information without the original reporting itself being included. When the members of CTIF-CFI or members of its staff, members of the police services and other officials seconded to CTIF-CFI, or external experts it calls upon, are summoned to testify in court, they are also not authorised to disclose the identity of the authors of the suspicious transaction reports.

In addition, the anonymity of AMLCOs who report suspicious transaction and of the financial institutions that employ them is further strengthened by Article 59 of the Anti-Money Laundering Law, which provides that the supervisory authorities competent for investigations and prosecutions, such as CTIF-CFI or the Public Prosecutor's Offices, shall take specific measures to ensure that the AMLCOs are not exposed to possible threats or hostile actions. Please refer to the Explanatory Memorandum of the Anti-Money Laundering Law for more information on this subject.

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



# Anti-Money Laundering Law of 18 September 2017 - Articles 57 to 59

## Art. 57

Disclosure of information in good faith to CTIF-CFI by an obliged entity or by one of its directors, members of staff, agents or distributors, or by the President of the bar association referred to in Article 52 shall not constitute a breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, and shall not involve the obliged entity or its directors, members of staff, agents or distributors, in liability of any kind, either civil, criminal or disciplinary, nor any adverse or discriminatory employment action, even in circumstances where they were not precisely aware of the predicate criminal activity, and regardless of whether any illegal activity actually occurred.

## Art. 58

Where CTIF-CFI forwards information to the Public Prosecutor, the Federal Public Prosecutor or the authorities referred to in Article 83, § 2, this does not include the disclosures received from obliged entities in accordance with Article 47, 54 and 66, § 2, third subparagraph, in order to preserve the anonymity of its authors.

If the persons referred to in Article 83, § 1, are summoned to testify in court, they are also prohibited from disclosing the identity of the authors referred to in the first subparagraph.

## Art. 59

The competent authorities for investigating and prosecuting money laundering and terrorist financing shall take all appropriate measures to protect directors, members of staff, agents or distributors of obliged entities who report suspicions of money laundering or terrorist financing, either internally, or to CTIF-CFI from being exposed to threats or hostile action.



# Explanatory Memorandum to the Anti-Money-Laundering Law of 18 September 2017 - Articles 57 to 59

## Art. 57

The draft Article transposes Article 37 of Directive 2015/849 as regards the protection of reporting entities when they disclose reports to the CTIF-CFI in good faith. The draft Article also takes into account FATF Recommendation 20. The draft Article reinforces the content of the protection in the former Article 32 of the Law of 11 January 1993 by expressly specifying that disclosure of information in good faith to the CTIF-CFI does not constitute a breach of any contractual restriction to the disclosure of information and that this report may not entail any adverse or discriminatory employment action (Article 37 of Directive 2015/849). Such immunity remains intact even in a situation in which the reporting entities did not have exact knowledge of the predicate criminal activity regardless of whether any illegal activity actually occurred (FATF Recommendation 20). As a result, for example, where an obliged entity had reasons to suspect that funds were of illicit origin, this origin potentially consisting of tax fraud, its responsibility may not be claimed by the customer because of the fact that it had not previously established that there was a case of serious tax fraud. In this respect, it is also specified that the report must be considered in good faith as long as it is not done with the aim of harming the customer and is not based on information that the entity knows is erroneous. Good faith furthermore implies that the obliged entity did not commit any manifest breach of the obligation of careful examination provided for by draft Article 35, § 1, and that it may not be considered that it should have known or in any case could not ignore that the transactions referred to in the report of suspicion were not linked to money laundering or terrorist financing. This, in particular, assumes that in its examination of the transaction concerned, the obliged entity appropriately takes into account all the pertinent information in its possession regarding the customer, the business relationship and the transaction.

This once again confirms that it is not up to the reporting entity to identify the criminal activity underlying its suspicion of money laundering. It suffices for the reporting entity to have the slightest suspicion that the funds it is to handle for the business relationship or the execution of the occasional transaction are of illicit origin for its duty of reporting to the CTIF-CFI to be triggered.

It is up to the CTIF-CFI, using an in-depth analysis, to make the link between the suspicion of money laundering and the criminal activity.

The protection of employees and representatives of the obliged entity who internally alert of a suspicion of money laundering or terrorist financing (cf. Article 38 of the Directive) is covered in draft Article 36.

## Art. 58

The draft Article takes over the content of Article 36 of the Law of 11 January 1993 to protect the anonymity of obliged entities that have reported suspicions and also, as required under Article 38 of Directive 2015/849, to protect reporting entities of any threat or any hostile act.

In other words, Public Prosecutors, examining magistrates, foreign departments equivalent to the CTIF-CFI, OLAF, the labour auditor, the Social Information and Investigation Service, the Minister of Finance, the State Security Service, the Belgian General Information and Security Service, or the Coordination Unit for Threat Analysis are not legally permitted to obtain a copy of the reports of suspicions even if the CTIF-CFI shares information. In practice, when the CTIF-CFI receives information, it is cross-referenced with the information sent or requested from the

bodies and obliged entities that the law allows it to question. This culminates in the communication that may be made to the public prosecutor's office or the authorities mentioned above being based on multiple sources without copying the original report itself.

When the members of the CTIF-CFI, its employees, the police force and other officers contracted thereby as well as the external expert they call upon, are summoned to act as a witness in court, they are also not authorised to reveal the identity of the author of the reports.

## Art. 59

The draft Article seeks to closely mirror the content of Article 30, § 4 of the Law of 11 January 1993 which transposed Article 27 of Directive 2005/60/EC of 26 October 2005 and transposes Article 38 of Directive 2015/849 as regards the protection of reporting entities from any threat or any hostile act.

This paragraph emphasises the responsibility in terms of competent authorities as regards investigations and prosecutions relating to ML/TF.

At the beginning of its activity, the CTIF-CFI was conscious of the physical risk that the legal obligation of obliged entities to communicate facts or suspicions of money laundering entailed for the employees of these institutions. This is why measures have already been taken both as regards the existing preventive legislation and the practical operational methods of the CTIF-CFI. Even though the draft Law still aims to reinforce the protection measures, the Law of 11 January 1993 already contained provisions which contributed to placing some distance between the natural person who detects suspicious transactions and the transmission of a written report to the CTIF-CFI.

In this way, the Law structures an internal process within the obliged entities concerned for examining contentious transactions by providing for the designation of persons responsible for the application of the Law as well as for writing and sending written reports to these responsible persons, the AMLCOs.

The Law of 11 January 1993 already provided for the information to be transmitted to the CTIF-CFI by the said responsible persons designated within the companies concerned.

Other provisions of the Law of 11 January 1993, while aiming for efficiency, also contributed to reinforcing the protection of the sources of information. This refers to the prohibition of disclosing to the customer concerned or third parties that the information has been sent to the CTIF-CFI or that an investigation into money laundering is underway.

However, it is clear that the professional secrecy subject to criminal sanctions (Article 458 of the Criminal Code) imposed by the Law to the members of the CTIF-CFI as well as to its members of staff (including the police force, other contracted officers and external experts) contributes to this protection of reporting entities sought by law.

As a consequence, the CTIF-CFI has already adopted in its operational practice a series of measures aiming not to expose natural persons and the institutions that employ them to potential threats or hostile action.

These measures are the following:

- For each dossier sent, the CTIF-CFI draws up a report to the judicial authorities (Crown Prosecutor or Federal Prosecutor), containing all the information received, gathered and analysed, whether these originate from reports of suspicions or any other legal source. This report never specifies the information received expressly following reports of suspicion. This information, whether it is at the origin of the dossier or subsequent thereto is never attached to these transmission reports. All the information is therefore included in a report that the CTIF-CFI is responsible for.
- The reports of transmission to the CTIF-CFI only contain the address of the department of the reporting entity concerned in order to allow the judicial authorities to supplement the information necessary for the investigation if necessary. For this purpose, the AMLCO constitutes an essential bridge between the reporting entity's staff and the Crown Prosecutor or the Federal Prosecutor.
- The information from reports of suspicions made by other professions (lawyers, notaries, auditors, chartered accountants, etc.) are, as explained above, included in the CTIF-CFI report, which as much as possible avoids identifying the source of the reports of suspicions as such. Where applicable, a separate and

confidential email containing certain sensitive information relating to this type of report is addressed to the Crown Prosecutor or the Federal Prosecutor at the same time as transmitting the report.

When the members of the CTIF-CFI, its employees, the police force and other officers contracted thereby as well as the external experts they call upon are summoned to act as a witness in court, they are also not authorised to reveal the identity of the author of the reports of suspicions.

From a law-enforcement aspect, the CTIF-CFI has also contributed to applying the law on the anonymity of witnesses who report suspicions to the CTIF-CFI and who may choose their work address as their elected domicile.

Although the provisions of the Law of 8 April 2002 on the anonymity of witnesses (Belgian Official Gazette, 31 May 2002) already fulfil this objective as regards the examining magistrate or the trier of fact (Articles *75bis*, *75ter* and *86bis* to *86quinquies* of the Code of Criminal Procedure), account should also be taken of similar protective measures where the reporting entities or their employees are interrogated as witnesses by the police after a referral by the CTIF-CFI to the judicial authorities. The aim of this provision is also to provide for confidentiality as a rule for situations in which this intelligence is not covered by the CTIF-CFI's professional secrecy. Services that ultimately handle the information are expected to put in place, if possible, provisions that do not compromise the anonymity of reporting entities.

In parallel, the CTIF-CFI has raised awareness among the justice system via the College of Crown Prosecutors and the network of legal experts in financial matters. This initiative culminated in a circular of 6 January 2009 that the Crown Prosecutor of Brussels addressed to various police forces in the district.

This is a specific measure relating to the protection of reporting entities emphasising the fact that under no circumstances whatsoever may police officers communicate to persons concerned by a legal dossier information that enables them to expressly or implicitly identify the institution or obliged entity from which a report of suspicion to the CTIF-CFI originates and/or who has contributed thereto.

Furthermore, the principle of evaluating interests and whether or not it is necessary to proceed with a hearing of the employees of the reporting professions is recalled, considering that the preventive system put in place pursues judicial aims. In this case, the absolute usefulness precisely of hearing the employees from whom the detection originates should be evaluated and in the affirmative, of hearing the AMLCO of the institutions as a priority. In all cases, the measures provided for by the law on the anonymity of witnesses should be extended by analogy to these hearings.



# Transfers of funds

Home > Financial oversight > Combating money laundering and the financing of terrori...

## Legal and regulatory framework

- Regulation (EU) 2015/847 of 20 May 2015 on information accompanying transfers of funds
- Anti-Money Laundering Regulation of the NBB: Article 23

## Other reference documents

- ESAs Joint Guidelines of 16 January 2018 under Article 25 of Regulation (EU) 2015/847 on the measures payment service providers should take to detect missing or incomplete information on the payer or the payee, and the procedures they should put in place to manage a transfer of funds lacking the required information

## Comments and recommendations by the NBB

- Comments and recommendations

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



# NBB anti-money laundering regulation of 21 November 2017 - Article 23

## Art. 23

Obligated financial institutions shall set up monitoring systems to monitor compliance with:

- 1° the provisions of the European Regulation on transfers of funds;
- 2° binding provisions concerning financial embargoes.

These monitoring systems must:

- 1° cover all customers' accounts and contracts and all their transactions;
- 2° allow rapid detection of any infringements of the provisions referred to in the first paragraph or detection in real time whenever these provisions require it;
- 3° be automated, unless the obliged financial institution can demonstrate that the nature, number and volume of transactions to be monitored do not require it;
- 4° be subject to an initial validation procedure and a regular review.



# Transfers of funds: Comments and recommendations by the NBB

Home > Financial oversight > Combating money laundering and the financing of terrori...

## Contents

- 1. European regulations on transfers of funds
- 2. Obligation to have a monitoring system
- 3. Internal policy and procedures with regard to transfers of funds
- 4. Internal control measures

## 1. European regulations on transfers of funds

The purpose of the European regulations on transfers of funds is to prevent payment systems from being used to launder money or finance terrorism.

### 1.1. Regulation 2015/847

Transfers of funds are governed by Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds (hereinafter "Regulation 2015/847"), which repealed the former Regulation (EC) 1781/2006. The purpose of this Regulation 2015/847 is to ensure the traceability of payments and to specify the obligations of the various payment service providers involved in transfers of funds..

More specifically, Regulation 2015/847 lays down rules with regard to the information on payers and payees that must accompany transfers of funds, in any currency, where at least one of the payment service providers involved in the transfer of funds is established in the European Union.

It lays down the obligations of financial institutions where they act as:

- a. the payment service provider ("PSP") of the payer;
- b. the PSP of the payee; and
- c. the intermediate PSP involved in the execution of a transfer of funds ("IPSP").

### 1.2. ESAs guidelines

Regulation 2015/847 has been supplemented by the ESAs Joint Guidelines on the measures payment service providers should take with regard to transfers of funds they receive to detect missing or incomplete information on the payer or the payee, and the procedures they should put in place to manage a transfer of funds lacking the required information.

Point 1(a) of these guidelines specifies that the guidelines apply to:

- a. financial institutions in their capacity as PSPs, as defined in Article 3(5) of Regulation 2015/847, where they act as the PSP of the payee; and
- b. financial institutions in their capacity as IPSPs, as defined in Article 3(6) of Regulation 2015/847.

The NBB therefore recommends that financial institutions acting as the PSP of the payee and/or as IPSP as referred

to above, give full consideration to the above-mentioned ESAs joint guidelines, in particular in determining:

- the factors that should be considered when establishing and implementing procedures to detect and manage transfers of funds that lack required information on the payer and/or the payee; and
- the measures they should take to manage the ML/FT risk where the required information on the payer and/or the payee is missing or incomplete.

However, the NBB notes that the general considerations set out in points 8 to 20 of these guidelines are also relevant for financial institutions in their capacity as PSPs of payers. It therefore expects financial institutions to also take full account of these general considerations when defining and implementing their policies, procedures and internal control measures relating to their activities in their capacity as PSPs of payers.

## 2. Obligation to have a monitoring system

In accordance with Article 23 of the Anti-Money Laundering Regulation of the NBB, financial institutions should set up a monitoring system to monitor compliance with the provisions of Regulation 2015/847.

More specifically, the purpose of this monitoring system is to ensure that all transfers of funds received by financial institutions in their capacity as IPSPs or PSPs of payees systematically carry complete information on the payer and the payee, as required under Regulation 2015/847.

### 2.1. Scope of the obligation to have a monitoring system

The obligation to have a monitoring system for transfers of funds applies to financial institutions providing payment services (in particular in their capacity as PSP of the payee or as IPSP).

### 2.2. Expectations of the NBB regarding the monitoring system

On the one hand, the NBB expects financial institutions where they act as the PSP of the payer to implement effective internal control mechanisms to ensure that all transfers of funds in which they are involved in that capacity systematically carry information on the payer and the payee, in accordance with Articles 4 to 6 of Regulation 2015/847. The NBB expects financial institutions to reject a transfer of funds where the required information is missing or incomplete.

On the other hand, where the financial institution acts as IPSP or as PSP of the payee, the Anti-Money Laundering Regulation of the NBB provides that the system for monitoring transfers of funds received should:

- i. cover all customers' accounts and contracts and all their transactions;
- ii. allow rapid detection of any infringements of the provisions of Regulation 2015/847;
- iii. be automated, unless the obliged financial institution can demonstrate that the nature, number and volume of transactions to be monitored do not require it; and
- iv. be subject to an initial validation procedure and a regular review.

The NBB expects this monitoring system to allow financial institutions to effectively carry out all the controls described in the above-mentioned ESAs joint guidelines, under the conditions specified therein, so that an alert is generated where transfers of funds received do not carry all the information required in accordance with Regulation 2015/847, enabling the financial institution to implement the required measures to manage transfers of funds where the information is missing or incomplete or has been provided using inadmissible characters or inputs.

### 2.3. Management of alerts generated by the monitoring system

The NBB considers that the proper management, in accordance with Regulation 2015/847 and the above-mentioned joint guidelines, of the alerts generated by the monitoring system referred to above is the responsibility of the AMLCO.

For the sake of efficiency, the financial institution's internal procedures may instruct its operational services to conduct a preliminary analysis of the alerts generated by the system for monitoring transfers of funds to ensure that they are apparently relevant. Where this preliminary analysis does not support the conclusion that the alerts are false, the transactions concerned must be referred to the AMLCO, in order for him to determine the measures for managing such alerts that should be taken in accordance with Regulation 2015/847, the ESAs joint guidelines and the internal procedures.

In addition, the AMLCO should, under his responsibility, put in place a process to analyse, as quickly as possible, alerts generated by the systems for monitoring transfers of funds, in order to determine, in accordance with Articles 9 and 13 of Regulation 2015/847, whether or not there are any suspicions of ML/FT. For more information about this analysis process, see the web pages « Analysis of atypical transactions » and « Reporting of suspicions ». In this respect, see also points 44 to 46 of the ESAs joint guidelines on this subject.

In general, the NBB also recommends that financial institutions ensure that, in accordance with Regulation 2015/847, all decisions and follow-up actions taken (and the reasons behind the decisions taken) are documented.

## 3. Internal policy and procedures with regard to transfers of funds

### 3.1. Integration of aspects relating to transfers of funds into the financial institution's AML/CFTP policy

The NBB expects all financial institutions to set out, in their AML/CFTP policy established pursuant to Article 8 of the Anti-Money Laundering Law, their strategy regarding:

- a. compliance with the obligations relating to the information accompanying transfers of funds executed on behalf of their customers in their capacity as payers;
- b. the management of transfers of funds received by a financial institution in its capacity as IPSP or PSP of a payee, where the required information is missing or incomplete or has been provided using inadmissible characters or input; and
- c. the measures to be taken with regard to PSPs or IPSPs that **repeatedly fail to provide the required information**.

In accordance with the principle of proportionality, the above policy should be more detailed in financial institutions that specialise in payment services.

### 3.2. Establishment of a procedure for monitoring transfers of funds

As indicated on the web page "Policies, procedures, processes and internal control measures", all financial institutions that execute transfers of funds should put in place a procedure for monitoring transfers of funds, taking into account in particular the above-mentioned joint guidelines of the ESAs.

This procedure should include the following:

- the internal control measures implemented to ensure that the transfers of funds executed on behalf of their customers in their capacity as payers carry all the information required;
- the criteria and process to identify transfers of funds received by a financial institution in its capacity as PSP of the payee or as IPSP that should be subject to real-time monitoring and those that may be monitored ex post;
- the analysis, decision and management process for the measures to be taken in accordance with Articles 7 and 8(1) of Regulation 2015/847 and the aforementioned joint guidelines, where the financial institution acts as the PSP of the payee, and Articles 11 and 12(1), where

- the financial institution acts as IPSP, where its system for monitoring transactions detects a transfer of funds received lacking the required complete information on the payer and the payee; the NBB expects these financial institutions to set up an operational system enabling them to immediately reject the said transfer of funds if necessary;
- the process to detect payment service providers of payers or intermediaries involved in transfers of funds who repeatedly fail to provide the required information on the payer or payee, and the process to decide on the measures to be taken in this case in accordance with Articles 8(2) and 12(2) of Regulation 2015/847; the process to submit transfers of funds received lacking the required information to the AMLCO for examination, in accordance with Articles 9 and 13 of Regulation 2015/847, in order for him to determine if there are any suspicions of ML/FT; see also the web page “Reporting of suspicions”.

If the financial institution concerned specialises in payment services, its procedure for transfers of funds should be more detailed, while remaining proportionate to the nature, size and complexity of its activities and ML/FT risks.

### 3.3. Record retention process

Regulation 2015/847 provides that information that allows to precisely identify the payer and the payee should be retained for a period of five years, which may be extended in certain circumstances, in order to be able to respond later to any requests from the competent authorities. In this context, the NBB expects financial institutions to take the necessary measures to comply with the record retention requirements of Regulation 2015/847, while complying with the legislation on the processing of personal data.

Furthermore, it should be noted that Article 60 of the Anti-Money Laundering Law imposes a retention period of ten years from the end of the business relationship with the customer or the date of execution of the occasional transaction, for the identification data of customers, agents and beneficial owners, where appropriate updated in accordance with Article 35 of the Anti-Money Laundering Law, as well as for the copy of the supporting documents or of the result of consulting an information source. By complying with the ten-year period provided for in the Anti-Money Laundering Law, the obligation set out in the European Regulation on transfers of funds to retain information on the payer and payee for a period of five years is automatically met.

## 4. Internal control measures

Financial institutions are expected to monitor periodically and on an ongoing basis that their transfers of funds policy and procedures are properly complied with and that the processes for implementing the organisational and operational obligations set out above are adequate.

With regard to the system for monitoring transfers of funds, the NBB recommends that the internal audit function pay particular attention to:

- the effectiveness of the monitoring system, taking into account in particular the number of alerts generated;
- the effectiveness of the process for analysing alerts generated by the system, taking into account the number of cases of information being reported to the AMLCO and the number of suspicious transaction reports related to a transfer of funds issue;
- the adequacy of the human and technical resources made available to the operational services responsible for analysing the alerts generated by the monitoring system for transfers of funds and to the AMLCO.

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



# Financial embargoes and assets freezing

Home > Financial oversight > Combating money laundering and the financing of terrori...

## Legal and regulatory framework

- Anti-Money Laundering Regulation of the NBB: Article 23

## Other reference documents

- FATF Guidance dated 28 February 2018 on counter proliferation financing
- See the relevant financial sanctions on the Treasury's website

## Comments and recommendations by the NBB

- 6 December 2016 - Horizontal letter: application of financial sanctions regime (Combating the financing of terrorism and of the proliferation of weapons of mass destruction)
- Comments and recommendations

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



# NBB anti-money laundering regulation of 21 November 2017 - Article 23

## Art. 23

Obligated financial institutions shall set up monitoring systems to monitor compliance with:

- 1° the provisions of the European Regulation on transfers of funds;
- 2° binding provisions concerning financial embargoes.

These monitoring systems must:

- 1° cover all customers' accounts and contracts and all their transactions;
- 2° allow rapid detection of any infringements of the provisions referred to in the first paragraph or detection in real time whenever these provisions require it;
- 3° be automated, unless the obliged financial institution can demonstrate that the nature, number and volume of transactions to be monitored do not require it;
- 4° be subject to an initial validation procedure and a regular review.

# Financial embargoes and assets freezing: Comments and recommendations by the NBB

Home > Financial oversight > Combating money laundering and the financing of terrori...

## Contents

- 1. Context
- 2. Overview of the different financial embargo and assets freezing mechanisms to be complied with
- 3. Obligation to have a monitoring system
- 4. Other organisational and operational measures to be taken
- 5. Practical implementation of freezing measures
- 6. Internal control measures

---

Financial institutions are subject to certain obligations regarding financial embargoes and assets freezing. This web page sets out (i) the context of financial embargoes and assets freezing measures, (ii) the different financial embargo and assets freezing mechanisms that financial institutions must comply with, (iii) the obligation to have a monitoring system, (iv) the other organisational and operational measures that financial institutions must take with regard to financial embargoes and assets freezes, (v) the practical implementation of freezing measures and the consequences thereof, in particular the obligation to report to the FPS Finance - Treasury Department and (vi) the internal control measures recommended by the NBB in this area.

Non-life insurance companies' attention is drawn to the fact that the obligations regarding embargoes and asset freezing apply to any natural and legal person regardless of the scope *ratione personae* of the Anti-Money Laundering Law. Some of the measures included on this web page are thus also applicable to non-life insurance companies.

## 1. Context

Embargo and assets freezing measures are taken as part of financial sanctions regimes. Financial sanctions are restrictive measures taken against governments of third countries, natural persons, legal persons or *de facto* groups, in order to put an end to certain criminal behaviour.

A financial sanctions regime is an instrument used by international or European institutions or the Belgian government for various purposes, including foreign policy, the fight against terrorism and its financing or the fight against the proliferation of weapons of mass destruction.

Although financial institutions must comply with all financial sanctions, this web page focuses mainly on financial embargoes and assets freezing measures related to the fight against terrorism and its financing, and to the fight against the proliferation of weapons of mass destruction. For the specific due diligence obligations relating to the fight against the proliferation of weapons of mass destruction, see the page "Ongoing due diligence and detection of atypical facts and transactions", where it is recalled that transactions that could be related to the proliferation of weapons of mass destruction should also be considered atypical because of the intrinsic characteristics of these transactions or of the persons acting as customers, agents, beneficial owners or counterparties in these transactions, in particular because of their links with the countries concerned or with persons or entities known to be involved in the proliferation of weapons of mass destruction.

The term "financial embargo" is generally understood to mean a restrictive measure or a sanction taken against a country at the national and/or international level for various reasons, as explained above. The term "assets freeze" refers to a temporary restriction of the right of ownership of a natural or legal person in the context of the fight against terrorism or the proliferation of weapons of mass destruction.

**Embargo and assets freezing measures must be implemented by financial institutions as soon as they enter into force. They create an obligation of result on their part.** Unlike other provisions of the Anti-Money Laundering Law, the application of embargo and assets freezing measures is not subject to a risk-based approach.

Attention is also drawn to the fact that violations of embargoes and assets freezes may give rise to **criminal sanctions** and that the Law of 13 May 2003 relating to the implementation of restrictive measures adopted by the Council of the European Union against some states, persons and entities also provides for sanctions in case of infringements of European regulations and decisions. . Since the entry into force of the Law of 2 May 2019 containing various financial provisions, the General Treasury Administration of the FPS Finance is competent to identify and record any infringements of financial restrictive measures. While the identification of such infringements does not fall within the NBB's legal competence, it is nevertheless incumbent on it, as the supervisory authority designated by the Anti-Money Laundering Law, to ensure that the financial institutions within its competence have developed and implement policies, procedures and internal control measures that are efficient and commensurate with their nature and size, in order to comply with the mandatory provisions on financial embargoes, as required by Article 8 § 1, 3°, of the Anti-Money Laundering Law (see point 3 below).

## 2. Overview of the different financial embargo and assets freezing mechanisms to be complied with

International organisations and authorities such as the United Nations and the European Union, and national authorities may impose restrictive measures on countries, organisations, legal persons or natural persons involved in or suspected of violating human rights or international law, criminal acts, terrorism, money laundering, etc.

Financial institutions must comply with the financial embargoes and assets freezing measures imposed by (i) the United Nations (provided that the resolutions concerned have been declared enforceable in Belgium), (ii) the European Union and (iii) the Belgian legislator.

### 2.1. The United Nations Security Council Resolutions

Pursuant to Chapter VII of the Charter of the United Nations (peacekeeping missions), the United Nations Security Council (hereinafter referred to as UNSC) may adopt resolutions in the event of any threat to the peace, breach of the peace, or act of aggression, in order to provide for financial embargo or assets freezing measures.

The UNSC resolutions on sanctions are transposed into European law by the European Union and are thus directly applicable in Belgium. **Since the entry into force of the above-mentioned Law of 2 May 2019, the freezing measures provided for by the UNSC resolutions must be implemented immediately in Belgium, without their first having to be confirmed by ministerial order (as was previously the case) or a European regulation** (see point 2.2. below). The Minister of Finance also issues a ministerial decree to require the persons subject to the Anti-Money Laundering Law to implement the UNSC freezing measures "without delay".

The adoption of a UNSC resolution is published on the United Nations website. Such resolutions are also published on the Treasury's website. Financial institutions are therefore encouraged to regularly consult the list of relevant UNSC resolutions on the Treasury's website.

### 2.2. The European regulations on restrictive measures

In the context of the Common Foreign and Security Policy, the European Union adopts European regulations:

- to transpose into European law the UNSC resolutions setting out financial embargo and assets freezing measures to be imposed; and
- to impose freezing measures autonomously, independently of any action taken by the United Nations.

These European sanctions are directly applicable in Belgium. For the consolidated list of the European sanctions, see the Treasury's website (which refers to the European Commission's website).

## 2.3. National list of persons or entities subject to freezing measures

UN Security Council Resolution 1373(2001) calls on all countries to freeze the funds and economic resources of persons and entities who commit or attempt to commit terrorist offences or who participate in or facilitate the commission of terrorist offences. In addition to Regulations 2580/2001 and 881/2002 and Common Position 2001/931/CFSP, Belgium has taken steps to draw up a national list.

In this respect, a consolidated national list of persons and entities whose assets or economic resources have been frozen in the context of AML/CFT has been drawn up pursuant to the Royal Decree of 28 December 2006 relating to specific restrictive measures against certain persons and entities within the framework of the fight against terrorism financing, ratified by Article 155 of the Law of 25 April 2007 containing various provisions. This Royal Decree requires all funds and economic resources of the persons and entities included in this national list to be frozen and prohibits funds or economic resources to be made available, directly or indirectly, to such persons or entities.

This national list is available on the Treasury's website.

## 2.4. Derogations granted by the Treasury

The General Administration of the Treasury may grant exemptions from financial sanctions upon request. For more information on this subject, see the Treasury's website.

# 3. Obligation to have a monitoring system

Pursuant to Article 8, § 1, 3°, the obliged entities should develop and implement policies, procedures and internal control measures that are efficient and commensurate with their nature and size in order to comply with the mandatory provisions on financial embargoes.

In accordance with Article 23 of the Anti-Money Laundering Regulation of the NBB, financial institutions should set up a monitoring system to monitor compliance with the binding provisions concerning financial embargoes and assets freezes.

## 3.1. Expectations of the NBB regarding the monitoring system

The monitoring system must screen customer databases and transactions involving the receipt or provision of funds, financial instruments or economic resources, to detect whether a customer or the beneficial owner of one of the above-mentioned transactions is subject to an assets freezing measure.

Pursuant to Article 23 of the Anti-Money Laundering Regulation of the NBB, this monitoring system should:

- i. cover all customers' accounts and contracts and all their transactions;
- ii. allow rapid detection of any infringements of the provisions on embargoes and freezing of assets or detection in real time whenever these provisions require it;
- iii. be automated, unless the financial institution can demonstrate that the nature, number and volume of transactions to be monitored do not require it; and
- iv. be subject to an initial validation procedure and a regular review.

The NBB also draws the attention of the financial institutions to the following:

### 3.1.1 Freeze lists to be taken into account

The monitoring system should take into account all the financial embargo and freezing mechanisms described in point 2 above. The list used by the monitoring system should therefore be updated very regularly and whenever a new person or entity is added in accordance with the rules laid down in the procedure for monitoring transactions with a view to complying with financial embargo and assets freezing obligations. The AMLCO must therefore provide

for a legal follow-up to monitor changes to the lists of financial embargoes and assets freezes. If the financial institution has branches abroad, these branches should comply with the local regulations on assets freezing. In that case, the group's parent company may also take into account the freeze lists of countries with which it has a branch-type link.

### 3.1.2. Setting up of the monitoring system

The monitoring system should make it possible to detect:

- on the one hand, customers, agents and beneficial owners whose identification data are identical to the available identification details, including aliases, of a person or entity that appears on an official list of sanctions applicable in Belgium; and
- on the other hand, the counterparties of financial transactions carried out by a customer or an agent whose surname, first name or alias or company name are identical to the data included in an official list of sanctions applicable in Belgium.

The NBB therefore recommends that financial institutions avoid basing their monitoring system on an exact match type reconciliation function and that they should determine what they deem to be a reasonable level of similarity. As an indication, it is noted that in practice, the most frequently used level of similarity is 85%.

### 3.1.3. Scope of the monitoring system

The screening mechanisms of the monitoring system should make it possible to detect funds, financial instruments and economic resources that:

- belong to or are owned by a listed person or entity;
- are held or controlled by a listed person or entity;
- are made available, directly or indirectly, to a listed person or entity.

### 3.1.4. Frequency of the screening

Financial institutions should carry out a screening before entering into a business relationship and before carrying out an occasional transaction, as well as when carrying out transactions involving third parties, such as, in particular, transfers of funds to third parties ordered by their customers or the receipt of transfers of funds executed by a third party on behalf of their customers.

Financial institutions should also recheck their customer databases when new persons or entities are added to the existing assets freeze lists.

## 3.2. Analysis of alerts generated by the monitoring system

The purpose of the analysis of the alerts is to determine whether the person or entity detected by the monitoring system is the person who is subject to a freezing measure or a homonym of that person.

There is homonymy when:

- the spelling of the surname and first name or alias or corporate name is identical to that of the listed person or entity, including where the surname is not distinguishable from the first name;
- the spelling of the surname and first name or alias or corporate name differs from that of the listed person, due in particular to different transcriptions from the same foreign alphabet, but sounds similar.

### 3.2.1. Role of the AMLCO

The AMLCO should, under its responsibility, put in place a process to analyse, as quickly as possible, alerts generated by the monitoring system. To this end, one or more persons from the AMLCO team should be appointed to carry out this task. If necessary, in case the AMLCO works alone, this function may be delegated to an AMLCO correspondent in an operational department, who will work under the responsibility of the AMLCO. The NBB insists that, where this possibility is availed of, the AMLCO remains fully responsible for all tasks related to the analysis of alerts generated by the monitoring systems, even where these tasks are delegated to an AMLCO correspondent in an operational department.

### 3.2.2. Steps to be taken in the event of an alert

The AMLCO must define in a procedure the steps to be taken in the event of an alert (see point 3.2. below). This procedure should include in particular:

- the comparisons to be made to identify cases of homonymy;
- the data that must be collected to allow the alerts to be processed adequately;
- the modalities of the reporting to the FPS Finance - Treasury Department,
- etc.

In the course of processing an alert, the AMLCO may contact the FPS Finance - Treasury Department, but this exchange of information is to be distinguished from the formal reporting mentioned in point 5 below.

### 3.2.3. Suspension of the execution of all transactions

In the event of an alert, financial institutions should suspend the execution of all transactions to or from a person or entity that may be listed, until the alert has been processed. This suspension may be subject to conditions such as the provision, by the customer, of additional information or the provision of documentation on the proposed transactions or the counterparties involved.

## 4. Other organisational and operational measures to be taken

The NBB recommends that, in order to be able to comply with their obligations with regard to financial embargoes and assets freezes, financial institutions also take the following measures:

- i. Integration of embargo and assets freeze aspects into their customer acceptance policy;
- ii. Formalisation of one or more monitoring procedures for financial embargoes and assets freezes;
- iii. Establishment of an operational system for the effective and immediate freezing of assets

### 4.1. Customer acceptance policy

The NBB expects each financial institution to clearly state in its AML/CFTP policy adopted pursuant to Article 8 of the Anti-Money Laundering Law **which objectives** it sets itself in complying with the mandatory provisions on financial embargoes and freezing of assets.

In practice, as indicated on the page "Policies, procedures, processes and internal control measures", the NBB recommends that financial institutions set out in the "customer acceptance policy" section of their AML/CFTP policy the **basic principles** that should be included in the procedures for implementing the mandatory financial embargo provisions that apply when entering into a relationship. The customer acceptance policy should enable each financial institution to ensure that it complies with its obligations with regard to financial embargoes, including its obligations with regard to the freezing of the assets of certain persons and entities as part of the fight against terrorism.

This implies, in particular, that it should be verified whether the customer, his agents or beneficial owners do not appear on the relevant embargo lists.

### 4.2. Development of one or more monitoring procedures for financial embargoes and assets freezes

Financial institutions should put in place one or more procedures for monitoring transactions with a view to complying with financial embargo and assets freezing obligations.

As indicated on the page "Policies, procedures, processes and internal control measures", this or these procedure(s) shall cover at least the following aspects with regard to financial embargoes and assets freezes:

- they organise the analysis, initial validation and regular review process, in accordance with Article 23 of the Anti-Money Laundering Regulation of the NBB, of the system implemented for monitoring the transactions;
- they specify the procedures for regularly updating the lists of persons subject to financial embargo and assets freezing measures, as applied by the system implemented for monitoring the transactions;
- they organise in a precise and detailed manner the process for analysing as soon as possible, under the responsibility of the AMLCO, the alerts generated by the systems for monitoring the transactions in order to ensure their relevance ;
- they organise in a precise and detailed manner, in the event of alerts whose relevance has been demonstrated:
  - the process for the immediate freezing of the assets concerned;
  - the procedures for notifying the competent service of the FPS Finance of the assets freeze; and
  - the subjection of the transaction concerned and, where applicable, of the business relationship within the framework of which the transaction took place, to a review under the responsibility of the AMLCO to determine whether they also generate suspicions of ML/FT.

### 4.3. Establishment of an operational system for the effective and immediate freezing of assets

The AMLCO should set up an operational system that allows to effectively freeze, with immediate effect, the assets of the customer concerned. In addition, financial institutions should ensure that this blocking system can also be activated when a correspondent bank with which they cooperate, detects a potential violation of an embargo or assets freeze.

## 5. Practical implementation of freezing measures

If the analysis of the alert leads the AMLCO to conclude that the customer or beneficiary of a transaction is subject to a financial embargo or assets freeze, this has several consequences.

### 5.1. Prohibition to enter into a relationship

Financial institutions may not enter into a relationship with a person or entity subject to a financial embargo or assets freezing measure.

### 5.2. Prohibition on assets being made available

Implementing a freezing measure implies freezing all assets of the listed customer. Transactions aimed at making assets available to a third party may not be carried out. The term "assets" is defined broadly and covers funds, financial instruments and economic resources. The term "economic resources" refers to all assets of any kind, whether tangible or intangible, movable or immovable, which are not funds but can be used to obtain funds, goods or services.

For bank-type financial institutions, this implies that the accounts of listed customers must remain inactive. In the case of financial institutions within the insurance industry, the performance of life insurance contracts must be frozen in any phase of the contract, save where only the insured is a listed person, as the insured neither pays nor receives funds.

### 5.3. Immediate reporting to the FPS Finance - Treasury Department

The NBB stresses that where a financial institution applies an assets freezing measure, it should contact the FPS Finance - Treasury Department **immediately** (cf. the Treasury's website or using the following e-mail address: [quesfinvragen.tf@minfin.fed.be](mailto:quesfinvragen.tf@minfin.fed.be)).

Financial institutions are expected to do this as soon as possible and, in any case, as soon as the analysis of the alert has demonstrated that the person or entity detected is indeed the person or entity that is subject to a freezing measure.

The NBB recommends that this reporting be made by the AMLCO. In that case, the AMLCO provides the General Administration of the Treasury with all the information at its disposal, so as to enable it to carry out the necessary verifications (for example: a copy of the identity card or passport of the person concerned, reference to the Regulation or Decision which imposes the sanction and which includes the name of the person or entity that is subject to the sanction, etc.).

#### 5.4. Review of the risk profile of a listed customer and of the persons related to him, and, if necessary, reporting to CTIF-CIF

Financial institutions should review the risk profile of customers included in a list of embargoes or assets freezes and of the persons related to them. They should implement appropriate due diligence measures with respect to the customer concerned and the persons related to him and should carry out a thorough examination of previously executed transactions, and, more broadly, of the functioning of all business relationships with the listed person or entity, which may be aimed at making funds, financial instruments or economic resources available to the listed person or entity or may be related to money laundering, terrorist financing or the financing of the proliferation of weapons of mass destruction. If the review of the customer's risk profile leads to a decision to terminate the business relationship, such decision may under no circumstances have the effect of returning the assets subject to the freezing measure to the customer.

Besides the assets freezing measure and its notification to the FPS Finance - Treasury Department, it may also be necessary to report a suspicion to CTIF (see the page "Reporting of suspicions" ).

#### 5.5. Lifting of financial embargo and assets freezing measures

If a financial embargo and assets freezing measure can be lifted, the financial institution should contact the FPS Finance - Treasury Department without delay to determine the concrete measures that should be taken.

### 6. Internal control measures

Financial institutions are expected to monitor periodically and on an ongoing basis that the policies and procedures for financial embargoes and assets freezes that have been validated are properly complied with and that the processes for implementing organisational and operational obligations related to financial embargoes and assets freezes are adequate.

With regard to the system for monitoring financial embargoes and assets freezes, the NBB recommends that the internal audit function pay particular attention to:

- the effectiveness of the monitoring system, taking into account in particular the number of alerts generated;
- the effectiveness of the process for analysing alerts generated by the system, taking into account the number of cases of information being reported to the FPS Finance - Treasury Department;
- the adequacy of the human and technical resources made available to the AMLCO for analysing the alerts generated by the monitoring system.



# Retention and protection of data and documents

Home > Financial oversight > Combating money laundering and the financing of terrori...

## Legal and regulatory framework

- Anti-Money Laundering Law: Articles 60 to 65
- Anti-Money Laundering Regulation of the NBB: Article 24

## Explanatory Memorandum of the Anti-Money Laundering Law

- Articles 60 to 65

## Other reference documents

- See the reference texts on the website of the Data Protection Authority
- CTIF-CFI's information note of 26 October 2017 regarding the disclosure of information to CTIF-CFI

## Comments and recommendations by the NBB

- Comments and recommendations

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



# Anti-Money Laundering Law of 18 September 2017 - Articles 60 to 65

## Art. 60

Obligated entities shall keep, using any type of record-keeping system, for the purposes of the prevention, detection or investigation of potential money laundering and terrorist financing by CTIF-CFI or other competent authorities, the following documents and information:

1° identification data referred to Sections 2 and 3 of Title 3, Chapter 1, where appropriate updated in accordance with Article 35, and a copy of the records or the result of checking an information source, referred to in Article 27, for a period of ten years after the end of the business relationship with their customer or after the date of an occasional transaction;

2° without prejudice to any other applicable document retention legislation, the records and registration data of transactions required to identify and precisely reconstitute the transactions conducted, for a period of ten years after carrying out the transaction;

3° the written report prepared in accordance with 45 and 46, in accordance with the methods described in 2°.

By way of derogation of the first subparagraph, the retention period of ten years shall be reduced to seven years in 2017 and respectively eight and nine years in 2018 and 2019.

## Art. 61

By way of derogation of Article 60, 1°, the obliged entities may substitute the retention of a copy of the records by the retention of references of these records, provided that the references, due to their nature and their retention methods, enable obliged entities to produce these documents immediately, upon request of CTIF-CFI or other competent authorities during the retention period laid down in the same Article, and without that these documents could have been changed altered in the meantime.

The obliged entities who intend to use the derogation referred to in the first subparagraph shall specify beforehand in their internal control procedures, the categories of records of which they retain references instead of a copy, as well as the methods of retrieving these documents through which they can be produced upon request, in accordance with the first subparagraph.

## Art. 62

§ 1. Without prejudice to any other applicable legislation, obliged entities are obliged to delete personal data at the end of the retention period referred to in Article 60.

§ 2. With respect to the retention of documents and information, referred to in Article 60, first subparagraph, regarding the business relationships ended or transactions concluded up to 5 years prior to the date of entry into force of this Law, the retention period of these documents and information shall be seven years.

## Art. 63

Obligated entities have systems enabling them fully respond, within the period of time laid down in Article 48 via secure and confidential channels, in order to ensure complete confidentiality, to requests for information from CTIF-CFI in accordance with Article 81, from the judicial authorities or supervisory authorities referred to in Article 85, within the scope of their respective powers, to determine whether the entities involved maintain or, in the ten years prior to this request, have maintained a business relationship with a specific person, as well as, where appropriate, to questions on the nature of this relationship.

## Art. 64

§ 1. The processing of personal data in pursuant to this Law is subject to the provisions of the Law of 8 December 1992 on the protection of privacy in relation to the processing of personal data and to the provisions of the European regulations that are directly applicable. This personal data processing is necessary to carry out a task in the public interest within the meaning of Article 5 of the same Law.

§ 2. Obligated entities only process personal data in accordance with this Law for ML/TF prevention purposes and do not subsequently process this data in a way that is incompatible with these purposes.

The processing of personal data collected in accordance with this Law for any other purposes than those laid down in this Law, i.e. for commercial purposes, is prohibited.

§ 3. Obligated entities provide their customers with the required information in accordance with Article 9 of the aforementioned Law of 8 December 1992 prior to establishing a business relationship or to carrying out an occasional transaction.

This information particularly includes a general notification of the obligations of obliged entities pursuant to the aforementioned Law when processing personal data for money laundering and terrorist financing prevention purposes.

## Art. 65

The person whose personal data are processed in accordance with this Law does not have the right to access and correct his or her data, nor the right to be forgotten, nor the right to portability of these data, nor the right to object, nor to the right not to be profiled, nor to the notification of security failures.

The right of the individual involved to access personal data relating to him is exercised indirectly, pursuant to Article 13 of the aforementioned Law of 8 December 1992, through the Commission for the Protection of Privacy established by Article 23 of the same Law.

The Commission for the Protection of Privacy only informs the applicant that the necessary verifications have been carried out and of the result of these verifications in terms of the legality of the processing in question. These data may be provided to the applicant when the Commission for the Protection of Privacy, by agreement with CTIF-CFI and after consulting the person responsible for the processing, finds on the one hand that the notification is not likely to reveal the existence of a disclosure referred to in Article 47 and 54, the action taken, or the use of CTIF-CFI's right to request additional information in accordance with Article 81, nor likely to compromise the goal of combating ML/TF, and on the other hand finds that this data relates to the applicant and is held by obliged entities, CTIF-CFI or supervisory authorities in accordance with this Law.



# NBB anti-money laundering regulation of 21 November 2017 - Article 24

## Art. 24

Obligated financial institutions shall record in writing, on paper or electronically, the measures that they have effectively implemented for the application of the due diligence requirements referred to in Book II, Title 3, of the Law, of those concerning analysis of atypical transactions and reporting of suspicions referred to in Book II, Title 4, of the Law, of the provisions of the European Regulation on transfers of funds and binding provisions concerning financial embargoes. They shall keep this justification for the period of time determined by Article 60 of the Law.



# Explanatory Memorandum to the Anti-Money-Laundering Law of 18 September 2017 - Articles 60 to 65

## Art. 60

The draft Article transposes Article 40 of Directive 2015/849 and consolidates Articles 13 and 15 of the Law of 11 January 1993 on keeping records of customer identification, where applicable of that of the customers' authorised agent and beneficial owners, of supporting documents used to verify the identity of these persons, of the result of the consultation of a reliable source of information, of all additional information necessary for the application of the customer acceptance policy and for the execution of the ongoing due diligence and enhanced due diligence obligations as well as the records and registration data of transactions, and written reports.

FATF Recommendation 11 demonstrates that in order to be able to fully cooperate and quickly comply with requests for information from the competent authorities in order to prevent or detect ML/TF acts or to conduct investigations on this subject, obliged entities must keep, for at least five years, the necessary information on its customers obtained through due diligence measures and the documents relating to transactions.

In order to avoid differences in the approach and to satisfy the requirements as regards protection of personal data and legal certainty, this duration of record-keeping within the EEA is contrary to the case for the FATF where a duration of a "minimum" of five years is provided for, the duration of record-keeping with the EEA being defined as a "maximum" of two times five years.

The duration of record-keeping within the EEA is five years after the end of the business relationship or the occasional transaction. However, Directive 2015/849 provides that, where necessary in order to prevent or detect the existence of ML/TF or conduct investigations on the subject, record-keeping for an additional period that does not exceed five years is possible.

The duration of investigations of economic and financial crimes, of which combating money laundering forms an important facet, is generally considerably long. This is largely due to the complexity of financial structures confectioned by criminals with a view to hiding their illegal activity or making it difficult to trace the route of the illegal assets.

However, these types of crime are essentially international. This forces judicial authorities to rely on several letters rogatory, which clearly also lengthen investigations. The same reasoning must be upheld for terrorist financing. These aspects aim for the period of record-keeping by obliged entities to be extended to that permitted by Directive 2015/849, i.e. ten years.

Currently, the record-keeping period is already a minimum of seven years pursuant, non-exhaustively, to Article III.86 of the Code of Economic Law as regards company accounting, Article 60 of the VAT Code or Article 315 1992 or even the 1992 Income Tax Code.

The major difference between these current record-keeping rules and the system under Directive 2015/849 is that the record-keeping period for obliged entities is currently a minimum period. These may, for their own reasons, decide to keep the information concerned for a longer period of time. There is no obligation of systematic destruction of these data after the seven-year period, as is currently the case under Directive 2015/849. After the ten-year record-keeping period, the documents must be destroyed.

This is fundamental because in the practice of legal investigations, it is not unusual for example for an examining magistrate to obtain information held by these obliged entities after the seven-year period as reminded of above. This information may be crucial to establish a money laundering crime or a terrorist financing mechanism.

As money laundering is a crime, Article 21 of the preliminary title of the Code of Criminal Procedure provides for time-barring of five years for public prosecution. Pursuant to Article 22 of the aforementioned preliminary title, this period doubles where an act that interrupts the time barring occurs within the initial period.

In practice, the judicial authorities therefore have ten years after the fact to conduct an investigation into money laundering.

Although the time-barring in terms of terrorist financing is even longer, Directive 2015/849 does not allow records to be kept for more than ten years.

Given the new obligation for obliged entities of destroying data at the end of the record-keeping period, it results from the foregoing that it is reasonable, coherent and proportionate for this period to reflect the maximum period for the time-barring of the money laundering crime.

The draft Article takes over the record-keeping provisions currently contained in Articles 13 and 15 of the Law of 11 January 1993 with the difference that the documents are no longer kept for a period of at least five years but for a period of a maximum of ten years, except in the case of provisions to the contrary in other legislation.

All the documents and information necessary for compliance with the obligations of due diligence of customers must be kept for ten years after the end of the business relationship with the customer or after the date of the transaction executed on an occasional basis. After this period, and without prejudice to any other applicable legislation, obliged entities must delete this personal data.

Therefore, the ten-year record-keeping period is required for prevention or detection of potential money laundering or potential terrorist financing and for the purposes of investigations on the subject by the CTIF-CFI or by other competent authorities such as supervisory authorities. Longer record-keeping will only be authorised for other ends and as long as this is expressly allowed based on legal provisions imposing longer record-keeping.

The opinion of the Council of State specifies that: "The fact of providing in the Law in a general manner for a duration of ten years for keeping documents and information, whilst Article 40, first paragraph, § 1, of the Directive limits it to five, does not seem to comply with the requirements provided for by the following paragraph to extend it to ten: "after having closely evaluated the need and the proportionality of this prolonged record-keeping and deeming it necessary for preventing or detecting money laundering or terrorist financing acts or conducting investigations on the subject".

The foregoing phrase does reserve the possibility of "contrary provisions in national law, which specifies in which circumstances obliged entities may or have to prolong record-keeping", but conditions imposed in this way, in these terms, by the Directive, assume that the Law is limited to determining the circumstances which would impose or allow the prolongation beyond five years, and therefore exclude that the Law from the outset set the duration of this period of record-keeping to ten years in all cases".

Recital 44 of Directive 2015/849 says: "The revised FATF Recommendations demonstrate that, in order to be able to cooperate fully and comply swiftly with information requests from competent authorities for the purposes of the prevention, detection or investigation of money laundering and terrorist financing, obliged entities should maintain, for at least five years, the necessary information obtained through customer due diligence measures and the records on transactions. In order to avoid different approaches and in order to fulfil the requirements relating to the protection of personal data and legal certainty, that retention period should be fixed at five years after the end of a business relationship or of an occasional transaction. However, if necessary for the purposes of prevention, detection or investigation of money laundering and terrorist financing, and after carrying out an assessment of the necessity and proportionality, Member States should be able to allow or require the further retention of records for a period not exceeding an additional five years, without prejudice to the national criminal law on evidence applicable to ongoing criminal investigations and legal proceedings. Member States should require that specific safeguards be put in place to ensure the security of data and should determine which persons, categories of persons or authorities should have exclusive access to the data retained".

The Government does not interpret this in the same way as the Council of State. Recital 44 specifically clarifies that the records must be kept for at least five years. This simply means that this is a minimum limit and this does not in any way exclude extending the period to its maximum.

However, the aim of the ten-year limit retained in the Belgian provision is justified by the need to be able to combat money laundering and terrorist financing. The preparatory work makes an evaluation in terms of necessity and proportionality.

It is also impossible to put in place a system for extending the obligation of record-keeping on a case-by-case basis. Even though this could be conceived for investigations underway, it is nevertheless standard in terms of economic and financial crimes that criminal acts are only reported several years after they were committed or that an investigation reveals culpable acts several years after the start of the investigation. These assumptions require record-keeping for the maximum period, especially as afterwards, the records must be destroyed.

It is this last point that fundamentally differs from what is currently provided for. The Law of 11 January 1993 provides for a minimum period of record-keeping of five years (without specifying a maximum) but above all does not impose the destruction of the data, meaning that it is not difficult to obtain them after the five-year period.

The second paragraph of this draft Article provides for a transitional period up to 2019 for the period during which to keep documents and information, notably seven years for the year 2017 and eight and nine years respectively for the years 2018 and 2019.

The supporting documents and the record-keeping concerned in the draft Article consist of documents that are necessary to identify and precisely reconstruct the transactions carried out.

The obligation to keep documents as defined by the draft Article also covers, as was already the case in the past, the written reports on atypical transactions and suspicious facts transmitted to the AMLCO as well as the analyses of these transactions and these facts that he/she has made and the decisions made on this basis.

However, Article 5quater, § 7 of Council Regulation (EC) No 329/2007 of 27 March 2007 concerning restrictive measures against the Democratic People's Republic of Korea also imposes for the transactions referred to in this Regulation record-keeping obligations in accordance with those of Directive 2015/849. Article 5quater, § 7 of Council Regulation (EC) No 329/2007 of 27 March 2007 states that: "For transactions falling within the scope of paragraph 3, credit and financial institutions referred to in Article 16 shall, in their activities with credit and financial institutions referred to in points (a) to (d) of paragraph 2:

a) apply customer due diligence measures established pursuant to Articles 8 and 9 of Directive 2005/60/EC of the European Parliament and of the Council (\*\*\*\*\*);

b) apply customer due diligence measures established pursuant to Articles 8 and 9 of Directive 2005/60/EC of the European Parliament and of the Council (\*\*\*\*\*);

c) require that information on payers accompanying transfers of funds is provided as required under Regulation (EC) No 1781/2006, as well as information on payees, such as the name of the payee and the payee's payment account number, and, where applicable, a unique transaction identifier, and refuse to process the transaction if any of this information is missing or incomplete;

d) maintain records of the transactions in accordance with point (b) of Article 30 of Directive 2005/60/EC;

e) where there are reasonable grounds to suspect that funds could contribute to North Korea's nuclear-related, ballistic-missile-related or other weapons-of-mass-destruction-related programmes or activities ('proliferation financing'), promptly inform the competent Financial Intelligence Unit (FIU), as defined by Directive 2005/60/EC, or any other competent authority designated by the Member State concerned, as indicated on the websites listed in Annex II, without prejudice to Article 3(1) or 6;

f) promptly report any suspicious transactions, including attempted transactions;

g) refrain from carrying out transactions which they reasonably suspect could be related to proliferation financing until they have completed the necessary action in accordance with point (e) and have complied with any instructions from the relevant FIU or competent authority.

For the purposes of this paragraph, the FIU, or any other competent authority serving as a national centre for receiving and analysing suspicious transactions, shall receive reports regarding potential proliferation financing and shall have access, directly or indirectly, on a timely basis, to the financial, administrative and law-enforcement information that it requires in order to perform that function properly, including the analysis of suspicious transaction reports.

## Art. 61

The draft Article takes over the record-keeping provisions currently contained in Article 38, § 2, second paragraph of the Law of 11 January 1993. Article 38, § 2, second paragraph of the Law of 11 January 1993 provided that: "By way of derogation from the provisions of Article 7, § 1, first paragraph and Article 13, the authorities referred to in § 1 may authorise, by way of a regulation, the bodies and persons subject to their supervision and referred to in Articles 2, § 1, 3 and 4, to keep references to supporting documents required when identifying the customer instead of a copy of these in the cases and under the conditions they determine".

Now, this possibility is included in the Law itself and it is therefore no longer necessary to provide specific provisions to this effect in sectoral regulations.

As was the case in the past, its purpose aims to reduce the administrative burden for obliged entities of taking and keeping copies of supporting documents where keeping and maintaining records of references of these supporting documents enable equivalent results to be obtained.

This means that the obliged entity which has recourse to this possibility may have the certainty of being able, thanks to these references, to quickly find and produce, at the request of the competent authorities (especially the CTIF-CFI and supervisory authorities) the supporting document on which it based its verification of the identity of the customer, authorised agent or beneficial owner without this document being able to be amended, altered or lost in the meantime. This measure in particular refers to the publications in the Belgian Official Gazette or other official publications that can be found with certainty at any point from the body that published them. However, the copy of the identity cards and passports may not be replaced by keeping and maintaining their references because these will not enable the obliged entity to find them with certainty later on and to produce the supporting document which it has used to meet its obligation of verification by the deadline given, with no amendment or alteration.

## Art. 62

The draft Article transposes Article 40, § 1, second paragraph and 40, § 2 of Directive 2015/849.

virtue of Article 40, § 1, second paragraph of Directive 2015/849, the obliged entities must erase the personal data after the authorised period of record-keeping.

Article 40, § 2 of Directive 2015/849 as well as Recital 45 provide for a transitional measure to ensure appropriate and effective administration of justice during the period of transposition of Directive 2015/849 within the legal orders of the Member States and in order to enable a good interaction with the national procedural law by imposing that information and documents that are useful for judicial proceedings underway to prevent and detect possible money laundering or terrorist financing or investigating on the subject, which are pending in the Member States at the date of entry into force of Directive 2015/849, i.e. 25 June 2015, are kept during a period of five years following this date with the possibility of extending this period by a new five-year period.

From an operational standpoint, it is not possible to determine all the legal proceedings in which such information and documents are necessary. It is just as impossible to determine today the information or documents that would be necessary in future proceedings. It is therefore necessary to provide for a transitional measure which is general in order to maintain the possibility of launching or continuing legal investigations that require data from prior to the entry into force of the Law.

This is why the draft Article imposes the seven-year period of record-keeping for documents and information relating to business relationships or transactions finalised or entered into up until five years before the entry into force of the present Law. In this way, legal certainty seems assured in that there would only be a single record-keeping system

## Art. 63

The draft Article takes over an already existing obligation under the Law of 11 January 1993 (Article 15, first paragraph) and transposes Article 42 of Directive 2015/849.

The obligation of record-keeping enables these transactions to be precisely reconstructed. It implies that obliged entities take the necessary measures to be able to respond completely and appropriately, as well as promptly, to the requests for information from the CTIF-CFI, judicial authorities or supervisory authorities referred to in draft Article 85. The obliged entities that have decentralised networks “will need to ensure that their organisation and especially their IT system is able to produce the necessary information to be able to allow the head office to meet the said requests for information forthwith” (Chamber of Representatives, 2003-2004, DOC 51 0383/001, p. 37).

The “secure channels” to which the draft Article refers means any means of communication, on whatever medium, that guarantees the confidentiality of the information sent.

## Art. 64

The draft Article transposes Articles 41, § 1 to 3 and 43 of Directive 2015/849. Recital 43 of Directive 2015/849 provides that “It is essential that the alignment of this Directive with the revised FATF Recommendations is carried out in full compliance with Union law, in particular as regards Union data protection law and the protection of fundamental rights as enshrined in the Charter”.

At this time, the protection of personal data is governed at European level by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter ‘Directive 95/46/EC’), as well as at a national level by the Law of 8 December 1992 on the protection of privacy with regard to the processing of personal data (hereinafter the ‘Law of 8 December 1992’), which transposes it.

On 25 May 2018, Directive 95/46/EC was repealed and replaced by Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), hereinafter ‘Regulation 2016/679’.

Regulation 2016/679 entered into force the twentieth day following that of its publication in the Official Journal of the European Union, i.e. 24 May 2016, but will only directly apply in the Member States from 25 May 2018. Regulation 2016/679 will at that time substitute the Law of 8 December 1992 which will probably be repealed.

Article 5, e) of the Law of 8 December 1992 provides that personal data may be processed only if [...]: “the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller or in a third party to whom the data are disclosed”. Article 6, § 1 of Regulation (EU) 2016/679 also provides that: “Processing shall be lawful only if and to the extent that at least one of the following applies: [...] e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;”.

Recital 42 of Directive 2015/849 says: “The fight against money laundering and terrorist financing is recognised as an important public interest ground by all Member States” and Article 43 of Directive 2015/849 says that the processing of personal data for the purposes of the prevention of money laundering and terrorist financing is considered to be a matter of public interest under Directive 95/46/EC”. Article 94, § 2 of Regulation 2016/679 provides that: “References to the repealed Directive shall be construed as references to this Regulation”. The processing of personal data for AML/CFT purposes continues to be considered a task carried out in the public interest.

According to Article 4 of the Law of 8 December 1992 and Article 5, § 1, b) of Regulation 2016/679, the data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.

The draft Article executes these provisions: it specifies the purpose of the collection, i.e. the prevention of ML/TF, prohibits the further processing in an incompatible way and confirms that this processing is necessary for a task carried out in the public interest.

In accordance with Article 9 of the Law of 8 December 1992 and Article 13 of Regulation 2016/679, the person concerned is informed by the obliged entities of the name and address of the data controller, the reason for the processing as well as a general warning concerning the obligations imposed by the draft Law to obliged entities where they process personal data for the purposes of ML/TF prevention.

## Art. 65

The draft Article transposes Article 41, § 4 of Directive 2015/849. Article 3, § 5, 4°, of the Law of 8 December 1992 provides that Articles 9 (right to be informed), 10, § 1 (right of access), and 12 (right of rectification) do not apply: “[...] 4° to the processing of personal data that has become necessary as a consequence of the application the Act of 11 January 1993 on the prevention of the use of the financial system for the purpose of money laundering;”.

Article 23, § 1 of Regulation 2016/679 also provides that European Union or Member State law may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34 of Regulation (EU) 2016/679 “when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard: [...] d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;”.

Article 23, § 2 of Regulation 2016/679 provides that any legislative measure referred to in § 1 shall contain specific provisions at least, where relevant, as to: “a) the purposes of the processing or categories of processing, (b) the categories of personal data; (c) the scope of the restrictions introduced; (d) the safeguards to prevent abuse or unlawful access or transfer; (e) the specification of the controller or categories of controllers; (f) the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing; (g) the risks to the rights and freedoms of data subjects; and (h) the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction.”.

Recital 46 of Directive 2015/849 strictly limits access by the person concerned and provides that: “The rights of access to data by the data subject are applicable to the personal data processed for the purpose of this Directive. However, access by the data subject to any information related to a suspicious transaction report would seriously undermine the effectiveness of the fight against money laundering and terrorist financing. Exceptions to and restrictions of that right in accordance with Article 13 of Directive 95/46/EC and, where relevant, Article 20 of Regulation (EC) No 45/2001, may therefore be justified. The data subject has the right to request that a supervisory authority referred to in Article 28 of Directive 95/46/EC or, where applicable, the European Data Protection Supervisor, check the lawfulness of the processing and has the right to seek a judicial remedy referred to in Article 22 of that Directive. The supervisory authority referred to in Article 28 of Directive 95/46/EC may also act on an ex-officio basis. Without prejudice to the restrictions to the right to access, the supervisory authority should be able to inform the data subject that all necessary verifications by the supervisory authority have taken place, and of the result as regards the lawfulness of the processing in question”.

In other words, the person concerned by the data processing carried out by the CTIF-CFI or by the obliged entity has no direct access to his/her data. The right is exercised indirectly, pursuant to Article 13 of the aforementioned Law of 8 December 1992 through which “Anyone proving his identity has the right to address the Commission for the Protection of Privacy [...]. The Commission for the Protection of Privacy shall only inform the data subject of the fact party that the necessary verifications have been carried out”.

However, this right of indirect access is only partial to:

- enable the obliged entities or the CTIF-CFI as well as the supervisory authorities of the obliged entities to accomplish their tasks as required for the draft Law; or
- avoid hindering the requests for intelligence, analysis, investigations or procedures of an official or judicial nature, conducted for the purposes of the draft Law and to avoid compromising prevention and detection in case of money laundering or terrorist financing and any investigations on the subject.

Apart from the right of access and rectification, the draft Article provides, in accordance with Article 23 of Regulation 2016/679, that the person concerned does not have the following rights provided for by this Regulation:

- right to erasure ('right to be forgotten'): Article 17 of Regulation 2016/679 provides that:
  - "1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies: [...]
  - (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6 (1), or point (a) of Article 9(2), and where there is no other legal ground for the processing; [...].
  - 2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.
  - 3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary: [...]
  - (b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; [...];
- right to data portability:
  - Article 20 of Regulation 2016/679 provides that: "1. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where: [...]
  - 3. [...] That right shall not apply to processing necessary for the performance of a task carried out in the public interest [...];
- right to object:
  - Article 21, § 1 of Regulation 2016/679 provides that:
    - "The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her [...];"
- right not to be subject to automated individual decision-making, including profiling:
  - Article 22 of Regulation 2016/679 provides that:
    - "1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.
    - 2. Paragraph 1 shall not apply if the decision: [...]
    - b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests [...];"
- right to notification of data breach: Article 34, § 1 of Regulation 2016/679 provides that: "When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay".

Article 23, § 1 of Regulation 2016/679 provides that "European Union or Member State law [...] may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34 [...] "when such a restriction [...] is a necessary and proportionate measure in a democratic society to safeguard: [...] d) the prevention, investigation, detection or prosecution of criminal offences [...] including the safeguarding against and the prevention of threats to public security [...]".

In accordance with the same Article 23 of this Regulation, the present Law excludes the exercise of these rights in the context of processing of data for the purpose of prevention of ML/TF.

# Retention and protection of data and documents: Comments and recommendations by the NBB

Home > Financial oversight > Combating money laundering and the financing of terrori...

## Retention of documents

In accordance with Article 60 of the Anti-Money Laundering Law, financial institutions should keep the following documents and information, using any type of record-keeping system:

1. the identification data of customers, agents and beneficial owners, where appropriate updated in accordance with Article 35 of the Anti-Money Laundering Law, and a copy of the supporting documents or of the result of consulting an information source, **for a period of ten years** from the end of the business relationship with the customer or the date of execution of the occasional transaction;
2. without prejudice to compliance with any other legislations on document retention, the supporting documents and records of transactions that are necessary to identify and accurately reconstruct the transactions carried out, **for a period of ten years** from the date of execution of the transaction;
3. the written report drawn up in the event of reporting to CTIF-CFI, **for a period of ten years** from the date of execution of the underlying transaction (according to the same terms and conditions as set out in point 2° above).

The retention period of ten years referred to above is reduced to seven years for transactions carried out in 2017, and to eight and nine years for transactions carried out in 2018 and 2019 respectively. It should be noted that, by complying with the ten-year period provided for in the Anti-Money Laundering Law, the obligation set out in the European Regulation on transfers of funds to retain information on the payer and payee for a period of five years is automatically met.

The NBB notes that the copy of the supporting documents that have been used by the financial institution to verify the identity of the customer or his agent, may be taken on a durable data storage device (that, according to the definition of Article 1.1.15° of the Code of Economic Law, may be an electronic storage device), which may also be used for its storage. The same retention obligations apply to documents that have been used by the institution to verify the identity of the beneficial owners or, failing that, to evidence that such verification did not prove to be reasonably possible.

Article 61 of the Anti-Money Laundering Law also provides that instead of keeping a copy of the supporting documents, financial institutions may keep the references of these documents, provided that, due to their nature and the modalities of their storage, these references allow them with certainty to produce the documents concerned immediately, at the request of CTIF-CFI or of other competent authorities (in particular the NBB), during the retention period laid down in the said Article, and that it has not been possible to modify or alter these documents in the meantime. Financial institutions considering making use of this derogation should specify in advance, in their internal control procedures, the categories of supporting documents of which they will keep the references instead of a copy, as well as the procedures for retrieving the documents concerned so that they can be produced on request.

In order to ensure that financial institutions are able to demonstrate a posteriori, in particular to the NBB in the exercise of its supervisory powers, that they have effectively fulfilled their legal and regulatory obligations with regard to customer and transaction due diligence and to the analysis of atypical transactions and reporting of suspicions, and that they have complied with the provisions of the European Regulation on transfers of funds and the mandatory

provisions on financial embargoes, Article 24 of the Anti-Money Laundering Regulation of the NBB requires that the written or electronic documents in which they have recorded the measures they have actually implemented to this end, be kept for the same periods as those indicated above.

## Protection of personal data

The Anti-Money Laundering Laws contains several provisions relating to the protection of personal data in its Articles 62 to 65. The NBB expects financial institutions to comply with these provisions as well as with those of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data ("General Data Protection Regulation" - "GDPR").

Attention is drawn in particular to the obligation to delete, on expiry of the periods referred to in point 1 above, personal data that have been kept in accordance with Article 60 of the Anti-Money Laundering Law and Article 24 of the NBB Anti-Money Laundering Regulation of the NBB (cf. Article 62, § 1, of the Anti-Money Laundering Law). Furthermore, it should be noted that persons whose personal data are processed for anti-money laundering purposes can exercise an "indirect" right of access through the Data Protection Authority, which was established by the Law of 3 December 2017. The scope of this right is described in Article 65, third paragraph, of the Anti-Money Laundering Law.

## Document retention procedure

In order to operationalise the rules set out in points 1 and 2 above, the NBB expects financial institutions to develop a document retention procedure (see also the page "Policies, procedures, processes and control measures").

This procedure should at least include:

1. a list of the information and documents to be kept,
2. the retention period,
3. the event from which the retention period is to be calculated, and
4. the rules to be respected regarding the confidentiality of the documents, i.e. their storage, persons having access to them, procedures for accessing data, etc. (even if the institution uses an external service provider to archive these data).

In this regard, the NBB invites financial institutions to set up mechanisms for accessing customer files and data relating to their transactions, that are adapted to their organisation and that allow the authorities responsible for AML/CFT to receive these files and data as soon as possible, in particular in order to be able to take them adequately into account in fulfilling their due diligence obligations and obligation to analyse atypical operations, and to be able to respond without delay to any request for additional information made by CTIF-CFI. Financial institutions must nevertheless take into account the recommendations on the processing of personal data issued by the Data Protection Authority.

5. the procedures for deleting personal data, in accordance with Article 62 of the Anti-Money Laundering Law, at the end of the retention period.

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



# Restriction of the use of cash

Home > Financial oversight > Combating money laundering and the financing of terrori...

## Legal and regulatory framework

- Anti-Money Laundering Law: Articles 6, 66 and 67

## Explanatory Memorandum to the Anti-Money-Laundering Law of 18 September 2017

- Articles 6, 66 and 67

## Other reference documents

See the website of FPS Economy

## Comments and recommendations by the NBB

- Comments and recommendations

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



# Anti-Money Laundering Law of 18 September 2017 - Articles 6, 66 and 67

## Art. 6

The restrictions on cash payments referred to in Article 66, § 2, first subparagraph, and Article 67, are also applicable to any natural person or legal person making payments or donations referred to in these provisions.

## Art. 66

§ 1. For the purposes of this Article the “sales price of real property” means the total amount that the buyer must pay and that relates to the purchase and financing of this property, including the resulting associated costs.

§ 2. The sales price of real property may only be paid by means of a bank transfer or cheque.

The agreement and deed of sale must specify the number(s) of the financial account from which the amount was or will be debited, as well as the identity of the account holders.

When notaries or real estate agents referred to in Article 5, § 1, 26° and 30°, find that the first and second subparagraphs are not complied with, they shall immediately inform CTIF-CFI using the methods described in Article 50.

## Art. 67

§ 1. For the purposes of this Article the following definition shall apply:

1° “consumer”: any natural person acting for purposes outside the framework of his commercial, industrial, craft or professional activity.

2° “precious materials”: gold, silver, palladium;

3° “old metals”: any used or reclaimed pieces of metal;

4° “copper cables”: any delivered copper cables, in any form, whether stripped or cut, shredded, ground or mixed with other materials, excluding flexible copper cables that are part of an appliance.

§ 2. Regardless of the total amount, no payment or donation may be made or received in cash for an amount above EUR 3 000 of its equivalent in another currency, as part of one or several transactions that seem to be related.

Except in case of public auction under the supervision of a bailiff, a person who is not a consumer may not pay any amount in cash when buying old metal, copper cables or goods containing precious materials from another person, unless these precious materials are only present in small quantities and only because of their necessary physical properties.

By way of derogation from subparagraph 2, a person who is not a consumer may only pay an amount of up to EUR 500 in cash when buying old metals or goods containing precious materials from a person who is a consumer, unless these precious materials are only present in small quantities and only because of their necessary physical properties. In this case these persons must identify and register the person who presents himself/herself with metals or goods containing precious materials.

The provision laid down in the first subparagraph does not apply to:

1° the sale of real property, referred to in Article 66;

2° transactions between consumers;

3° the obliged entities referred to in Article 5, § 1, 1°, 3°, 4°, 6°, 7°, 10° and 16°, as well as other natural persons when they carry out transactions with these entities.

§ 3. When the submitted accounting documents, including bank statements, do not enable to determine how payments or donations have been made or received, these are presumed to have been carried out or received in cash.

Subject to evidence to the contrary, any payment or donation in cash is presumed to be made on Belgian territory, and therefore subject to the provisions of this article when at least one of the parties resides or conducts an activity in Belgium.



# Explanatory Memorandum to the Anti-Money-Laundering Law of 18 September 2017 - Articles 6, 66 and 67

## Art. 6

Draft Article 6 has the sole purpose of indicating that the *ratione personae* scope of two provisions of the Law, namely Article 66, § 2, first paragraph, and Article 67, which relate to payments and donations in cash, is not limited to the obliged entities but encompasses all natural or legal persons.

## Art. 66

Draft Article 66 takes over Article 20 of the Law of 11 January 1993 and adds the option to state more than one account number in the contract and formal deed of sale, as well as the obligation to state the names of the holder(s) of the debited account(s) in the contract and deed of sale.

This information must be stated as soon as they are known by the estate agent or notary. However, they are not responsible for verifying it beyond doing so against the data provided on the cheque or the bank account statements.

In view of the controversy in the past about the notion of "sale price of real property" which according to some interpretations refers only to the price of the property in the strict sense, it is clarified in the present Law that the sale price of property refers to the total amount that the buyer must pay and that relates to the purchase and financing of this property. This amount therefore not only includes the costs relating to the sale, i.e. the registration fees and other taxes, the mortgage arrangement fees, the fees and expenses of the notary, the estate agent fees where applicable, as well as the amount deposited with the acting notary in the event of a higher offer, but also the costs relating to potential contracts associated with the sale such as mortgage contracts, life insurance or debt balance insurance in case of death, including the costs of mortgage registration. Consequently, in the context of a property sale, payments may only be made by bank transfer or cheque.

By way of reminder, estate agents and notaries who identify a payment made by a method other than bank transfer or cheque are obliged to report this to the CTIF-CFI, whether the payment was made in their presence or otherwise (Parliamentary documents, Chamber of Representatives, meeting 2003-2004, doc. 51 0383/001, pages 39 and 40).

## Art. 67

Draft Article 67 does not change the essence of the approach of Article 21 of the Law of 11 January 1993. By way of reminder, Belgium had opted to limit cash payments collected by merchants in order not to subject them to the other obligations provided for by the Law of 12 January 2004, following the entry into force of Article 2bis, 6), of Directive 91/308/EEC (inserted by Article 1, 2), of Directive 2001/97/EC). This principle relating to the restriction of cash payments therefore remains in this draft.

The changes introduced by draft Article 67 to Article 21 of the Law of 11 January 1993, seek two objectives:

- to pool all the provisions relating to restrictions to payments and donations in cash, as will be clarified in the comments regarding § 3 (purchase of copper cables, old metals and precious materials);
- and to remedy the following problems with the application of the aforementioned Article 21:
  - the restricted scope, both *ratione materiae* (the payments for sales or services) and *ratione personae* (the merchants and service providers), makes it impossible to encompass different situations in which sometimes cash payment is important (exchanges against payment, namely of gold or cars; pharmacists; farmers; non-profit associations, etc.);
  - the rule of the double threshold (ten per cent and EUR 3 000) is complex and cannot easily be understood by the merchant;
  - the sale of gold to professionals by consumers is subject to complicated rules that are not particularly efficient, part of which are laid down in Article 21 of the Law of 11 January 1993 and the other in Article 69 to 71 of the Law of 29 December 2010 containing miscellaneous provisions (I);
  - the burden of proof of payment in cash falls to the supervisory authority; and
  - the burden of proof of the payment having occurred in Belgium falls to the authority, which is a difficult task since payment in cash leaves no trace.

### Scope

To first remedy the issue with regard to the scope, it is suggested that it be clarified and extended, while maintaining a series of exceptions.

*Ratione materiae*, draft Article 67 applies to all payments, regardless of the nature of the underlying obligation. This can therefore be either of a contractual or extra-contractual nature.

Furthermore, draft Article 67 also refers to donations, such as donations to non-profit associations.

*Ratione personae*, draft Article 67 applies to all persons, natural or legal persons, and no longer only to merchants and service providers.

There are three exceptions for situations that also do not come under the scope of Article 21 of the Law of 11 January 1993:

1° Draft Article 67 will never be applicable to the transactions referred to in draft Article 66, i.e. the sale of immovable property.

Consequently, if for example an estate agent or a notary receives a sum of money from a future buyer of a property, he/she would be faced with administrative sanctions pursuant to Article 132 and not criminal sanctions pursuant to Article 137, even if this amount comes to more than EUR 3 000.

2° Draft Article 67 will not apply to transactions between consumers. Payments and donations in cash between consumers will consequently not be subject to any restriction. The term 'consumer' is included in Article I.1, 2° of the Code of Economic Law.

The ratio legis of the exception regarding the restriction of payments and donations in cash for consumers is the following: first of all Directive 2015/849/EU does not require it; equally, the application of a restriction for consumers would probably have little effect on the prevention of ML/TF given the rarity of transactions between consumers for high-value assets; moreover it is impossible to systematically supervise consumers given that they are not obliged to keep written records of their transactions; finally, such supervision would require access to their homes and it seems out of proportion to conduct such supervision in the absence of suspicions of ML/TF.

3° Draft Article 67 will not apply to the payments or donations in cash executed by or with financial institutions referred to in Article 5, § 1, 1°, 3°, 4°, 6°, 7°, 10° and 16°, i.e. banks for which transactions in cash are inherent to their activity. The transactions referred to are those executed by or with the following financial institutions: the NBB, bpost, credit institutions, payment institutions, issuers of electronic money, stockbroking firms and bureaux de change. Even though payments (not to be confused with the term 'payment transaction' referred to in Article I.9, 6° of the Code of Economic Law) in cash at a bank are rare (and donations even more so), it is useful to provide for this exception to avoid any controversy as to the nature of a considerable sum paid in cash to an institution that comes under this exception.

It goes without saying that for purposes of consistency, the exception does not only have to be applied to the financial institution but also to the other person, who may be a natural person or a legal person, such as the customers with whom the financial institution executes the cash transaction.

Consequently, a merchant is still of course allowed to bring weekly takings in cash to the bank, irrespective of the amount concerned.

*Double threshold: EUR 3 000 and ten per cent*

The second problem relates to the application of the double threshold when the price of the sale or service reached EUR 3 000: the cash payment could not exceed ten per cent of the price of the sale or service (threshold 1) and cumulatively, as long as this amount did not come to more than EUR 3 000 (threshold 2).

Contrary to Article 21 of the Law of 11 January 1993, the limit of EUR 3 000, referred to in draft Article 67, no longer relates to the amount of a sum to be paid but rather to the sum paid or donated in cash. As a result, a donation of EUR 5 000 can be made and received in cash up to EUR 3 000; the payment or the donation of the balance needs to be made and received in another way. This flexibility is justified by the very low threshold of EUR 3 000 and by the complexity of the aforementioned Article 21, which initially did not allow any payment in cash whatsoever if the price exceeded a certain amount, which penalised every minimal payment in cash, and which since the change in the law of 29 March 2012, permits a payment in cash of ten per cent of the price, which makes the rule more complex.

*The sale of gold*

The third problem relates to the special rule reserved for the sale of gold to professionals by consumers.

The sale of gold is currently covered in two provisions:

- Articles 69 and 70 of the Law of 29 December 2010 containing miscellaneous provisions (I) which essentially determine that professional buyers of precious metals or old metals must identify the purchaser who pays in cash by his/her first name, surname and date of birth, and that the purchase of copper cables may not be paid in cash;
- Article 21, second paragraph of the Law of 11 January 1993, inserted by Article 3 of the Law of 15 July 2013 containing urgent provisions on the fight against tax fraud: with regard to the prohibition for merchants of precious metals from receiving the sales price in cash over and above the limit laid down pursuant to Article 21, first paragraph, the second paragraph has added a prohibition for this merchant from settling the purchase price in cash for EUR 5 000 or more (since 1 January 2014, this amount has been reduced to EUR 3 000). Consequently, merchants in precious metals must for the time being stick to the cash payment limit of ten per cent or EUR 3 000, not only when selling gold (pursuant to the first paragraph) but also when purchasing it, at least when this gold falls under the definition of "precious metals" (pursuant to the second paragraph).

The reason for adding this second paragraph is that there have been considerable laundering operations with gold (19th Annual Report of the CTIF-CFI 2012, page 80 *et seq.*) and that the CTIF-CFI and the FPS Economy have identified the fact that since the rise in gold prices in 2012, considerable quantities of gold in the form of ingots have been sold by African individuals to Belgian merchants for cash.

There is still the question as to whether the cash payment limit as referred to in Article 21 applies both to the purchase and the sale by a precious metals merchant of gold ingots deemed to be investment gold.

The answer to this is certainly in the affirmative as regards the sale of gold ingots by merchants; given that gold ingots are movable property like any other, the sale thereof by a merchant is subject to the restriction laid down in Article 21, first paragraph of the Law of 11 January 1993.

The answer is less obvious for the purchase of gold by precious metals merchants, as referred to in Article 21, second paragraph of the Law of 11 January 1993.

The term 'precious metals' refers in particular to the definition given in Article 69 of the Law of 29 December 2010 containing miscellaneous provisions (I), which appears to exclude investment gold such as ingots and coins.

As regards the sale of gold ingots, Article 21, first paragraph refers to the sale price of "assets". The parliamentary work for the Law of 12 January 2004 amending the Law of 11 January 1993, states that this concerned movable property and that the provision did not apply to "securities" (Chamber of Representatives, DOC 51, 0383/001, p. 41).

It was considered that such a measure was unnecessary for the sale of securities given that the trading of securities implies the intervention of financial intermediaries already subject to the Law of 11 January 1993.

To remedy these difficulties of interpretation, draft Article 67 adds the following changes:

- the complex notion of 'precious metals' defined in Article 69 of the Law of 29 December 2010 containing miscellaneous provisions (I), is broadened to the simpler term 'precious materials'. While Article 69 of the aforementioned Law only referred to gold, silver and platinum, from now on palladium is also stated.
- except in the case of a public sale under the supervision of a bailiff, a person who is not a consumer (for example, a company such as a jeweller or gold wholesaler) may not pay any amount in cash when buying old metal, copper cables or goods containing precious materials (unless these precious materials are only present in small quantities and only because of their necessary physical properties). 'Goods' here must be understood to mean the physical movable goods that themselves contain precious materials; securities are therefore excluded. The sale and purchase of securities will, however, remain subject to the general restriction of EUR 3,000 for payments and donations in cash as provided for in § 2. The intention of the exclusion of goods that have a small amount of precious materials in them and only for their necessary physical properties is to exclude goods such as computers and mobile phones. These products contain a very small quantity of gold in the places necessary to ensure good conductivity. If, however, a mobile phone is gold-plated or encrusted with diamonds, these precious materials are not present because of their necessary physical properties, meaning that the prohibition on payment in cash is applicable in the case of a purchase by a non-consumer. As regards the exception for public sales under the supervision of a bailiff, this is justified by the fact that the transfer of ownership that precedes the sale is traceable, the payment in cash incurs no risk of dealing in stolen goods or of ML/TF, and the bailiff is an obliged entity pursuant to the Law. The type of seller (consumer or not) is of no importance.

This complete ban on payment in cash for old metals, copper cables or goods that contain precious materials by a purchaser who is not a consumer is justified in view of the increased risk of money laundering and dealing in stolen goods that has been identified as regards these goods. The scope of the ban encompasses old jewels made of gold, silver or platinum. This is perfectly in line with the National Security Plan 2016-2019 regarding property crime (strategic goal 1, p. 62), namely by contributing to an integrated approach for dealing in stolen goods (goal 4) and to a focused administrative approach to itinerant criminal groups, by reinforcing the supervision of commercial businesses where stolen goods are likely to be sold (goal 5).

As regards, for example, the purchase of gold by professionals, the aforementioned registration obligation does not prevent dealing in stolen goods: unscrupulous merchants regularly circumvent these by overvaluing the quantity bought from certain consumers so as to avoid registering the data of other sellers who sell jewels of suspicious origin. Even by reinforcing this registration system by adding other information such as the amount bought, the price, the transaction date, the signature of the seller and the identification of the purchaser on the purchase slip, etc., the document can still be forged.

Moreover, this total ban for purchasers who are not consumers on cash purchases of goods that contain these precious materials is likely to exclude from the market itinerant purchasers with a dubious background and support honest and reliable local merchants.

By way of reminder, as regards the purchase of copper cables, draft Article 67, § 2, second paragraph, barely changes the rule under Article 70 of the Law of 29 December 2010 containing miscellaneous provisions (I), all payments in cash remaining prohibited.

When Article 67, § 2, second paragraph, which prohibits cash payment in the case of a purchase by a non-consumer of old metals, copper cables or goods that contain precious materials is adopted, the obligation for merchants to register information on the seller who has paid in cash as provided for in Article 70, § 3, of the Law of 29 December 2010 containing miscellaneous provisions (I) will lapse. Moreover, all provisions that restrict payments and donations in cash will be contained in one single piece of legislation, which will facilitate the understanding thereof both for citizens and authorities.

An exception is provided for to this total ban for small cash payments of up to EUR 500. The introduction of the restriction on cash payments has the purpose of combating fraud pursuant to organised property crime as set out in the National Security Plan. This may not lead to the consumer who occasionally sells precious metal in the form of an old ring being obliged to build a commercial relationship with the purchaser. In such cases, cash payment is still permitted up to an amount of EUR 500. As an example, this means that in the case of a gold price of EUR 1 150 per troy ounce (around 31.10 grams), a consumer can offer more than 13 grams of 24-carat gold for sale. Often, old jewels are of a lower quality of gold, meaning that this standard of EUR 500 covers these occasional transactions by

consumers. In those cases, the existing identification obligation will be maintained. The introduction of the restriction on cash payments equally has no effect for consumers who offer old metals for sale. In such cases, cash payment is still permitted up to an amount of EUR 500.

The removal of the identification obligation for payments by bank transfer is justified by the fact that since the introduction of the Law of 11 January 1993, the financial sector has become increasingly compliant. Moreover, payment by bank transfer opens the way for the public prosecutor's office to investigate the traceability of criminal property as part of its integrated approach to tackling crime.

#### *Proof of the use of cash*

The fourth problem relates to the burden of proof of payment in cash: failing the presence of accounting evidence or confession, the proof of payment in cash must be delivered by presumption. Article 67, § 3, first paragraph determines that payments or donations are presumed to have been made or received in cash when it is not possible to determine, by way of accounting documents, that these payments or donations were made or received in any other way.

#### *Proof of the place of payment of donation in cash*

The fifth problem relates to the location of the payment: in view of the fact that Article 21 is a criminal provision, the principle of territoriality stated in Articles 3 and 4 of the Criminal Code, according to which a criminal law applies to infringements committed on Belgian territory applies, except where the law expressly determines that it also applies outside Belgian territory.

Pursuant to this principle, only payments and donations made in Belgium are subject to the restrictions on payments in cash. It may be difficult to establish the location of a payment or donation in cash when one of the parties is in another country given that such a transaction, by its very nature, leaves no trace. This is the case where a Belgian merchant purchases goods in Germany and claims to have paid for them in this country.

To remedy this issue, draft Article 67, § 3, second paragraph makes the rebuttable presumption that the payment or the donation is made in Belgium where one of the parties is either Belgian, or resides or conducts his/her activity in Belgium.

When a legal person is involved, the nationality or place of residence of the natural persons responsible is of no importance. As a result, in the case of a payment or donation in cash of more than EUR 3 000 abroad by an EBVBA/SPRLU governed by Belgian law, the sole director of which is Swedish and resides in Sweden, he/she will be criminally liable for the infringement of the restriction determined under Belgian law.

Given that this is a rebuttable presumption, it can be rebutted by any legal means, such as proof of that person's presence in or travel to the foreign country at the time of the transaction.

In addition to the five problems raised here, the term "equivalent" is also added after the euro amount to cover transactions executed in a foreign currency, which is sometimes the case in import and export transactions.

Finally, the restriction of EUR 3 000 remains applicable on a whole set of transactions which appear to be linked.

Compared to the former Article 21, the term "*fractionnement*" is no longer included given that this term does not appear in the Dutch-language version of the Directive (or in the English version).

The transactions that cumulatively meet the following criteria are likely to be linked:

- they are between the same parties (e.g. payments between company A and company B);
- they have the same linked purpose or purposes (e.g. several works conducted by the same company or for the same site, various consecutive donations to a non-profit association by the same person or by that person's family members);
- they are close to each other in time (question of fact).

The same transactions which are split up for no reason will certainly constitute linked transactions.

As a result, several grouped purchases may be paid for in cash only up to EUR 3 000 for the whole amount of purchases given that the balance will need to be paid in another way.

Moreover, splitting the purchases of goods will not be able to lead, for example, to a spreading of the restriction on

payments and donations in cash, as was the case in the past.



# Restriction of the use of cash: Comments and recommendations by the NBB

Home > Financial oversight > Combating money laundering and the financing of terrori...

## Contents

- 1. Purchase of real property
- 2. Transactions other than the purchase of real property
- 3. Proof
- 4. Sanctions
- 5. Internal procedures and control

The issues surrounding the use of cash have been given particular attention by the legislator, who has grouped all provisions laying down restrictions in this matter in a specific chapter of the Anti-Money Laundering Law (Articles 66 and 67). This chapter has a broad scope as it applies, in principle, to “any natural person or legal person making payments or donations” (see Article 6 of the Anti-Money Laundering Law).

The NBB expects financial institutions to take into account the provisions of the aforementioned chapter when performing their obligation to identify occasional customers and their ongoing due diligence obligation. Regulation (EU) 2018/1672 of the European Parliament and of the Council of 23 October 2018 on controls on cash entering or leaving the Union and repealing Regulation (EC) No 1889/2005 should also be complied with.

The main rules on the subject are summarised below.

## 1. Purchase of real property

As was the case under the Law of 11 January 1993, the sales price of real property may only be paid “by means of a bank transfer or cheque”, excluding any cash payment (see Article 66, § 2, first paragraph, of the Anti-Money Laundering Law). Real estate agents and notaries who find that a payment has been made otherwise than by means of a bank transfer or cheque are required to notify CTIF-CFI of this fact, “whether the payment was made in their presence or otherwise”. In this case, the reporting to CTIF-CFI is “objective”, meaning that it must not be assessed whether the transaction is suspected of being linked to money laundering or terrorist financing.

However, the Anti-Money Laundering Law introduced two new elements:

1. the agreement and deed of sale must henceforth specify the number(s) of the financial account(s) from which the amount was or will be debited, as well as the identity of the account holders;
2. the Anti-Money Laundering Law now specifies what is meant by “the sales price of real property”, namely “the total amount that the buyer must pay and that relates to the purchase and financing of this property, including the resulting associated costs”.

It should be noted that financial institutions are not subject to the obligation described above to submit an “objective” reporting to CTIF-CFI in case of cash payments of real property sales prices. However, where a financial institution is asked to perform a cash transaction for which it has reason to suspect that it is linked to the cash payment of all or part of the sales price of real property, the NBB recommends that the financial institution notify CTIF-CFI by submitting a reporting of suspicions.

## 2. Transactions other than the purchase of real property

For transactions other than the purchase of real property, the Anti-Money Laundering Law groups all provisions restricting the use of cash in a single article (Article 67) and provides for a simplified approach by proposing clearer rules to remedy the problems regarding the implementation of the former provision of the Law of 11 January 1993.

### 2.1 General rule for restricting the use of cash

In accordance with Article 67, § 2, first paragraph, of the Anti-Money Laundering Law, “regardless of the total amount, no payment or donation may be made or received in cash for an amount above EUR 3 000 of [sic] its equivalent in another currency, as part of one or several transactions that seem to be related”.

#### 2.1.1. Scope

##### a. *ratione materiae*

The scope *ratione materiae* of the former provisions of the Law of 11 January 1993 has been expanded since, according to Article 67 of the Anti-Money Laundering Law, this restriction applies to **all payments** regardless of the nature of the underlying obligation, and no longer only to payments made in the context of a sale or the provision of services. The underlying obligation may now therefore be of a contractual or extra-contractual nature.

The restriction also applies to **donations** other than those between natural persons acting outside their professional capacity and, in particular, to donations made to non-profit associations or foundations.

##### b. *ratione personae*

The scope *ratione personae* of the restriction has also been expanded as Article 67 of the Anti-Money Laundering Law applies to all natural or legal persons, and no longer only to merchants and service providers.

##### c. Exemptions

The restriction provided for in Article 67, § 2, first paragraph, of the Law does not apply to:

- the sale of real property as referred to in Article 66 of the Anti-Money Laundering Law (see point 1 above);
- “transactions between consumers”;
- “the obliged entities referred to in Article 5, § 1, 1°, 3°, 4°, 6°, 7°, 10° and 16° [of the Anti-Money Laundering Law], as well as other natural [or legal] persons when they carry out transactions with these entities”. These entities are financial institutions for which cash transactions are considered inherent to their activities.

Without prejudice to the specific rules for transactions relating to the purchase of precious materials, particularly gold (see below), the above-mentioned general rule of restricting the use of cash therefore does not apply to cash transactions carried out by customers of:

- credit institutions governed by Belgian law, Belgian branches of European or non-European credit institutions, and credit institutions governed by the law of another Member State which rely on a tied agent established in Belgium to provide investment services and/or perform investment activities in Belgium;
- payment or electronic money institutions governed by Belgian law, Belgian branches of European or non-European payment or electronic money institutions, and payment or electronic money institutions governed by the law of another Member State that carry out their activities in Belgium through one or more persons who are established there and represent them there; and
- stockbroking firms governed by Belgian law, branches of European or non-European stockbroking firms in Belgium, and stockbroking firms governed by the law of another Member

State which rely on a tied agent established in Belgium to provide investment services and/or perform investment activities in Belgium.

Conversely, the restriction on cash transactions applies in particular to:

- life insurance companies governed by Belgian Law and branches of European or non-European life insurance companies in Belgium;
- settlement institutions and central securities depositories, and
- amutual guarantee societies.

### 2.1.2. Scope of the restriction

The limit of EUR 3 000 no longer applies to the amount of a price to be paid but rather to the amount of the sum that has been paid or donated in cash. For instance, a payment or donation of EUR 5 000 may be made and received in cash up to EUR 3 000 and the payment or donation of the remaining amount should be made and received otherwise.

However, the limit of EUR 3 000 remains applicable for “several transactions that seem to be related”. Related transactions are, for example, transactions presenting each of the following characteristics:

- they are carried out between the same parties;
- they have the same purpose or linked purposes (e.g. several works conducted by the same company for the same site, various consecutive donations to a non-profit association by the same person or by that person’s family members);
- they are close to each other in time.

Furthermore, transactions with the same characteristics that are split up for no reason should certainly also be considered as linked transactions. As in the past, splitting transactions may not lead to the restriction not being applied.

## 2.2 Specific rules for the sale of gold, copper cables, old metals and precious materials

The Anti-Money Laundering Law simplified and coordinated all provisions relating to the purchase of precious metals, copper cables or old metals. In such cases, subject to the exceptions provided for in the Law (particularly public auctions or purchases of old jewels from consumers), Article 67, § 2, second paragraph, of the Anti-Money Laundering Law prohibits any cash payment of the purchase price by a professional to a customer; conversely, the payment of the purchase price of the same goods by a consumer is subject to the general restriction described above.

It should be noted that all financial institutions falling under the supervisory powers of the NBB are subject to the specific prohibition described in Article 67, § 2, second and third paragraphs, of the Anti-Money Laundering Law when acting as the purchaser of gold or precious metals in particular. When acting as the seller of these same goods, the general limit of EUR 3 000 for cash payments applies if the financial institution does not belong to a category exempted from this restriction (see above).

For more information on this subject, see the Explanatory Memorandum of the Anti-Money Laundering Law.

## 3. Proof

The Anti-Money Laundering Law significantly changed the rules of evidence for cash payments. In short, it reversed the burden of proof in the matter by stipulating that, when the submitted accounting documents, including bank statements, cannot be used to determine how payments or donations have been made or received, they are presumed to have been carried out or received in cash. Furthermore, the burden of proof for tracing the payment was revised. For more information on this subject, see the Explanatory Memorandum of the Anti-Money Laundering Law.

## 4. Sanctions

The Anti-Money Laundering Law provides for a system of criminal sanctions and administrative settlements which can respectively be imposed or proposed by the FPS Economy in case of a breach of the provisions of the Law relating to the restriction of the use of cash. For more information on this subject, see the Explanatory Memorandum of the Anti-Money Laundering Law.

## 5. Internal procedures and control

Where relevant for the activities performed and without prejudice to the fact that the risk-based approach requires taking into account the ML/FT risks specifically associated with transactions involving large amounts of cash, the internal procedures of financial institutions should be established in such a manner as to guarantee compliance with the aforementioned rules restricting the use of cash. In particular:

- the internal procedures of a financial institution not benefiting from the exemption described in Article 67, § 2, fourth paragraph, 3°, of the Anti-Money Laundering Law should prevent customers from making cash payments exceeding the limit of EUR 3 000;
- the internal procedures of a financial institution purchasing/selling precious metals should prevent the purchase price of these precious metals being paid in cash, except in the extraordinary cases provided for in the Anti-Money Laundering Law.

The NBB moreover recommends having financial institutions' internal audit function verify whether they properly take into account the aforementioned rules relating to the restriction of the use of cash, both in the context of implementing their obligation to identify occasional customers and in the context of their ongoing due diligence obligation.

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



# Supervision by the NBB

Home > Financial oversight > Combating money laundering and the financing of terrori...

**Reporting by financial institutions**

**External whistleblowing**

**Supervisory powers and measures of the NBB**

**National cooperation**

**International cooperation**

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



# Reporting by financial institutions

Home > Financial oversight > Combating money laundering and the financing of terrori...

## Legal and regulatory framework

- Anti-Money Laundering Law: Article 91

## Explanatory Memorandum of the Anti-Money Laundering Law

- Article 91

## Comments and recommendations by the NBB

- Communication NBB\_2020\_002 of 23 January 2020 containing the conclusions of the horizontal analysis of a sample of summary tables of the overall assessment of the risks of money laundering and/or terrorist financing
- Comments and recommendations

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



# Anti-Money Laundering Law of 18 September 2017 - Article 91

## Art. 91

Without prejudice to the prerogatives granted to it to perform its other statutory supervisory tasks, the Bank can, for the purposes of exercising the supervisory powers conferred on it by or pursuant to this Law, request any information and any document, in any form, and in particular any information on the organisation, operation, situation and transactions of the obliged entities referred to in Article 5, § 1, 4° to 10°, including information about the relationship between an obliged entity and its customers.

The Bank can undertake on-site inspections and take cognizance of and copy, on the spot, any data and any document, file or record and have access to any computer system:

1° to verify compliance with the provisions of Book II of this Law and its implementing decrees and regulations, the implementing measures of Directive 2015/849, the European Regulation on transfers of funds and the due diligence requirements imposed by the binding provisions on financial embargoes;

2° to be able to verify the appropriate nature of the management structures, the administrative organisation, the internal control and the ML/FTP risk management policies.

The prerogatives referred to in the first and second subparagraphs also include access to the agendas and minutes of the meetings of the various bodies of the obliged entity and of their internal committees as well as to all associated documents and to the results of the internal and/or external opinions on the operation of the aforementioned bodies.

As part of its supervisory task and, in particular, of its inspections as referred to in the second paragraph, the Bank's staff are authorised to obtain any information and explanation from the managers and staff of the obliged entity that they deem necessary for the exercise of their tasks and can request meetings to this end with the managers or staff of the obliged entity they indicate.



# Explanatory Memorandum to the Anti-Money-Laundering Law of 18 September 2017 - Article 91

## Art. 91

Draft Article 91 lists the powers of the NBB for the exercise of this supervision.

These in particular include the power to:

- request any information and any document, in any form, and in particular any information on the organisation, operation, situation and transactions of the obliged entities, including information about the relationship between an obliged entity and its customers.
- undertake on-site inspections and take note of and copy, on site, any data and any document, file or record and have access to any computer system, in order:
  - to verify compliance with the legal and regulatory provisions, including the European regulations and regulatory technical standards as regards AML/CFT; and
  - to be able to verify the appropriate nature of the management structures, the administrative organisation, the internal control and the AML/CFT risk management policies.

In the same way as in the Banking Law, it is clarified that the access to information granted to the NBB for its supervision also includes access to the agendas and minutes of the meetings of the various bodies of the obliged entity and of their internal committees as well as to all associated documents, and to the results of the internal and/or external opinions on the operation of the aforementioned bodies.

When conducting on-site inspections, the members of staff of the NBB may collect any information and explanation that they deem necessary from the managers and staff during meetings with them.

In practice, the NBB applies the same method when exercising its supervisory powers as regards AML/CFT as that based on which it exercises its general prudential supervisory tasks, which consists of a combination of off-site supervision and on-site supervision (inspections).

Off-site supervision consists of collecting and examining a broad range of data to identify the risk profile of the financial institution concerned, and to determine the supervisory action to take, based on the risk profile. The information concerned relates both to the general characteristics of the financial institution (quality of the general governance and of the corporate culture, the type and nature of the activities, the quality of compliance and internal audit functions, etc.), and to aspects specifically related to AML/CFT (capacity of the function of the AMLCO, conformity of the procedures for AML/CFT with the legal and regulatory requirements, specific circumstances, etc.). This information may come from a wide variety of sources. It can for example be information obtained during the exercise of general prudential supervisory powers, information that the financial institution must provide periodically to the NBB (such as periodic reports or responses to periodic questionnaires) or following specific requests for information, or even information from external sources (for example information sent by the CTIF-CFI, by other Belgian or foreign authorities, public information, customer complaints, etc.).

In addition to the fact that “off-site” supervision may lead to actions vis-à-vis financial institutions to remedy any shortcomings established, this supervision also serves to identify financial institutions for which an on-site inspection may be advisable and to determine the purpose thereof.

These tasks are conducted by inspectors in accordance with a clear audit methodology that ties in with the methodology applied for general prudential supervision. They are not only intended for verifying, on-site, the compliance of internal procedures with legal and regulatory obligations but also the effective implementation of these internal procedures and their efficiency in preventing ML/TF transactions. In this respect, the inspectors conduct

inspections by taking random samples in files, which must enable them to determine, as objectively as possible, the level of effectivity and efficiency of the procedures and measures for AML/CFT laid down by the financial institutions. These spot checks in files do not, however, consist of a systematic and exhaustive search of all shortcomings that the institution concerned could be accused of as regards the preventive obligations. The inspections culminate in the drafting of a report, which formally sets out the flaws or shortcomings and lists the measures that the financial institution must take to remedy these. The inspection reports are regularly followed up to ensure that the financial institution has effectively taken the recommended measures by the established deadlines. Moreover, they constitute an especially important source of information for the exercise of off-site supervision.

# Reporting by financial institutions: Comments and recommendations

Home > Financial oversight > Combating money laundering and the financing of terrori...

## Contents

- 1. Overall risk assessment (business-wide risk assessment)
- 2. Periodic questionnaire
- 3. Activity report by the AMLCO
- 4. Exemption policy

## 1. Overall risk assessment (business-wide risk assessment)

### 1.1 Documents to be submitted

In order to meet their legal and regulatory obligations relating to the overall risk assessment (see the page devoted to this topic), financial institutions are required to complete and submit to the NBB the following two documents:

- The first document contains a summary table that provides a global overview of the overall risk assessment carried out by the institution. The NBB specified its expectations regarding the content of the summary table of the overall risk assessment in its Communication NBB\_2020\_002 of 23 January 2020 containing the conclusions of the horizontal analysis of a sample of summary tables of the overall assessment of the risks of money laundering and/or terrorist financing (see points 1.2. and 1.3. below).
- The second document contains a number of specific questions relating to the way in which the overall risk assessment process has been conducted.

These documents are available in English, French and Dutch.

For any questions regarding these documents, the NBB's AML/CFT supervisory team can be contacted at the following e-mail address: [supervision.ta.aml@nbb.be](mailto:supervision.ta.aml@nbb.be).

### 1.2 Distinction between the overall risk assessment and the reporting of results to the NBB

As indicated in its Communication NBB\_2020\_002 of 23 January 2020, the NBB found that it would be useful to specify its expectations regarding the **content of the summary table** which was to be submitted to it by the financial institutions by 15 July 2018 and which will have to be resubmitted in case of future updates of the overall risk assessment:

- the risk identification phase: the NBB expects the summary table to include *all* significant activities of the financial institution, as well as the inherent risk attributed by the financial institution to each of these activities (i.e. also the description of the inherent risks considered "Low" by the financial institution). Thus, the financial institution demonstrates that all of its activities have been subject to a risk analysis;
- in contrast, the summary table may differ from the overall risk assessment itself **with regard to the inherent risks that the financial institution has assessed as "Low"**, in the sense that the table must **not include**

**the management measures taken for these risks or the level of residual risk attached to each inherent risk identified as “Low”** (gap analysis phase);

- as a result, the summary table must **also not list the actions to be taken** for these inherent risks assessed as “Low” by the financial institution (action plan).

In its Communication NBB\_2020\_002, the NBB also specified that the model in Annex 1 to Circular NBB\_2018\_02 of 24 January 2018 on the overall assessment of money laundering and terrorist financing risks was provided **as an example** to the financial institutions for drafting the overall risk assessment summary table or even the overall risk assessment itself. The columns included in this model list the absolute minimum of information to be reported to the NBB with regard to the overall risk assessment. However, there is nothing to prevent the financial institutions from adding other columns with regard to the risk identification phase including, for example, the risk scenarios (in what ways can the risk materialise?) or an assessment of the residual risk.

Finally, the NBB specified in this Communication that, by submitting a summary table, financial institutions are not exempted from documenting the process of the overall risk assessment itself and from making this documentation available to the NBB in its capacity as AML/CFT supervisory authority (that can always request this documentation when needed) .

### 1.3 Deadlines for submission and updating

When implementing the overall risk assessment process for the first time after the entry into force of the Anti-Money Laundering Law, institutions were requested to provide the NBB with a first version of both documents by 1 April 2018 at the latest. This first version, which was primarily intended to allow the NBB to monitor the timely progress of the assessment work, had to reflect the state of progress of the overall risk assessment on that date.

The final version of these documents, which had to reflect the full and finalised risk assessment, in accordance with the provisions of Articles 16 and 17 of the Anti-Money Laundering Law, was to be submitted to the NBB by 15 July 2018 at the latest.

**Starting from its own risk classification**, the NBB carried out a **horizontal analysis** and an assessment of a substantial number of overall risk assessment **summary tables** and the related questionnaires. On the basis of the analyses performed, the NBB also generated a number of **more general findings**. It specified these findings, as well as several **(non exhaustive) resulting transversal expectations and recommendations** in its Communication NBB\_2020\_002 of 23 January 2020.

In this Communication, it moreover indicated that **each AMLCO should, with the support of his senior officer responsible for AML/CFT, review the overall risk assessment of his financial institution in light of this Communication**, identify any improvements and/or updates to be made and perform the improvements and/or updates required. The conclusions of this review should be communicated to the NBB in the AMLCO's next annual activity report (to be submitted by 30 June through eCorporate). Where appropriate, the updated **overall risk assessment summary table** should also be submitted to the NBB (either also through eCorporate or by e-mail for financial institutions that do not have access to eCorporate).

More in general, it should finally be recalled that the overall risk assessment process is a continuous exercise and that the NBB will continue to monitor this process afterwards. Therefore, institutions are asked to **update the aforementioned documents each time the overall risk assessment is adjusted**, and, if necessary, to **submit the new updated version of the summary table to the NBB simultaneously with a copy of the AMLCO's annual activity report**, as referred to in Article 7 of the Anti-Money Laundering Regulation of the NBB (see below) **and with the periodic questionnaire**.

### 1.4 Transmission channel

Institutions that have access to eCorporate should submit the completed documents through this application. Institutions that do not have access to eCorporate should send the completed documents to the following e-mail address: supervision.ta.aml@nbb.be.

## 2. Periodic questionnaire

Through this questionnaire, the NBB seeks to obtain standardised information from the financial institutions in order to implement its risk-based approach in exercising its legal supervisory powers in the field of AML/CFT (see the page "Supervisory powers and measures available to the NBB"). This information relates to the inherent ML/FT risks to which the financial institutions are exposed, on the one hand, and to the quality of the risk management measures taken by them on the other hand. On the basis of both assessments, the residual ML/FT risk and the supervisory priorities can then be determined for each institution. Each financial institution is expected to send the the completed periodic questionnaire to the NBB in accordance with the following rules.

## 2.1 Documents to be submitted

For each category of institutions subject to supervision by the NBB, separate questionnaires are available, which – to the extent possible – take into account the specific activities performed in the different sectors. A total of four different questionnaires were prepared for the following categories of institutions: (i) credit institutions, (ii) stockbroking firms, (iii) life insurance companies and (iv) payment institutions and electronic money institutions. Settlement institutions should answer the questionnaire for credit institutions:

- Credit institutions
- Life insurance companies
- Stockbroking firms
- Payment institutions and electronic money institutions
- Indicative list of countries presenting a higher risk of money laundering or terrorist financing (Annex 1 to the above-mentioned questionnaires)

All questionnaires are available in English, French and Dutch.

For any questions regarding these questionnaires, the NBB's AML/CFT supervisory team can be contacted at the following e-mail address: [supervision.ta.aml@nbb.be](mailto:supervision.ta.aml@nbb.be).

## 2.2. Frequency and deadline for submission

In order to be able to regularly update its classification of financial institutions according to the ML/FT risks associated with them, the NBB invites these institutions to reply **annually** to the said periodic questionnaire, of which a new version is established each year and made available under point 2.1 above.

Replies should be sent to the NBB through OneGate **by 30 June of each year**. The electronic form in which the requested information must be provided is available in OneGate **from 1 May of the previous year**.

## 2.3 Transmission channel

The financial institutions should submit their answers to the periodic questionnaire through OneGate, where it will be available in electronic form. The NBB automatically receives the information provided by each institution as soon as the electronic form is closed and sent.

In order to guarantee the safety of the information provided, each institution must have an electronic certificate to access the OneGate application. These certificates can be obtained from various external service providers (inter alia *Globalsign*, *Isabel* and/or *Quo Vadis*). Institutions that do not have a Belgian CBE number can exceptionally request to be exempted from using an electronic certificate by sending an e-mail to [supervision.ta.aml@nbb.be](mailto:supervision.ta.aml@nbb.be). If the requested exemption is granted, the institution concerned is granted a login and password to access the OneGate application in order to reply to the periodic questionnaire.

More information about the OneGate application and how to access it can be found under the following link: [www.nbb.be/onegate](http://www.nbb.be/onegate).

## 2.4 Procedure for answering the questionnaire

### a) Answering the questions

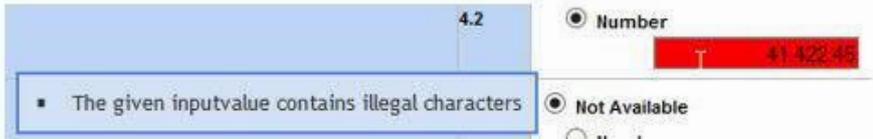
In the electronic form that will be available in OneGate, each financial institution should provide the necessary information by selecting in the drop-down menu, for each question, the answer that best suits its organisation (e.g. 'yes', 'no' or 'not applicable').

Where numerical information is requested, the responding institution usually has the choice between the options 'not available' or 'digit'. If the institution does not have the statistical information required to provide a reliable answer to a question, the option 'not available' should be chosen. If the institution does have the required information, the option 'digit' must be chosen and the correct figure must be entered. Finally, if the question is not relevant to the responding institution, the option 'digit' must be chosen and '0' must be entered.

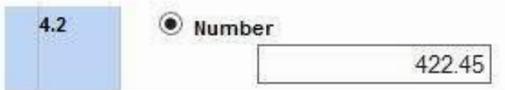
**Please note:**

Numbers should always be entered without points or commas to separate the thousands. Points may only be used as a decimal separator. If the number is not entered in the correct format, an error message will appear and it will not be possible to close the form.

- Example error message:



- Correct format:



## b) Reference date for answering the questions

As regards the reference date for answering the questions, the following distinction must be made.

The questions aimed at obtaining statistical information in principle always mention the date or period to which the information requested should relate. In almost all cases, the information requested should (i) relate to the situation on 31 December of the previous calendar year (e.g. number of customers as at 31 December 20XX), (ii) or relate to the previous calendar year (e.g. number of payments made to high-risk countries in 20XX).

As regards the qualitative questions, which are aimed, for example, at verifying compliance of the internal procedures with the legislation in force, or which concern the checks, if any, performed by a financial institution, the information provided by the responding institution should always relate to the **situation as at 31 December of the previous calendar year**.

## c) Responsibility for the accuracy of the answers

The answers to the questionnaire should be submitted to the NBB under the ultimate responsibility of the responding financial institution's senior management.

It should also be noted that the AMLCO appointed within each financial institution in accordance with Article 9, § 2, of the Anti-Money Laundering Law is, pursuant to the same legal provision, primarily tasked not only with analysing atypical transactions in order to determine whether these transactions should be considered suspicious and be notified to the CTIF-CFI, but also with implementing the policies and procedures referred to in Article 8 of the Law, particularly the internal control measures and procedures which are necessary to ensure compliance with the Law and which are covered in the questionnaire. Article 9 of the Law also provides that this person responsible should ensure, in general, that the institution fulfils all its obligations with regard to AML/CFT and, more in particular, that an adequate administrative organisation and adequate internal control measures are set up, as required pursuant to Article 8 of the Law. The AMLCO should also have the power to propose, on his own initiative, all necessary or useful measures in this regard to the senior management of the institution, including the release of the necessary resources (see the page « Governance »).

The NBB therefore expects the financial institution's senior management to decide which answers should be given

to the questionnaire, on the proposal of the AMLCO.

In the context of specific control actions or on-site inspections, the NBB will not fail to verify the accuracy and quality of the answers provided by the institutions.

## 3. Activity report by the AMLCO

### 3.1 Document to be submitted

Article 7 of the Anti-Money Laundering Regulation of the NBB requires the AMLCO to establish an activity report and send it to the management committee (or to the senior management if there is no management committee) and to the board of directors at least once a year.

This report is an important document for the management bodies, as it allows them to properly perform their tasks. This report is specific for AML/CFT, as the nature of the subject requires specific treatment, although it is also important from a prudential point of view (from a compliance function perspective). The expected content of this report is set out on the "Governance" page.

Each financial institution is expected to send a copy of the aforementioned activity report to the NBB in accordance with the following rules.

### 3.2 Deadline for submission

The copy of the AMLCO's activity report should be sent to the NBB **no later than 30 June of the year following the year to which it relates**. Life insurance companies, however, should respect the reporting dates laid down in the e-Corporate circular.

### 3.3 Transmission channel

Institutions that have access to eCorporate should submit a copy of the activity report through this application. Institutions that do not have access to eCorporate should send the completed documents to the following e-mail address: [supervision.ta.aml@nbb.be](mailto:supervision.ta.aml@nbb.be).

## 4. Exemption policy

### 4.1 Context

Using the reportings mentioned above (overall risk assessment, periodic questionnaire and activity report by the AMLCO), the NBB collects standardised information relating to, on the one hand, the ML/FT risks facing supervised institutions and, on the other, the measures adopted by these financial institutions to manage those risks. The information collected by the NBB enables it to monitor, by applying a risk-based approach, the correct implementation of the anti-money laundering legislation by the financial institutions.

However, the aforementioned reporting obligations also place an administrative burden on the financial institutions, which have to collect the information requested and submit it to the NBB using the various reporting instruments. The NBB therefore ensures that the reporting obligations and burden are at all times proportionate to the objectives pursued.

The NBB has found that the administrative burden caused by these reportings cannot be considered reasonable for all financial institutions, particularly not for some institutions which fall within the scope *ratione personae* of the Anti-Money Laundering Law and are therefore also subject to the NBB's supervision but do not conduct activities in Belgium or are only exposed to a very limited extent to ML/FT risks in Belgium. In this respect, see the examples included in the point on the principle of proportionality on the page "Governance".

The NBB considers that such financial institutions can submit a request to be exempted from the reportings referred to in *1. Overall risk assessment* and *2. Periodic questionnaire*.

## 4.2 Procedure

Financial institutions that consider themselves eligible for an exemption from the various reporting obligations and have not yet obtained an exemption from the NBB should submit a motivated request for this purpose to the NBB (by e-mail to [supervision.ta.aml@nbb.be](mailto:supervision.ta.aml@nbb.be)). This request should at least contain:

- a description of the institution's business model;
- a description of the reasons for setting up the Belgian establishment;
- a general description of the exact functions and tasks conferred upon the Belgian establishment;
- a more specific description of the functions and tasks to be performed by the Belgian establishment in the context of the implementation of the institution's AML/CFT policies and procedures.

If the information requested has already been submitted to the NBB as part of the registration of the Belgian establishment on the NBB's official lists, a simple reference to the information already provided may suffice.

## 4.3 Consequences

If the NBB approves the exemption request, the financial institution will receive confirmation from the NBB that it is exempted, in principle for an indeterminate period of time, from submitting the reportings referred to above in *1. Overall risk assessment* and *2. Periodic questionnaire*.

The institution concerned should, however, confirm annually that the circumstances which led to the granting of an exemption (e.g. the institution's business model and the tasks and functions conferred upon the Belgian establishment) have remained unchanged. This statement should be submitted to the NBB in accordance with the arrangements for submitting the AMLCO's annual activity report, which in such cases can be limited to a confirmation that the conditions for benefiting from the exemption are still being met, that there have been no developments that could lead to the Belgian establishment being exposed to new ML/FT risks, and that as a result, the exemption previously granted by the NBB remains fully justified, without any changes, taking into account the principle of proportionality.

Additionally, the institution's AMLCO should always notify the NBB spontaneously and without delay of any plans by the institution to change the Belgian establishment's business model, enabling the NBB to analyse these changes in the business plan in a timely fashion and to assess whether the previously granted exemption from the reportings mentioned above remain justified.

## 4.4 Scope of the exemption

The exemption granted on the basis of this chapter only results in the financial institution concerned not having to submit the reportings expected by the NBB. It therefore does not release the institution from all other obligations imposed on it by the Belgian anti-money laundering legislation and regulations. Where appropriate, however, the principle of proportionality can be applied in accordance with the relevant legal and regulatory requirements (see in this context "Organisation and internal control in financial institutions"). Nevertheless, there can be no derogation from the AMLCO's obligation to draw up an activity report at least once a year and submit it to the management committee (or the institution's senior management if it does not have a management committee) and the board of directors, in accordance with Article 7 of the Anti-Money Laundering Regulation of the NBB, and to provide the NBB with a copy. However, as indicated above, the content of this annual activity report can be limited to a description of the specific functioning of the Belgian establishment.

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



# Business-wide ML/TF risk assessment

[Home](#) > [Financial oversight](#) > [Combating money laundering and the financing of terrori...](#)

- [Overview](#)
- [Example](#)
- [Questionnaire](#)



# Periodic questionnaire

[Home](#) > [Financial oversight](#) > [Combating money laundering and the financing of terrori...](#)

- [Credit institutions](#)
- [Life insurance companies](#)
- [Stockbroking firms](#)
- [Payment institutions and electronic money institutions](#)
- [Indicative list of countries presenting a higher risk of money laundering or terrorist financing \(Annex 1 to the above-mentioned questionnaires\)](#)



# External whistleblowing

Home > Financial oversight > Combating money laundering and the financing of terrori...

## Legal and regulatory framework

- Anti-Money Laundering Law: Article 90

## Explanatory Memorandum of the Anti-Money Laundering Law

- Article 90

## Comments and recommendations by the NBB

- Comments and recommendations

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



# Anti-Money Laundering Law of 18 September 2017 - Article 90

## Art. 90

The supervisory authorities shall set up efficient and reliable mechanisms for the reporting, by the obliged entity's managers, staff members, agents and distributors or by third parties, to these authorities of supposed or actual breaches of the provisions of this law, its implementing decrees and regulations, the implementing measures of Directive 2015/849, the European Regulation on transfers of funds and the due diligence requirements laid down in the mandatory provisions on financial embargoes.

The mechanisms referred to in the first subparagraph shall include specific procedures for the receipt of reports on breaches and their follow-up.

The supervisory authority may not inform the obliged entity or third parties of the identity of the person who submitted the report.

No civil, criminal or disciplinary proceedings may be brought against and no professional sanction may be imposed on the staff member or representative of the obliged entity who submitted a report to the supervisory authority in good faith because of the fact that he/she submitted the aforementioned report. This protection shall also apply if the report submitted in good faith mentions information that is or should have been included in a notification of a suspicious transaction.

Any adverse or discriminatory treatment of this person, as well as any termination of this person's employment at or representation of the entity because of the reporting, is prohibited.

[The provisions of this Article are without prejudice to the application of special provisions regarding the reporting of breaches to a supervisory authority.]

*Sixth subparagraph inserted by Article 116 of the Law of 30 July 2018 – Belgian Official Gazette of 10 August 2018*



# Explanatory Memorandum to the Anti-Money-Laundering Law of 18 September 2017 - Article 90

## Art. 90

Article 90 of the draft Law transposes Article 61 of Directive 2015/849. It introduces an obligation for all supervisory authorities referred to in draft Article 85 to set up efficient and reliable mechanisms for reporting, by the obliged entity's managers, members of staff, agents and distributors or by third parties, of supposed or actual breaches by an obliged entity of its obligations for the prevention of ML/TF.

To ensure the efficiency of these mechanisms, the draft provision guarantees the anonymity of the person who makes such a report, vis-à-vis both the obliged entity and third parties.

The provision also guarantees exemption for this person from civil, criminal or disciplinary liability and protects this person from professional sanctions ensuing from submitting such a report to a supervisory authority, on the condition that it was done in good faith. Under the same condition, the draft Law clarifies that this person may not be inconvenienced for having communicated information to the supervisory authority in the context of reporting a suspicious transaction. This provision supplements the exception to the prohibition of informing third parties that a report was made to the CTIF-CFI. This exception, included in Article 56, § 1 of the draft Law, also applies in the context of the reporting mechanism introduced by Article 90 of the draft Law.

Finally, it is clarified that an obliged entity that is aware that the report it is the subject of comes from a member of its staff or one of its agents or distributors, is prohibited from giving this person adverse or discriminatory treatment within the employment relationship or, a fortiori, from terminating this relationship.



# External whistleblowing: Comments and recommendations by the NBB

Home > Financial oversight > Combating money laundering and the financing of terrori...

## Contents

- 1. Scope ratione personae
- 2. Object of reporting a breach
- 3. Protection of the person reporting the breach
- 4. Action taken on the report
- 5. Processing of personal data

Besides the internal warning system for AML/CFTP that financial institutions should set up pursuant to Article 10 of the Anti-Money Laundering Law to allow their staff members, agents and, in the case of electronic money institutions, distributors, to inform the AMLCO and the senior officer responsible for AML/CFTP, through a specific, independent and anonymous channel, of any breaches of the Anti-Money Laundering Law (see the page "Internal whistleblowing" on this website), the NBB has also set up an external whistleblowing system for reporting breaches of the Anti-Money Laundering Law and regulations.

The practical details of this reporting system are set out on the NBB's website under the heading "Report a breach". In this regard, the NBB recommends that financial institutions ensure that – as part of the training sessions to be organised pursuant to Article 11 of the Anti-Money Laundering Law – the NBB's external whistleblowing system is referenced in a written medium (e.g. a slide including a hyperlink to the appropriate section of the NBB's website).

It should be noted that this internal reporting system of the NBB is not specifically designed for reporting breaches of the Anti-Money Laundering Law and regulations, but that it has a more general scope, as it can also be used for breaches of the prudential legislation and regulations applicable to financial institutions that are subject to supervision by the NBB.

This web page, however, only focuses on breaches of the anti-money laundering legislation and regulations.

## 1. Scope ratione personae

The NBB's external whistleblowing system can be used by anyone wishing to notify the NBB of any potential or actual breach or violation of the provisions of the anti-money laundering legislation and regulations committed by financial institutions subject to the supervision of the NBB, as defined on the web page "Scope".

In practice, the external whistleblowing system is accessible inter alia to the staff members of a financial institution, its agents or subcontractors and to the intermediaries, agents and distributors whose services it makes use of.

## 2. Object of reporting a breach

In the context of AML/CFTP, the external whistleblowing system set up by the NBB can be used to report suspected or actual breaches of the following legal and regulatory texts:

- i. the Anti-Money Laundering Law,
- ii. the Anti-Money Laundering Regulation of the NBB,
- iii. the implementing measures of Directive 2015/849,
- iv. the European Regulation on transfers of funds, and
- v. the binding provisions relating to financial embargoes as defined in Article 4, 6° of the Anti-Money Laundering Law;

provided that these breaches have been committed by a financial institution that is subject to supervision by the NBB or by its managers, staff members, agents, subcontractors or distributors.

### 3. Protection of the person reporting the breach

Article 36/7/1 of the Law of 22 February 1998 establishing the Organic Statute of the NBB prohibits any civil, penal or disciplinary proceedings, any professional sanctions and any unfavourable or discriminatory treatment, and any termination of the employment contract of the whistleblower because of his having reported a breach. The Bank may impose an administrative sanction on any financial institution that violates this prohibition.

The NBB will use the information supplied in the breach report exclusively for the purpose of performing its legal tasks. That information is subject to the rules on professional secrecy laid down in the Law of 22 February 1998 establishing the Organic Statute of the National Bank of Belgium. The protection of the person reporting the breach and of the person accused in this report is therefore guaranteed.

If the person reporting a breach is subject to adverse or discriminatory action, he/she may file a new external report to inform the NBB.

### 4. Action taken on the report

In carrying out its task to monitor AML/CFTP prevention mechanisms, the NBB analyses the information which it receives and takes the action that it deems appropriate.

Since the NBB and the persons involved in the performance of its supervisory tasks are bound by professional secrecy, the person reporting the breach cannot be informed of the action taken on the information received.

### 5. Processing of personal data

The name and contact details of the person reporting a breach of the anti-money laundering legislation or regulations are registered by the NBB. The NBB processes these data solely for the purpose of the investigation triggered by the report and in accordance with the current regulations on the processing of personal data. The NBB treats these data as confidential. However, the NBB cannot rule out the possibility that in certain circumstances, owing to a statutory obligation, these personal data must be disclosed to other persons, in which case the person concerned will be notified in advance.

The data relating to the persons accused in a report are likewise treated in accordance with the current legislation on personal data protection.

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



# Supervisory powers and measures of the NBB

Home > Financial oversight > Combating money laundering and the financing of terrori...

## Legal and regulatory framework

- Anti-Money Laundering Law: Articles 7 and 85 to 98

## Explanatory Memorandum of the Anti-Money Laundering Law

- Articles 7 and 85 to 98

## Other reference documents

- Guidelines of 7 April 2017 on risk-based supervision
- FATF Guidance dated 23 October 2015 for a Risk-Based Approach: Effective Supervision and Enforcement by AML/CFT Supervisors of the Financial Sector and Law Enforcement

## Comments and recommendations by the NBB

- Comments and recommendations

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



# Anti-Money Laundering Law of 18 September 2017 - Articles 7 and 85 to 98

## Art. 7

Unless otherwise stipulated, the competent authorities and the obliged entities, in accordance with the provisions of this Law, shall implement the preventive measures referred to in Book II, in a differentiated manner, according to their ML/TF risk assessment.

## Art. 85

§ 1. Without prejudice to the prerogatives granted to them by or pursuant to other legal provisions, the following authorities shall monitor compliance with the provisions of Book II of this Law, its implementing decrees and regulations, the implementing measures of Directive 2015/849, the European Regulation on transfers of funds, and the due diligence requirements laid down in the mandatory provisions on financial embargoes:

1° the Minister of Finance, through his representative referred to in Article 22 of the Law of 22 February 1998 establishing the organic statute of the National Bank of Belgium, with regard to the latter;

2° the Administration of Treasury with regard to the obliged [entity] referred to in Article 5, § 1, [...] 3°; § 1, 2° modified by Article 115 of the Law of 30 July 2018 – Belgian Official Gazette of 10 August 2018

3° the National Bank of Belgium, hereinafter called “the Bank”, with regard to the obliged entities referred to in Article 5, § 1, 4° to 10°[, including for the activities carried out by these entities in the capacity of lenders within the meaning of Article I.9, 34° of the Code of Economic Law];

*§ 1, 3° modified by Article 102, 1° of the Law of 2 May 2019 – Belgian Official Gazette of 21 May 2019*

4° the Financial Services and Markets Authority, hereinafter called “the FSMA”, with regard to the obliged entities referred to in Article 5, § 1, 11° to 20°[, excluding lenders within the meaning of Article I.9, 34° of the Code of Economic Law, which fall within the supervisory competence of the National Bank of Belgium pursuant to 3°];

*§ 1, 4° modified by Article 102, 2° of the Law of 2 May 2019 – Belgian Official Gazette of 21 May 2019*

5° the Federal Public Service Economy, SMEs, Self-Employed and Energy with regard to the obliged entities referred to in Article 5, § 1, 21°, and 29° to 31°;

6° the Supervisory Board of Auditors with regard to the obliged entities referred to in Article 5, § 1, 23°;

7° the Institute of Tax Accountants and Tax Consultants with regard to the obliged entities referred to in Article 5, § 1, 24°;

8° the Institute of Accounting professionals and Tax Experts with regard to the obliged entities referred to in Article 5, § 1, 25°;

9° the National Chamber of Notaries with regard to the obliged entities referred to in Article 5, § 1, 26°;

10° the National Association of Bailiffs with regard to the obliged entities referred to in Article 5, § 1, 27°;

11° the President of the Bar Association to which they belong with regard to the obliged entities referred to in Article

5, § 1, 28°;

12° the Federal Public Service Home Affairs with regard to the obliged entities referred to in Article 5, § 1, 32°;

13° the Gaming Commission with regard to the obliged entities referred to in Article 5, § 1, 33°;

§ 2. The King shall designate the authorities that are competent to monitor, without prejudice to the prerogatives granted to them by or pursuant to other legal provisions, compliance with the provisions referred to in § 1 by the entities to which He, where appropriate, extends the scope of all or part of the provisions of Book II of this Law pursuant to Article 5, § 1, 22°, and § 4.

§ 3. Without prejudice to the prerogatives granted to them in paragraph 1 and by or pursuant to other legal provisions, the following authorities shall monitor compliance with the provisions of Book III:

1° with respect to the provisions of Article 66, § 2, first subparagraph and of Article 67: the Federal Public Service Economy, SMEs, Self-Employed and Energy;

2° with respect to the provisions of Article 66, § 2, second and third subparagraph:

a) the National Chamber of Notaries with regard to the obliged entities referred to in Article 5, § 1, 26°;

b) the Federal Public Service Economy, SMEs, Self-Employed and Energy with regard to the obliged entities referred to in Article 5, § 1, 30°.

## Art. 86

§ 1. Supervisory authorities or, where appropriate, authorities designated by other laws may issue regulations that apply to the obliged entities under their competence and that complete the provisions of Books II and III and their implementing decrees on a technical level, taking into account the national risk assessment referred to in Article 68.

Where appropriate, the regulations referred to in the first subparagraph shall only take effect after their approval by the King.

If the supervisory authorities or, where appropriate, the other authorities referred to in the first subparagraph fail to issue the regulations referred to in the first subparagraph or fail to amend them in the future, the King shall be empowered to issue these regulations Himself or to amend them.

§ 2. Depending on what they deem necessary for an effective application of the provisions referred to in Article 85, § 1, the supervisory authorities shall:

1° send circulars, recommendations or other forms of communication to the obliged entities in order to clarify the scope of the obligations arising from the aforementioned provisions for these entities;

2° take measures to raise the obliged entities' awareness of ML/FT risks; and

3° take measures to inform the obliged entities of the developments in the legal AML/CFTP framework.

## Art. 87

§ 1. The supervisory authorities shall exercise their supervision based on a risk assessment. To that end, they shall ensure that they:

1° have a clear understanding of the ML/FT risks present in Belgium, based on relevant information concerning national and international risks, including the report drawn up by the European Commission pursuant to Article 6(1) of Directive 2015/849 and on the national risk assessment referred to in Article 68;

2° base the frequency and intensity of on-site and off-site supervision on the obliged entities' risk profile.

The risk profile referred to in the first subparagraph, 2°, shall be the result of the combination of:

1° an assessment of the level of the ML/FT risks to which the obliged entity is exposed, taking into account in particular the characteristics of its sector of activity, its customers, the products and services offered by it, the geographic areas where it conducts its business and its distribution channels, on the one hand; and

2° an assessment of the management of these risks, including in particular an assessment of the measures it has taken to identify and reduce these risks and an assessment of its level of compliance with the applicable legal and regulatory obligations, on the other hand.

The supervisory authorities shall ensure that they possess relevant information on the obliged entities that is necessary to establish their risk profile.

The obliged entities' risk profile shall be reviewed by the supervisory authority:

1° periodically, with a frequency that has been adapted to take into account in particular the characteristics of the sector of activity and the risk profile previously attributed to the obliged entity; and

2° when important events occur that could affect the level of the ML/FT risks to which the obliged entity is exposed or the management of these risks by the obliged entity.

§ 2. When exercising their supervisory powers, the supervisory authorities shall take into account the risk assessment discretion left to the obliged entities pursuant to this Law. To that end, they shall examine the relevance of the overall risk assessment conducted by the obliged entities in accordance with Article 16 and shall take into account the risk factors listed in Annexes II and III.

## Art. 88

In the cases referred to in Article 13, § 3, third subparagraph, where the additional measures imposed by the obliged entity on the establishment operated by it in the third country concerned are not sufficient to efficiently manage the ML/FT risk, the supervisory authority competent pursuant to Article 85 may require that the group does not establish a business relationship or that it ends the relationship and does not perform any transactions. If necessary, the supervisory authority shall demand that the establishment in the third country concerned be closed.

## Art. 89

§ 1. Except for the case where they are called upon to testify in criminal proceedings, the supervisory authorities referred to in Article 85, § 1, 2°, the members and former members of their bodies and their staff who are involved in exercising the supervision laid down in this Law, or the persons designated for that purpose shall be bound by professional secrecy and may not disclose confidential information they became aware of in exercising their supervisory powers pursuant to this Law to any person or authority.

Except for the case where they are called upon to testify in criminal proceedings, the supervisory authority referred to in Article 85, § 1, 5°, the members and former members of its staff who are involved in exercising the supervision laid down in this Law, or the persons designated for that purpose shall be bound by professional secrecy and may not disclose confidential information they have received from another supervisory authority in the context of exercising their supervisory powers pursuant to this Law to any person or authority.

§ 2. Paragraph 1 is without prejudice to the disclosure of confidential or secret information to third parties in the cases laid down in the Law.

§ 3. The supervisory authorities referred to in paragraph 1 and the members or former members of their bodies and their staff shall be exempt of the obligation laid down in Article 29 of the Code of Criminal Procedure.

§ 4. Breaches of this Article shall be punished by the penalties laid down in Article 458 of the Penal Code. They shall be subject to the provisions of Book 1 of the Penal Code, including Chapter VII and Article 85.

## Art. 90

The supervisory authorities shall set up efficient and reliable mechanisms for the reporting, by the obliged entity's managers, staff members, agents and distributors or by third parties, to these authorities of supposed or actual breaches of the provisions of this law, its implementing decrees and regulations, the implementing measures of Directive 2015/849, the European Regulation on transfers of funds and the due diligence requirements laid down in the mandatory provisions on financial embargoes.

The mechanisms referred to in the first subparagraph shall include specific procedures for the receipt of reports on breaches and their follow-up.

The supervisory authority may not inform the obliged entity or third parties of the identity of the person who submitted the report.

No civil, criminal or disciplinary proceedings may be brought against and no professional sanction may be imposed on the staff member or representative of the obliged entity who submitted a report to the supervisory authority in good faith because of the fact that he/she submitted the aforementioned report. This protection shall also apply if the report submitted in good faith mentions information that is or should have been included in a notification of a suspicious transaction.

Any adverse or discriminatory treatment of this person, as well as any termination of this person's employment at or representation of the entity because of the reporting, is prohibited.

[The provisions of this Article are without prejudice to the application of special provisions regarding the reporting of breaches to a supervisory authority.]

*Sixth subparagraph inserted by Article 116 of the Law of 30 July 2018 – Belgian Official Gazette of 10 August 2018*

## Art. 91

Without prejudice to the prerogatives granted to it to perform its other statutory supervisory tasks, the Bank can, for the purposes of exercising the supervisory powers conferred on it by or pursuant to this Law, request any information and any document, in any form, and in particular any information on the organisation, operation, situation and transactions of the obliged entities referred to in Article 5, § 1, 4° to 10°, including information about the relationship between an obliged entity and its customers.

The Bank can undertake on-site inspections and take cognizance of and copy, on the spot, any data and any document, file or record and have access to any computer system:

1° to verify compliance with the provisions of Book II of this Law and its implementing decrees and regulations, the implementing measures of Directive 2015/849, the European Regulation on transfers of funds and the due diligence requirements imposed by the binding provisions on financial embargoes;

2° to be able to verify the appropriate nature of the management structures, the administrative organisation, the internal control and the ML/FTP risk management policies.

The prerogatives referred to in the first and second subparagraphs also include access to the agendas and minutes of the meetings of the various bodies of the obliged entity and of their internal committees as well as to all associated documents and to the results of the internal and/or external opinions on the operation of the aforementioned bodies.

As part of its supervisory task and, in particular, of its inspections as referred to in the second paragraph, the Bank's staff are authorised to obtain any information and explanation from the managers and staff of the obliged entity that they deem necessary for the exercise of their tasks and can request meetings to this end with the managers or staff of the obliged entity they indicate.

## Art. 92

Relations between the obliged entity and a particular customer do not come under the powers of the Bank unless the supervision of the obliged entity so requires.

## Art. 93

§ 1. Without prejudice to the other measures prescribed by this Law or by other legal or regulatory provisions, the Bank may order an obliged entity as referred to in Article 5, § 1, 4° to 10°, by a deadline it determines:

1° to comply with specific provisions of Book II of this Law, its implementing decrees and regulations, the implementing measures of Directive 2015/849, the European Regulation on transfers of funds and the due diligence requirements imposed by the binding provisions on financial embargoes;

2° to make the necessary adjustments to its management structures, its administrative organisation, its internal control and its ML/FTP risk management policies; or

3° to replace the persons referred to in Article 9.

§ 2. Without prejudice to the other measures prescribed by this Law or by other legal or regulatory provisions, where the obliged entity to which an order has been issued pursuant to paragraph 1, fails to comply with this order on the deadline set, and provided that the obliged entity has been able to defend its case, the Bank can:

1° publish the infringements found and the fact that the obliged entity has not complied with the order issued to it;

2° impose a penalty on it which may not be less than EUR 250 nor more than EUR 50 000 per calendar day nor, in total, more than EUR 2 500 000.

The penalties imposed pursuant to the first subparagraph shall be collected by the administration of FPS Finance which is responsible for collecting and recovering non-fiscal debts, in accordance with Article 3 et seq. of the Law on State Property of 22 December 1949.

## Art. 94

Without prejudice to the other measures prescribed by this Law or by other legal or regulatory provisions and by the prerogatives granted to the Bank to perform its other statutory supervisory tasks, where it finds that on the deadline set pursuant to Article 93, § 1, the situation has not been remedied, the Bank can:

1° appoint a special commissioner.

In such a case, the written, generic or specific authorisation of the special commissioner is required for all the actions and decisions of all the bodies of the obliged entity including its general meeting, and for the actions of the persons responsible for its management; the Bank may however limit the scope of the operations subject to the authorisation.

The special commissioner may submit any proposal he considers appropriate to all bodies of the obliged entity, including the general meeting.

The members of the management and governing bodies and the persons responsible for management who carry out actions or make decisions without having received the necessary authorisation from the special commissioner shall be jointly and severally liable for any loss arising therefrom incurred by the obliged entity or by a third party.

If the Bank has published the name of the special commissioner in the Belgian Official Gazette and has specified the actions and decisions that are subject to his authorisation, any actions or decisions made without the required authorisation shall be null and void unless ratified by the special commissioner.

Under the same conditions, any decision of the general meeting which has been made without the necessary authorisation of the special commissioner shall be null and void unless ratified by the special commissioner.

The remuneration of the special commissioner shall be set by the Bank and paid by the obliged entity.

The Bank may appoint a deputy commissioner;

2° order the replacement of all or part of the members of the statutory governing body of the obliged entity by a deadline it determines and, where no replacement occurs by this deadline, appoint one or more provisional managers or administrators to replace the management and governing bodies as a whole of the obliged entity, who alone or collegially, depending on the case, shall have the powers of the persons replaced. The Bank shall publish its decision in the Belgian Official Gazette.

With the authorisation of the Bank, the provisional manager(s) or administrator(s) may call a general meeting and draw up the agenda thereof.

The Bank may request, in accordance with the methods it determines, that the provisional manager(s) or administrator(s) provide a report on the measures taken in connection with their task.

The remuneration of the provisional manager(s) or administrator(s) shall be determined by the Bank and borne by the obliged entity.

The Bank may, at any time, replace the provisional manager(s) or administrator(s), either ex officio, or at the request of the majority of the shareholders or members if they can prove that the management by the parties concerned no longer offers the necessary guarantees;

3° suspend, for a period to be determined by the Bank, the direct or indirect exercise of all or part of the obliged entity's business or prohibit such business; such suspension may, to the extent determined by the Bank, imply the total or partial suspension of pending contracts.

The members of the management and governing bodies and the persons responsible for management who carry out actions or make decisions in violation of the suspension or prohibition order shall be jointly and severally liable for any loss arising therefrom incurred by the obliged entity or by a third party.

If the Bank has published the suspension or prohibition order in the Belgian Official Gazette, any actions or decisions contravening it shall be null and void;

4° withdraw the authorisation.

In the case of obliged entities which are credit institutions, the decision to withdraw the authorisation shall be taken in accordance with Council Regulation (EU) No 1024/2013 of 15 October 2013 conferring specific tasks on the European Central Bank concerning policies relating to the prudential supervision of credit institutions;

In urgent cases, the Bank may take the measures referred to in the first paragraph without previously issuing an order, provided that the obliged entity has been able to defend its case.

## Art. 95

Where the Bank finds that an obliged entity as referred to in Article 5, § 1, 6° d) or 7° e), has committed in Belgium a serious breach of the provisions of Book II of this Law, its implementing decrees and regulations, the implementing measures of Directive 2015/849, the European Regulation on transfers of funds or the due diligence requirements imposed by the binding provisions on financial embargoes, the measures referred to in Article 94, 3°, include the power to prohibit the obliged entity from providing services in Belgium through one or more agents or distributors in Belgium designated by the Bank.

## Art. 96

When adopting measures pursuant to Article 93, § 2, 2°, the Bank shall take account inter alia of:

- 1° the gravity and the duration of the breaches;
- 2° the financial strength of the obliged entity involved, as indicated in particular by its total turnover;
- 3° any benefits or profits derived from the breaches by the obliged entity involved, insofar as they can be determined;
- 4° the losses to third parties caused by the breaches, insofar as they can be determined;
- 5° the level of cooperation of the obliged entity involved with the Bank;
- 6° any previous breaches by the obliged entity involved.

## Art. 97

The Bank shall inform the ESA's of the measures it has taken pursuant to Articles 93, 94, 2° and 4°, and 95, and of any appeal in relation thereto and of the outcome thereof.

## Art. 98

Where the Bank, in the context of its supervisory task and in particular of its inspections as referred to in Article 91, second subparagraph, identifies a breach of the provisions of Article 66, § 2, first subparagraph, or of Article 67, it shall notify the Federal Public Service Economy, SMEs, Self-employed and Energy as soon as possible.

# Explanatory Memorandum to the Anti-Money-Laundering Law of 18 September 2017 - Articles 7 and 85 to 98

## Art. 7

As already specified above (see the general explanation above), one of the most important developments, both in the FATF Recommendations and in the European regulatory framework, is that it is emphasised more expressly and more generally than before that a risk-based approach should be used as the cornerstone for the mechanisms to prevent ML/TF, and not only by the obliged entities but also by the competent authorities. This development is as a consequence reflected in the present draft Law too, transposing Directive 2015/849, and in particular:

- as regards the definition of the national policy on AML/CFT, by formalising a national risk assessment (see Book IV, Title 1, below), which must be based on the Supranational Risk Assessment conducted by the European Commission, in accordance with Article 6 of the Directive;
- as regards preventive measures taken by the obliged entities, by conducting a two-tier risk assessment, in particular:
  - a general assessment of the risks to which the obliged entities are exposed, based on the nature of their activities, the characteristics of the customers they deal with, and the characteristics of the channels through which these customer relations occur, etc. (cf. Book II, Title 2, below). This assessment must allow them in particular to establish policies and procedures for AML/CFT which are in proportion to and differentiated on the basis of the risks;
  - assessment of the risks associated with each client, which will determine the level of intensity of the due diligence measures that must be taken on a case-by-case basis (cf. Article 19, § 2, below).
- as regards the exercise of supervision by the competent authorities on compliance by the obliged entities with the obligations pertaining to AML/CFT, by defining a risk-assessment-based supervisory model per obliged entity that falls under their supervision (cf. Article 87, below).

The goal of this general application of a risk-based approach is to promote optimal allocation of the resources available for AML/CFT at all levels and to make prevention as effective as possible.

It should also be emphasised that, although the risk-based approach is applied for a very large proportion of the mechanisms for AML/CFT provided for by this draft Law, for certain aspects of these mechanisms, a more traditional approach is nevertheless followed based on compliance with the rules (“rules-based approach”). This applies for example to the obligation to report information to the CTIF-CFI (cf. Book II, Title 4, Chapter 2, below).

It should also be noted that this risk-based approach does not extend to the provisions of other laws or to European regulations that are also relevant based on the intended objectives of this draft Law, and that are based exclusively on the rules-based principle. This applies in particular for application of the European Funds Transfer Regulation or the binding provisions on financial embargos, as defined in draft Article 4, 5° and 6° (see below).

## Art. 85

Draft Article 85, §§ 1 and 2 attributes to the various authorities listed therein the responsibility of exercising the supervisory powers as regards the various categories of obliged entities (listed in draft Article 5). These provisions, which transpose Article 48, paragraphs 1 and 9 of Directive 2015/849, fit in with Article 39, § 1, first paragraph, of the

Law of 11 January 1993, and make no material changes to the attribution of powers provided for in this Article. To avoid doubts as to the competent authority for a particular category of obliged entities, it seemed preferable to opt, as part of § 1 of this draft Article, for a nominative and exhaustive indication of all authorities concerned, while the Law of 11 January 1993 designates some of these in generic terms (i.e.: the oversight, supervisory or disciplinary authorities of the undertakings and persons concerned (...)).

This new technique to designate the competent supervisory authorities shows, more clearly than in the past, that certain undertakings or persons, especially those that exercise their activities in the financial sector, may simultaneously fall under the supervisory powers of several authorities where they belong to different categories of obliged entities as listed in Article 5.

With the exception of bpost, which is only subject to the draft law as regards its activities regarding financial postal services and the issue of electronic money (cf. Article 5, § 1, 3°), the undertakings and persons that belong to the other categories of entities listed in Article 5 are subject to the provisions of the present draft Law for all their professional activities. That is also the case under the Law of 11 January 1993. This is justified by the fact that the mechanisms for AML/CFT implemented within the same obliged entity can only be effective if they show consistency throughout the various activities it exercises.

This means that the obliged entities may fall, for the entirety of their activities, under competing supervisory powers of different authorities.

As such, for example an insurance company that may exercise life insurance activities as referred to in Article 5, § 1, 5°, falls under the supervisory powers of the NBB pursuant to § 1, 4° of the present draft Article. If the same undertaking also additionally exercises mortgage-lending activities as referred to in Article 5, § 1, 20°, it falls, as such, under the supervisory powers of the FSMA.

Every authority that exercises supervisory powers on a particular entity must be able to take into account the entire organisation of that entity, without thereby being obstructed in the exercise of its powers by limitations associated with the activities exercised, which would fall under the powers of another authority.

Nevertheless, in order to guarantee a coherent approach to supervision and the optimal application of the resources allocated by those authorities to the exercise of their powers as regards AML/CFT, as well as to avoid overlap in supervision, those authorities must establish appropriate mechanisms between them for cooperation and sharing of information in accordance with the provisions of draft Article 121, § 1.

Taking into account the powers of the King under Article 5, § 1, 22° and § 4 to extend the scope of all or part of the draft Article to new categories of obliged entities, and taking into account the need to subject these new categories to the supervision of an authority to guarantee the effectiveness of this extension, draft Article 85, § 2 provides that the King will, in case of extension of the scope of the Law, designate the authority competent for the supervision of the new categories of obliged entities.

As regards the restrictions on cash payments, § 3, point 1° gives general supervisory powers to the FPS Economy, SMEs, Self-Employed and Energy. It should be emphasised that this power is limited to the supervision of cash payments. As regards the other obligations arising from this draft Law, the FPS Economy, SMEs, Self-Employed and Energy only has powers vis-à-vis the obliged entities referred to in Article 5, § 1, 21° and 29° to 31° (see Article 85, § 1, 5° of the draft Law).

Pursuant to Article 85, § 3, 2°, the FPS Economy is competent for the supervision of compliance with the provisions of Article 66, § 2, second and third paragraphs by the obliged entities referred to in draft Article 5, § 1, 30° (estate agents), whilst the National Chamber of Notaries is tasked with the supervision of compliance of the aforementioned provisions of Article 66 by the obliged entities referred to in Article 5, § 1, 26° (notaries).

## Art. 86

The present draft Law, just like the Law of 11 January 1993, applies to obliged entities that exercise activities in very diverse sectors. With a view to effectively applying the prevention mechanisms required under this Law, taking this diversity into account, it is important for the aforementioned supervisory authorities to be able to supplement, on technical points, the provisions of Book II and III of the present draft Law and the Decrees that will be adopted for

the implementation thereof. Just as in Article 38, § 1 of the Law of 11 January 1993, taken over in this Article, draft Article 86, § 1, grants to these authorities the powers to draw up rules to this end (a power that must of course be exercised proportionately).

Where this is required by virtue of their legal status, the authorities concerned shall submit their rules for approval to the King, in which case the approval forms a prerequisite for the entry into force thereof.

As also specified in Article 38, § 1 of the Law of 11 January 1993, the King can take over from the authorities that fail to adopt such rules if He deems necessary.

§ 2 of the same draft Article moreover specifies that, with a view to the effective application of the legal and regulatory AML/CFT framework by the obliged entities for which they are competent, the supervisory authorities shall undertake initiatives (through awareness-raising campaigns) to improve these obliged entities' understanding of the ML/TF risks, and their knowledge and understanding of their legal and regulatory obligations as regards AML/CFT (by sending circulars or recommendations or by organising information sessions) as they deem necessary.

## Art. 87

Draft Article 87 lays down the rules that all competent authorities referred to in Article 85 must comply with as part of the exercise of their supervisory powers. It transposes Article 2, paragraph 9, Article 48, paragraphs 6 to 8, and Articles 16 and 18, paragraph 3 of Directive 2015/849.

While Article 39, § 1, second paragraph of the Law of 11 January 1993 offers the supervisory authorities the possibility of exercising their powers based on a risk assessment, the new draft Article 87, § 1, obliges them to make use of such a risk-based approach and describes the implications thereof.

In the first place, this supervisory approach requires the authorities concerned to acquire a good understanding of the ML/TF risks that exist in Belgium. For this, the authorities will need to use the Supranational Risk Assessment drawn up by the European Commission pursuant to Article 6, paragraph 1 of Directive 2015/849 and the national risk assessment referred to in Article 68 of the present draft Law as a basis. The authorities shall supplement this information where necessary with all other relevant information on national and international risks that they deem useful or necessary to obtain a better understanding of those risks.

The draft provision also clarifies that the risk-based supervision primarily consists of determining the frequency and intensity of both on-site and off-site supervision based on the risk profile of the obliged entities. This profile is derived both from an assessment of the ML/TF risks the obliged entity is exposed to, especially taking into account the characteristics of its activity sector, its clientele, the products and services it offers, the geographical zones where it exercises its activity, and its delivery channels, and an assessment of how these risks are managed, which in particular entails an assessment of the measures it has taken to identify and mitigate these risks, and an assessment of its level of compliance with the legal and regulatory obligations.

To be able to apply a profile to each obliged entity they supervise, the authorities concerned must ensure that they have relevant information for each of these entities, both in terms of the inherent risk to which they are exposed, and in terms of the quality and efficiency of the measures they take to manage and mitigate the risks.

When determining their risk-related supervision model, the NBB and the FSMA shall take into consideration the guidelines that will be published by the ESAs on the subject, in accordance with Article 48, paragraph 10 of Directive 2015/849. Although these guidelines do not apply to the other supervisory authorities referred to in Article 85, they can be used as a useful source of inspiration for them to define their own risk-based supervisory models.

§ 2 of the draft Article draws consequences from the fact that not only the supervisory authorities, but also the obliged entities under their supervision, must apply a risk-based approach. It is clarified that the supervision does not need to be exercised in such a way as for the supervisory authority to impose its own risk assessment on all obliged entities, but that it should take into account the fact that it is at the discretion of each obliged entity to assess its own risks, taking into account its own specific characteristics and its own situation. However, this provision of the draft Article emphasises the fact that an essential part of the supervision consists of ensuring that the general risk assessment referred to in draft Article 16, which each obliged entity must conduct and which must form the basis of the organisational measures it takes, is relevant and takes account of all the risk factors required. In this respect, it

should be noted that the obliged entities must be able, pursuant to Article 17, second paragraph of the draft Law, to demonstrate to their supervisory authorities that the policies, procedures and internal control measures they enforce are appropriate in view of the ML/TF risks they have identified as part of their risk assessment.

## Art. 88

Draft Article 88 concerns the case in which an obliged entity has set up a branch or subsidiary in a high-risk third country (within the meaning of draft Article 4, 9°), and in which the measures enforced by the Belgian parent undertaking on this branch or subsidiary are inadequate to sufficiently mitigate the ML/TF risks run by this latter, and consequently the whole group. In such a case, Article 88 grants the supervisory authority of the obliged entity that is the parent undertaking of the group concerned, the power to impose restrictions to the activities exercised in the branch or subsidiary, or even to put a stop to such activities. This provision transposes Article 45, paragraph 5, second sentence, of Directive 2015/849.

## Art. 89

Article 89 establishes the conditions required for efficient cooperation and sharing of information between the supervisory authorities which are competent, in particular, for the obliged entities from the financial sector. The legal status of the NBB and of the FSMA, as laid down respectively in the Law of 22 February 1998 establishing the Organic Statute of the National Bank of Belgium and in the Law of 2 August 2002 on the supervision of the financial sector and on financial services, imposes strict obligations of professional secrecy both to the members of their bodies and to their members of staff, entailing criminal sanctions (cf. in particular Articles 35 et seq. of the Law of 22 February 1998 establishing the Organic Statute of the National Bank of Belgium and 74 et seq. of the Law of 2 August 2002) arising from the European Directives that apply to them. To be able to derogate therefrom with a view to cooperating in the supervision of the obliged entities as regards AML/CFT, it is essential that the confidential information provided by the NBB and the FSMA to other national competent supervisory authorities (especially the FPS Finances and the FPS Economy) benefit within the receiving authority from the same level of protection against disclosure to third parties as it does within the sending authority. That is the purpose of this Article of the draft Law.

§ 1, first paragraph of the draft Article imposes the obligation of professional secrecy to the Federal Public Service Finance's General Administration of the Treasury, in its capacity as supervisory authority pursuant to Article 85 of this draft Law, as well as on its members of staff involved in the exercise of this supervisory power or on the persons appointed for this purpose, equal to that which the NBB and the FSMA, the members of their bodies and their members of staff are bound by.

The second paragraph of the same provision provides for a similar provision for the Federal Public Service Economy, SMEs, Middle Classes and Energy, where it acts as supervisory authority pursuant to Article 85, § 1, 5° of the present draft Law, for its members of staff involved in the exercise of this supervisory power or for the persons appointed thereto. Nevertheless, the professional secrecy obligation is in such a case limited to the confidential information they have received from another supervisory authority as part of the exercise of the supervisory powers by virtue of this draft Law.

Paragraphs 2, 3 and 4 of draft Article 89 regulate professional secrecy in the same way as in Articles 35, § 2, first indent, 1° and 35, § 1, second and third indents of the aforementioned Law of 22 February 1998, and Articles 74, second paragraph, 1° and 3°, in fine, and 87, § 2 of the aforementioned Law of 2 August 2002. Consequently, the professional secrecy described in § 1 does not stand in the way of the communication of confidential information to third parties in the cases established by and pursuant to the law; the authorities and persons bound by this professional secrecy are exempt from the obligation to report breaches contained in Article 29 of the Code of Criminal Procedure; and breaches of professional secrecy are punishable as determined in Article 458 of the Criminal Code.

## Art. 90

Article 90 of the draft Law transposes Article 61 of Directive 2015/849. It introduces an obligation for all supervisory authorities referred to in draft Article 85 to set up efficient and reliable mechanisms for reporting, by the obliged entity's managers, members of staff, agents and distributors or by third parties, of supposed or actual breaches by an obliged entity of its obligations for the prevention of ML/TF.

To ensure the efficiency of these mechanisms, the draft provision guarantees the anonymity of the person who makes such a report, vis-à-vis both the obliged entity and third parties.

The provision also guarantees exemption for this person from civil, criminal or disciplinary liability and protects this person from professional sanctions ensuing from submitting such a report to a supervisory authority, on the condition that it was done in good faith. Under the same condition, the draft Law clarifies that this person may not be inconvenienced for having communicated information to the supervisory authority in the context of reporting a suspicious transaction. This provision supplements the exception to the prohibition of informing third parties that a report was made to the CTIF-CFI. This exception, included in Article 56, § 1 of the draft Law, also applies in the context of the reporting mechanism introduced by Article 90 of the draft Law.

Finally, it is clarified that an obliged entity that is aware that the report it is the subject of comes from a member of its staff or one of its agents or distributors, is prohibited from giving this person adverse or discriminatory treatment within the employment relationship or, a fortiori, from terminating this relationship.

The Law of 11 January 1993, in Article 39, § 2, only very briefly describes the powers of the supervisory authorities for the exercise of their supervision, thereby relying on other legislation that defines the general supervisory powers and associated powers of those authorities. In contrast, the present draft Law opts, in the interest of greater transparency and legal certainty, to clarify the powers of each supervisory authority concerned for the exercise of its AML/CFT powers.

Such a clarification is particularly useful for the NBB.

Given that the supervisory powers granted to it in the area of AML/CFT by the present draft Law concern the majority of the financial institutions it is competent for from a prudential point-of-view, it is not advisable that the powers it must use to exercise this supervision should be drawn from a large number of distinct sectoral laws which may differ between them. The equal treatment of these obliged entities as regards supervision, irrespective of the category to which they belong, requires a single definition in this draft Law of the supervisory powers of the NBB vis-à-vis all obliged entities.

For the credit institution sector, the powers of the NBB for the exercise of its AML/CFT supervision must be described in specific terms, especially given that the general competence for the supervision of a considerable number of credit institutions subject to the present Law was transferred from the NBB to the European Central Bank (hereinafter the 'ECB') pursuant to the Single Supervisory Mechanism (hereinafter the 'SSM').

In Chapter 2 of Book IV, Title 4 of the present draft Law, an exhaustive list is given of the powers conferred on the NBB by law as part of the exercise of its supervisory powers in the area of AML/CFT. This is provided in an identical way vis-à-vis all obliged entities for which it is competent pursuant to draft Article 85, § 1, 3° of the aforementioned draft Law.

In order to draw up this list and at the same time to safeguard the overall supervision of the NBB, Articles 91 to 94 for the most part take over the provisions of the Law of 25 April 2014 on the legal status and supervision of credit institutions (hereinafter the 'Banking Law') and especially Articles 135, 136, 139, 236, 345 and 346, adjusting these provisions where necessary to the context of AML/CFT supervision.

## Art. 91

Draft Article 91 lists the powers of the NBB for the exercise of this supervision.

These in particular include the power to:

- request any information and any document, in any form, and in particular any information on the organisation, operation, situation and transactions of the obliged entities, including information about the relationship between an obliged entity and its customers.

- undertake on-site inspections and take note of and copy, on site, any data and any document, file or record and have access to any computer system, in order:
  - to verify compliance with the legal and regulatory provisions, including the European regulations and regulatory technical standards as regards AML/CFT; and
  - to be able to verify the appropriate nature of the management structures, the administrative organisation, the internal control and the AML/CFT risk management policies.

In the same way as in the Banking Law, it is clarified that the access to information granted to the NBB for its supervision also includes access to the agendas and minutes of the meetings of the various bodies of the obliged entity and of their internal committees as well as to all associated documents, and to the results of the internal and/or external opinions on the operation of the aforementioned bodies.

When conducting on-site inspections, the members of staff of the NBB may collect any information and explanation that they deem necessary from the managers and staff during meetings with them.

In practice, the NBB applies the same method when exercising its supervisory powers as regards AML/CFT as that based on which it exercises its general prudential supervisory tasks, which consists of a combination of off-site supervision and on-site supervision (inspections).

Off-site supervision consists of collecting and examining a broad range of data to identify the risk profile of the financial institution concerned, and to determine the supervisory action to take, based on the risk profile. The information concerned relates both to the general characteristics of the financial institution (quality of the general governance and of the corporate culture, the type and nature of the activities, the quality of compliance and internal audit functions, etc.), and to aspects specifically related to AML/CFT (capacity of the function of the AMLCO, conformity of the procedures for AML/CFT with the legal and regulatory requirements, specific circumstances, etc.). This information may come from a wide variety of sources. It can for example be information obtained during the exercise of general prudential supervisory powers, information that the financial institution must provide periodically to the NBB (such as periodic reports or responses to periodic questionnaires) or following specific requests for information, or even information from external sources (for example information sent by the CTIF-CFI, by other Belgian or foreign authorities, public information, customer complaints, etc.).

In addition to the fact that “off-site” supervision may lead to actions vis-à-vis financial institutions to remedy any shortcomings established, this supervision also serves to identify financial institutions for which an on-site inspection may be advisable and to determine the purpose thereof.

These tasks are conducted by inspectors in accordance with a clear audit methodology that ties in with the methodology applied for general prudential supervision. They are not only intended for verifying, on-site, the compliance of internal procedures with legal and regulatory obligations but also the effective implementation of these internal procedures and their efficiency in preventing ML/TF transactions. In this respect, the inspectors conduct inspections by taking random samples in files, which must enable them to determine, as objectively as possible, the level of effectivity and efficiency of the procedures and measures for AML/CFT laid down by the financial institutions. These spot checks in files do not, however, consist of a systematic and exhaustive search of all shortcomings that the institution concerned could be accused of as regards the preventive obligations. The inspections culminate in the drafting of a report, which formally sets out the flaws or shortcomings and lists the measures that the financial institution must take to remedy these. The inspection reports are regularly followed up to ensure that the financial institution has effectively taken the recommended measures by the established deadlines. Moreover, they constitute an especially important source of information for the exercise of off-site supervision.

## Art. 92

It is important to emphasise that the NBB, in the exercise of its supervisory powers, pursues a general-interest goal, which does not consist of subjecting every transaction executed by an obliged entity to supervision, but rather to ascertain whether this entity has developed organisational measures and effectively applied them to enable it to comply with its legal and regulatory obligations and thereby contribute efficiently to AML/CFT. Draft Article 92 as a consequence clarifies that relations between the obliged entity and a particular customer do not come under the powers of the NBB. Nevertheless, when assessing the relevance, efficiency and effective application of the internal

procedures of the obliged entity, it is necessary to base such an investigation on a sample of transactions or client dossiers. This draft Article gives the NBB the power to take cognisance of dossiers and individual transactions of clients to the extent required for the supervision of the obliged entity.

## Art. 93

Where an obliged entity fails to take the measures recommended by the NBB as part of the exercise of its powers as regulated by Articles 91 and 92, Article 93, § 1 gives the NBB the power to increase the binding nature of its recommendations by imposing a deadline by which the obliged entity must take the measures imposed.

These measures can seek to guarantee that the obliged entity complies in particular with some of its AML/CFT obligations (Article 93, § 1, 1°) or offers solutions for the weaknesses and shortcomings identified in its management structures, administrative organisation, internal control and policy regarding the management of ML/TF risks (Article 93, § 1, 2°). Where it appears that the problems identified are linked with the manner in which the manager responsible and/or the AMLCO appointed pursuant to draft Article 9 discharges their responsibilities, the NBB can also order the obliged entity to replace this person by the deadline it determines (Article 93, § 1, 3°).

If the obliged entity that has received an order pursuant to § 1 remains in breach when the deadline has elapsed, the NBB may take additional measures to oblige it to comply with the order, as long as the obliged entity has been able to use its legal remedies. These can include the following measures, depending on what the NBB deems most efficient:

- publishing the infringements found and the fact that the obliged entity has not complied with the order issued to it; and/or
- imposing a penalty calculated per calendar day on which the imposed measures were not applied.

It should be noted that the penalties are intended to make the obliged entity remedy the situation of non-compliance rather than to stigmatise the institution and punish a current or past breach. The penalties are equally not intended to be equivalent to administrative sanctions pursuant to this draft Law as is the case in other financial legislation, namely the Banking Law. Imposing penalties comes under the competence of the NBB's Board of Directors and not of the Sanctions Committee. This does not mean that there are no procedural guarantees attached to the adoption thereof. The general principles of administrative law offer the obliged entities the necessary procedural guarantees. Furthermore, 36/22 of the Law of 22 February 1998 establishing the Organic Statute of the National Bank of Belgium, which lays down that appeals against certain decisions of the NBB may be lodged with the Council of State via an accelerated procedure, is supplemented by a separate (bicameral) draft Law entailing that such an appeal may be lodged against all enforcement action taken by the NBB pursuant to draft Article 93 and against all other administrative measures it may take pursuant to Articles 94 and 95.

The amount of the penalties that may be imposed therefore lies between EUR 250 and EUR 50 000 per calendar day and may not come to more than EUR 2 500 000 in total.

The penalties imposed pursuant to the first paragraph are collected by the Treasury.

## Art. 94

Article 94 also lists the administrative measures that the NBB may impose over and above — or instead of — the publication of the shortcoming or the enforcement of penalties pursuant to Article 93, § 2, on an obliged entity that has not heeded an order imposed pursuant to Article 93, § 1 by the deadline given.

These administrative measures, which are comparable to the measures provided for under Article 236 of the Banking Law, are not penalties. Equally, they neither intend to nor result in establishing the culpability of the obliged entity or punishing it, but rather aim to ensure that the obliged entity will in the future participate effectively in AML/CFT and to protect society and the financial sector from these criminal phenomena.

The preparatory work for the Banking Law (Parliamentary documents, Chamber of Representatives, 2013-2014, Doc 53 3406/001, p.192) states the following in this respect: “Because of their preventive nature, these administrative measures come under the task of the administrative police, which is inherent to the action of the supervisory authority. The name ‘administrative measures’ does not mean that these measures can be taken with no procedural guarantees for those concerned. Given that the measures specified are based on legal actions of the active administration, they clearly have to adhere to the general principles of administrative law to which the supervisory authority is subject as an administrative authority. This includes the adversarial debate, the principle of impartiality, the right to be heard and compliance with the principle of proportionality. (see A. Dirxx, “La CBFA, les infractions à la législation financière et la sanction par les amendes administratives”, in *Le droit pénal financier en marche/Het financieel strafrecht in opmars*, AEDBF, Anthemis, 2009, p. 273, 5 to 7)”.

The administrative measures listed and explained in draft Article 94 are the following:

- appointing a special commissioner, whose written authorisation is required for all the actions and decisions of all the bodies of the obliged entity, or for some of its actions and decisions, with the right to take the initiative to present to these bodies any proposal he or she deems useful;
- ordering the replacement of all or part of the members of the statutory governing body of the obliged entity and, in the absence of a replacement by the deadline, appointing one or more provisional managers or administrators to replace the management and governing bodies as a whole of the obliged entity.
- suspending, for a particular period of time, the direct or indirect exercise of all or part of the obliged entity's business or prohibiting such business; and
- withdrawing the authorisation of the obliged entity. For obliged entities that are credit institutions, the decision to withdraw the authorisation is made in accordance with Council Regulation (EU) No 1024/2013 of 15 October 2013 conferring specific tasks on the European Central Bank concerning policies relating to the prudential supervision of credit institutions. Specifically, the NBB will send the ECB a proposal for a decision in this respect.

It should be noted that Articles 93 and 94 transpose Article 59, paragraph 2, a) to d) of Directive 2015/849 as regards the powers of the NBB but extends the range of measures which the NBB may use compared to the minimum required by the Directive.

## Art. 95

Article 95, which transposes Article 48, paragraph 4, second sentence of Directive 2015/849, refers to the specific case in which administrative measures are imposed on payment institutions or electronic money institutions governed by the law of another Member State and which exercise their activities on the Belgian territory via agents or distributors established in Belgium. In that case, the measure to restrict or prohibit activities, as referred to in draft Article 94, 3°, entails that the NBB has the power to prohibit the use of one or more agents or distributors established in Belgium that it designates.

## Art. 96

Draft Article 96 gives a non-exhaustive list of the criteria that must be taken into account when determining the penalty referred to in Article 93, § 2, 2° to guarantee its proportionality. These criteria, which are laid down in Article 60, paragraph 4 of Directive 2015/849, relate to the gravity and duration of the breach which the penalty seeks to end, to the degree with which the obliged entity cooperates with the NBB, to any previous breaches, to the financial strength of the obliged entity and, where applicable, insofar as this can be determined, to the benefit or profit derived by the obliged entity from the breach, as well as to the loss that third parties have suffered from this breach.

## Art. 97

Article 97 transposes, as regards the obliged entities that come under the competency of the NBB, Article 62, paragraph 1 of Directive 2015/849, which provides that all administrative measures imposed to obliged entities from the financial sector must be notified to the ESAs. This communication shall, where applicable, be made by the ECB in the case of the withdrawal of an authorisation that comes under its competencies.

## Art. 98

The specific role of supervising compliance with the provisions of Article 66, § 2, first paragraph, or of Article 67 of the draft Law, which relate to the restriction of the use of cash, is reserved to the FPS Economy (cf. draft Article 85, § 3). However, this provision entails that, if in the exercise of its supervisory powers the NBB establishes that these provisions are not complied with, it must inform the FPS Economy thereof. The NBB must inform the FPS Economy on the breaches identified but not investigate them, contrary to the latter.

# Supervisory powers and measures of the NBB: Comments and recommendations by the NBB

Home > Financial oversight > Combating money laundering and the financing of terrori...

## Contents

- 1. Role of the NBB in AML/CFT
- 2. Supervisory powers and measures of the NBB
- 3. Organisation of AML/CFT supervision within the NBB

## 1. Role of the NBB in AML/CFT

The provisions governing the NBB's competence in AML/CFT are laid down in Articles 85 to 98 of the Anti-Money Laundering law.

Pursuant to this Law, the NBB is responsible in particular for monitoring compliance by financial institutions (as defined on this website) with their European and national obligations relating to the fight against money laundering and terrorist financing (AML/CFT), as well as with their obligations with regard to assets freezes and transfers of funds.

The NBB exercises off-site supervision (for example by examining the reportings received from financial institutions) and on-site controls.

The NBB's Sanctions Committee has the power to take disciplinary action. Where a financial institution violates a legislative or regulatory provision whose compliance is monitored by the NBB, it may be subject to one of the administrative sanctions laid down in the Anti-Money Laundering Law (see the page "Administrative Sanctions").

## 2. Supervisory powers and measures of the NBB

The NBB's supervisory powers and measures in AML/CFT are specified in Articles 91 to 98 of the Anti-Money Laundering Law. In accordance with these provisions, the NBB may:

- "request any information and any document", in any form whatsoever, and in particular any information on the organisation, operation, situation and transactions of the financial institutions (including information about the relationships between a financial institution and its customers, to the extent necessary for exercising its supervision);  
The NBB uses this power in particular to require financial institutions subject to its supervision to provide it with the information and reports detailed on the page "Reporting by financial institutions".
- conduct on-site inspections and take cognizance of and copy, on the spot, any data and any document, file or record, and have access to any computer system to verify compliance with the law and to verify the appropriate nature of the management structures, the administrative organisation, the internal control and the ML/FT risk management policies;
- order a financial institution to comply with the provisions of Book II of the Anti-Money Laundering Law, to make the necessary adjustments, to replace certain persons so that its management structures, internal organisation and policies/procedures and processes are in line with the NBB's expectations. The NBB may,

where a financial institution fails to comply with its order by the deadline set and provided that the financial institution has been able to defend its case:

- publish the infringements found and the fact that the obliged entity has not complied with the order issued to it;
- impose a penalty payment on it which may not be less than EUR 250 nor more than EUR 50 000 per calendar day, nor, in total, more than EUR 2 500 000.

Finally, if the NBB finds that the situation has not been remedied by the deadline it has set, the law provides for a gradual system of measures that can be taken: appointment of a special commissioner in addition to the management bodies, replacement of the statutory governing body, temporary suspension of all or part of the business, withdrawal of the authorisation and prohibition on providing services in Belgium.

In order to ensure the consistency between AML/CFT supervision and general prudential supervision, the provisions of the Anti-Money Laundering Law conferring supervisory and enforcement powers on the NBB have been aligned with the corresponding provisions of the prudential laws.

### 3. Organisation of AML/CFT supervision within the NBB

Since January 2016, AML/CFT supervision is organised around two teams:

- a specialised team ("the AML/CFT Group"), whose purpose is mainly:
  - to perform the tasks related to the development, with the assistance of the legal service, of the AML/CFT supervisory policy, and
  - to exercise off-site supervision of all financial institutions subject to supervision (cross-sectoral competence); and
- the inspection services, which remain responsible for the on-site AML/CFT controls.

In carrying out its tasks, the AML/CFT Group works closely together with the NBB services responsible for general prudential supervision, in order to maintain the overall consistency of the supervisory actions with regard to each of the financial institutions subject to supervision.



## National cooperation

[Home](#) > [Financial oversight](#) > [Combating money laundering and the financing of terrori...](#)

### Legal and regulatory framework

- [Anti-Money Laundering Law: Article 121](#)

### Explanatory Memorandum of the Anti-Money Laundering Law

- [Article 121](#)

### Other reference documents

- [General Memorandum of Understanding of 14 March 2013 for collaboration between the NBB and the FSMA to ensure the coordination of the supervision of the institutions under their respective supervision](#)
- [Protocol of 17 September 2019 defining the modalities of cooperation and information exchange between the NBB and CTIF-CFI](#)

### Comments and recommendations by the NBB

- [Comments and recommendations](#)



# Anti-Money Laundering Law of 18 September 2017 - Article 121

## Art. 121

§ 1. The supervisory authorities shall cooperate and exchange all useful information whenever necessary for the exercise of the supervisory powers conferred on them by or pursuant to this Law, in particular with respect to obliged entities which simultaneously fall within the competence of several of them and with respect to obliged entities that are part of a group comprising subsidiaries or branches that fall within the competence of several of them.

§ 2. The CTIF-CFI and the supervisory authorities referred to in Title 4 shall cooperate and exchange all useful information whenever necessary for the exercise of the powers conferred on them by or pursuant to this Law.

§ 3. For the purposes of this Article, the obligation of professional secrecy to which the supervisory authorities concerned and the CTIF-CFI are subject, is waived.



# Explanatory Memorandum to the Anti-Money-Laundering Law of 18 September 2017 - Article 121

## Art. 121

National cooperation is covered in Article 49 of Directive 2015/849, which lays down that the Member States must ensure that national authorities have effective mechanisms to enable them to cooperate and coordinate, especially concerning national risk assessments and the establishment of the national policy regarding AML/CFT (referred to in Article 7 of the Directive).

National cooperation in the area of the national risk assessment and of the policy on AML/CFT that takes place between the competent authorities, within the national coordinating bodies, is regulated in Title 1 of Book IV of the draft Law (Articles 68 to 72).

It does however seem useful to provide for an express obligation of cooperation between the supervisory authorities, especially because of the potential overlap of their supervisory areas, particularly when this concerns authorities that supervise obliged entities that are financial institutions (see the comment in draft Article 85).

Paragraph 1 of draft Article 121, which imposes on supervisory authorities the obligation of cooperating and sharing information, will in practice only relate to the supervisory authorities in the financial sector, although the obligation is worded more broadly to apply to all supervisory authorities.

The information that the supervisory authorities referred to could share, with a view to applying the provisions of the present draft Law, can be of any nature whatsoever, including information of a prudential nature. Certain information can after all be relevant both as part of prudential supervision and as part of AML/CFT (for example to assess the 'fit & proper' nature of the shareholders and managers, the quality of the internal control system or the compliance function).

The second paragraph of the draft Article moreover sets out that the CTIF-CFI and the supervisory authorities must cooperate and mutually share all information they might possess and that could be useful for the exercise of their respective powers as regards AML/CFT (especially the supervisory and sanctioning powers of the authorities referred to in Title 4).

Given that the supervisory authorities are obliged to cooperate, an express derogation must be provided for from the professional secrecy to which these supervisory authorities are bound, as part of the exercise of their task of supervising compliance with the provisions of this law (cf. draft Article 89) or in another capacity, namely as prudential supervisor of the financial institutions (cf. Article 35 of the Law of 22 February 1998 establishing the Organic Statute of the National Bank of Belgium for the latter). To facilitate cooperation between the CTIF-CFI and the supervisory authorities, the professional secrecy to which these authorities are bound pursuant to Articles 83, § 1 or 89 of the draft Law, or to another legislation, must also be lifted. Consequently, § 3 of draft Article 121 expressly provides for an exception to these professional secrecy obligations to remove any legislative obstacle to cooperation.



# National cooperation: Comments and recommendations by the NBB

Home > Financial oversight > Combating money laundering and the financing of terrori...

The national cooperation and exchange of information between Belgian supervisory authorities with competence in the field of AML/CFT have their legal basis in Article 121 of the Anti-Money Laundering Law. All Belgian supervisory authorities are henceforth bound by a legal obligation of professional secrecy equivalent to the obligation that applies to the NBB, thereby removing all legal barriers to the exchange of confidential information required for exercising supervision.

In practice, the NBB cooperates with the following Belgian authorities:

1. the CTIF;
2. the FSMA;
3. the FPS Finance (Treasury);
4. the FPS Economy.

The cooperation with the FSMA, the FPS Finance (Treasury) and the FPS Economy is particularly important for ensuring the overall coherence of supervisory actions when multiple financial institutions belonging to the same group fall within the competences of different supervisory authorities or when a single financial institution falls under the supervisory competences of two authorities simultaneously. In the context of this cooperation, authorities should exchange all information useful for exercising their respective supervisory powers, particularly as regards:

- the governance and organisational arrangements of the financial institutions concerned and the assessment thereof by the authorities;
- the policies, procedures and internal control of these financial institutions and the assessment thereof by the authorities;
- the information provided by the financial institutions, particularly as part of the ad hoc or periodic reportings required by these authorities;
- these authorities' assessment of the ML/FT risks associated with these financial institutions;
- the authorities' findings concerning these financial institutions' compliance with AML/CFT obligations;
- the supervisory actions envisaged or performed by these authorities, the results thereof and the decisions that could be taken on that basis;
- etc.

This cooperation could also lead to coordinated or even joint control actions. For instance, representatives of the FSMA, of the FPS Finance (Treasury) or of the FPS Economy could, where relevant, be involved in on-site AML/CFT inspections carried out by the NBB's services, or vice versa. This cooperation is without prejudice, however, to the legal supervisory powers respectively conferred upon each of these authorities with regard to the financial institutions concerned.

The NBB's cooperation with CTIF-CFI is different from that with the other three aforementioned Belgian authorities in that CTIF-CFI's tasks are of a different nature than those assigned to the NBB. As a "financial information unit", CTIF-CFI does not exercise supervision of the obliged financial institutions and therefore does not necessarily have accurate information e.g. on financial institutions' governance, organisation, internal procedures, etc. However, since CTIF-CFI receives reportings of suspicions from financial institutions, it could be alerted by the atypical reporting behaviour of certain institutions (e.g. systematically late reportings of suspicions or systematically late replies to CTIF-CFI's requests for information, regularly deficient and incomplete reportings, reportings that are not based on suspicions, etc). Such information is inherently useful for the exercise of the NBB's supervisory powers.

To ensure that such information is communicated to the supervisory authorities whenever useful, on the one hand, Article 83, § 2, 3°, of the Anti-Money Laundering Law lifts the professional secrecy legally imposed on CTIF-CFI to enable it to provide the supervisory authorities with all information useful to them for exercising their supervisory and sanctioning powers. On the other hand, Article 121, § 3, of the Anti-Money Laundering Law creates a duty of cooperation between CTIF-CFI and the Belgian supervisory authorities, in particular the NBB, and stipulates that they should cooperate and exchange all useful information whenever necessary for the exercise of the powers conferred upon them by or pursuant to the Law.

Such a cooperation and exchange of confidential information with all Belgian authorities concerned can be implemented case by case based on the provisions of the Law whenever this is deemed necessary by one of these authorities. However, in order to concretely and efficiently organise this national cooperation and these exchanges of information and, where appropriate, to determine the minimum frequency of these exchanges, the authorities concerned may consider it appropriate to specify the terms in Memorandums of Understanding (MoUs). Thus far, the NBB has signed MoUs with the FSMA (see the General Memorandum of Understanding for collaboration of 14 March 2013) and with CTIF-CFI (see the Protocol defining the modalities of cooperation and information exchange of 17 September 2019).

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



## International cooperation

Home > Financial oversight > Combating money laundering and the financing of terrori...

### Legal and regulatory framework

- Anti-Money Laundering Law: Articles 129 to 131

### Explanatory Memorandum of the Anti-Money Laundering Law

- Articles 129 to 131

### Other reference documents

- Multilateral agreement on the practical modalities for exchange of information between the ECB and the National Competent Authorities (signed by the NBB on 11 January 2019)

### Comments and recommendations by the NBB

- Comments and recommendations

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



# Anti-Money Laundering Law of 18 September 2017 - Articles 129 to 131

## Art. 129

For the purpose of this Chapter, the following definitions shall apply:

- 1° “Belgian supervisory authorities”: the authorities referred to in Article 85;
- 2° “Belgian obliged entities”: the entities referred to in Article 5, §§ 1 and 4.

## Art. 130

§ 1. In order to exercise effectively the supervisory powers set out in Title 4 in respect of Belgian obliged entities which are branches, subsidiaries or other forms of establishment of obliged entities subject to the law of another Member State or of a third country, the Belgian supervisory authorities shall cooperate and exchange all relevant information with the competent supervisory authorities of the Member State or third country concerned.

The Belgian supervisory authorities shall also cooperate and exchange all relevant information with the competent supervisory authorities of another Member State or of a third country which monitor compliance with the policies and procedures referred to in Article 45 (1) of Directive 2015/849, at the level of the group to which a Belgian obliged entity as referred to in the first paragraph belongs.

§ 2. In order to monitor compliance effectively with the provisions of Book II, Title 1, Chapter 2, the Belgian supervisory authorities shall cooperate and exchange all relevant information with the competent supervisory authorities of the Member States and third countries in which the group to which the Belgian obliged entity belongs has other establishments.

They shall cooperate and exchange, inter alia, all relevant information with a view to determining whether the conditions for the application of Article 43(2)(2) are met.

§ 3. Where the Bank intends to take a measure as referred to in Article 95, it shall notify the competent supervisory authority of the Member State to the law of which the obliged entity is subject and shall cooperate with a view to ensuring that the serious breaches detected are ended as soon as possible.

§ 4. The Belgian supervisory authorities shall communicate to the competent supervisory authorities of the Member States or third countries any information that would be relevant for the exercise by the latter of their power to impose sanctions and measures on the obliged entities that fall within their competence, in accordance with Articles 58 to 60 of Directive 2015/849 or equivalent provisions of their national legislation.

## Art. 131

Cooperation and exchanges of information covered by professional secrecy pursuant to Article 130 shall be subject to compliance with at least one of the following conditions:

1° the competent supervisory authority of the Member State or of the third country is subject, in accordance with the provisions of its national law, to a system of professional secrecy at least equivalent to that to which the Belgian supervisory authorities are subject;

2° the competent supervisory authority of the Member State or of the third country has signed a cooperation agreement with the Belgian supervisory authority which provides for:

a) reciprocity in the exchange of information;

b) the prohibition to use the disclosed information for purposes other than monitoring compliance by the group or the obliged entities which belong to it, with the AML/CFTP obligations or the prudential supervision thereof without the prior written authorisation of the communicating authority;

c) the prohibition to transmit the information received to any third party without the prior written authorisation of the communicating authority.

# Explanatory Memorandum of the Anti-Money Laundering Law of 18 September 2017 - Articles 129 to 131

## Art. 129 and 130

As already underlined, taking into account the transnational nature of ML/TF, international cooperation is extremely important, including between national supervisory authorities and their foreign equivalents. In Directive 2015/849, only some scattered provisions cover this aspect, sometimes in a very general way (cf. Article 48, § 5, which mentions the general principle of cooperation between competent authorities vis-à-vis obliged entities which form part of a group), and sometimes in very specific cases (cf. Articles 28 and 58, § 5, second paragraph). However, no provision among these organises the cooperation and sharing of information between supervisory authorities competent for AML/CFT, whether within the EEA or with equivalent authorities from third countries. The Law of 11 January 1993 does not include more. However, the need for an appropriate legal framework governing such cooperation is implicit in the application of the aforementioned provisions of the Directive and is a condition for the effectiveness of a mechanism for overseeing cross-border activity. In order to supplement the European system and to guarantee that sharing of information does not remain confined within national territories, the draft Law should therefore contain more detailed and broader rules on this subject.

It should be pointed out that the Directive is equally silent on the subject of sharing information between competent supervisory authorities on the subject of AML/CFT and competent authorities in prudential matters only, notably the ECB, which is not competent on the subject of AML/CFT under the SSM. In this matter, for a national supervisory authority competent on this subject, not being able to share confidential information with the ECB, the largest European prudential supervisory authority to date, is a major handicap for the prevention of ML/TF. Vice versa, too, it is a handicap for the ECB, which would not be able to systematically integrate the pertinent information on AML/CFT in its prudential supervision. However, this issue cannot be resolved at a national level: it can only be resolved by amending the EU legislation.

Draft Article 129 states two new definitions specific to the present section and with the sole aim of aiding readability and comprehension: they enable the supervisory authorities referred to in draft Article 85 to be easily distinguished from their foreign counterparts, as well as the obliged entities to which the draft Law applies, from obliged entities subject to foreign legislation.

Draft Article 130 transposes the aforementioned Article 48, § 5 of the Directive by splitting it up into the different cases that could occur based on the capacity of an obliged entity that forms part of a group and comes under the supervision of a Belgian supervisory authority. This particularly refers to the case of a financial institution among those referred to in Article 5, § 1, 4° to 21° which forms part of a group and is subject to the supervision of the NBB or the FSMA.

As a result, the first case provided for (§ 1) is that where the Belgian supervisory authority is competent for the “solo” supervision of a Belgian obliged entity that forms part of a group with its parent company established outside the Belgian territory (in another Member State of the EEA or in a third country). In application of the provision in the first draft paragraph, the Belgian authority is able to make use of the cooperation and will share all useful information with the supervisory authorities of the parent company with a view to exercising its “solo” supervisory competence of the Belgian obliged entity.

Under these same circumstances, the Belgian supervisory authority must offer its cooperation to the foreign supervisory authority competent for the parent company to enable it better to supervise the group policy it applies.

The second scenario referred to (§ 2) is that where the Belgian supervisory authority is competent for the supervision of the group policy because the obliged entity under its competence is the parent company of the group. In this case, the Belgian authority will ask, if necessary, for the cooperation of the supervisory authorities in the countries in which the group is based with a view to supervising the group policy.

In accordance with the provisions of Article 28 of the Directive, it will in particular cooperate with its foreign counterparts in order to ascertain, where applicable, that the Belgian obliged entity that calls on one of its subsidiaries or branches established in a high-risk third country as a third party business introducer complies with the conditions provided for to this effect with the aforementioned Article 28 of the Directive, transposed in Article 43 of the draft Law.

The following paragraph (§ 3) transposes Article 48, § 4, in fine, of the Directive and refers to the specific case of enforcement measures against payment and electronic money institutions governed by the law of another Member State and that act in Belgium through a network of agents or distributors. This concerns only the NBB which is competent for the obliged entities. It must notify and cooperate with the supervisory authority of the head office of the obliged entity concerned before adopting any measure of this nature.

Finally, the last paragraph (§ 4) of the draft Article transposes Article 58, § 5, second paragraph of the Directive which states that supervisory authorities must cooperate and coordinate their action in terms of imposing disciplinary measures and penalties.

## Art. 131

As regards the European supervisory authorities, and in particular the NBB, the implementation of the aforementioned provisions which especially transpose the general obligation of cooperation provided for under Article 48, § 5 of the Directive raises the issue of the legal exceptions to professional secrecy that should be provided for, taking into account the different status (for example the prudential supervisory authority or FIU) the various authorities may have in each State between which cooperation and therefore sharing of information is authorised including and in particular where the information to be shared does not exclusively concern AML/CFT but is also information of a prudential nature. As already underlined, some information may be useful both for the prudential supervisor and for AML/CFT; however, it should be recalled that the communication of non-public information by a prudential authority is bound by strict restrictions based on the prudential Directives (cf. the exceptions to professional secrecy listed exhaustively in Directive 2013/36/EU of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC, known as “CRD IV”, and Directive 2009/138/EC of 25 November 2009 on the taking-up and pursuit of the business of Insurance and Reinsurance, known as “Solvency II”). The extent to which the NBB, an authority with a dual role, could be authorised to share information of a prudential nature with a foreign counterpart in matters of combating money laundering which would not at the same time be competent for the prudential domain, must therefore be regulated at a national level in compliance with the European legislative framework. It is understood that, in any case, information of a purely prudential nature and not useful for the foreign authority’s exercise of its AML/CFT competencies is not authorised.

Draft Article 131 authorises this sharing of information but subjects it to the condition, apart from the aforementioned requirement of pertinence, of the existence of certain guarantees inspired by CRD IV destined to preserve the confidential nature of the information transmitted. As a result, the supervisory authority receiving the information must be subject to professional secrecy at least equivalent to that which applies to the Belgian supervisory authority which transmits it, either by having entered into a Memorandum of Understanding (‘MoU’), which provides for the reciprocity of the communications made, as well as the prohibition of using the information sent for reasons other than AML/CFT or prudential supervision and sending it to third parties without prior authorisation in writing from the authority that transmits it.

Where it is provided that information may be used or divulged only with the express permission of the authority that transmits it, it may make its permission subject to adherence to strict conditions.

Where applicable, where the information is shared with adherence to the aforementioned conditions, the professional secrecy obligation to which the supervisory authorities concerned are subject is lifted.



# International cooperation: Comments and recommendations by the NBB

Home > Financial oversight > Combating money laundering and the financing of terrori...

The international cooperation and exchange of information between supervisory authorities with competence in the field of AML/CFT have their legal basis in Articles 129 to 131 of the Anti-Money Laundering Law. This legal framework is based on the legislation applicable in prudential matters and, as a result, the previous legal barriers no longer apply if the conditions set out in the current Law are met. Account is also taken of the principle of territoriality governing the AML/CFT legislations of the European Economic Area Member States and third countries.

Article 130 of the Anti-Money Laundering Law describes the different situations in which the Belgian supervisory authorities (particularly the NBB) are required to cooperate with their foreign counterparts. For instance, the following applies to the NBB in the context of its scope *ratione personae* as defined in Article 85 of the Anti-Money Laundering Law:

- Where the entity concerned is a branch, a subsidiary or other form of establishment on the Belgian territory (particularly a network of agents or distributors) of a foreign financial institution, this entity is subject, in Belgium, not to the AML/CFT law of its country of origin but to the Belgian Anti-Money Laundering Law, and the authority competent for monitoring compliance with this Belgian legislation is not the supervisory authority of the country of origin but the NBB; nevertheless, this territorial supervisory power should be exercised taking into account the dependence of the supervised entity on its registered office or its parent company, which is itself an obliged entity that is supervised in its country of origin. For example, the efficiency of the Belgian entity's AML/CFT governance arrangements is dependent on the compliance thereof with those of the parent company. Conversely, the AML/CFT situation of the Belgian entity could impact that of its parent company in its country of establishment. Article 130, § 1, first paragraph, of the Anti-Money Laundering Law therefore requires the NBB to cooperate and exchange all useful information with the supervisory authority of the country of origin that is competent with regard to the parent company.
- In the same situation, both the FATF standards and Directive 2015/849 stipulate that the parent company should establish internal AML/CFT policies and procedures that apply to all entities of the group, including the Belgian entity; the authority competent for monitoring compliance with this obligation is the authority of the country of origin. However, Article 130, § 1, second paragraph, of the Anti-Money Laundering Law requires the NBB to cooperate with this foreign authority to monitor the effective implementation of the group policy and procedures by the Belgian entity.
- Article 130, § 2, of the Anti-Money Laundering Law contains provisions mirroring those described above, which apply where the Belgian entity is the parent company of a group that has established obliged entities in other Member States or in third countries;
- Article 130, § 2, first paragraph, of the Anti-Money Laundering Law is formulated in such a way that, in the case of a Belgian obliged entity belonging to a foreign group, this provision also constitutes the legal basis enabling the NBB to cooperate with the competent authorities of Member States or third countries, other than the country of establishment of the group's parent company, in which this group has other establishments.

The conditions under which the NBB may communicate confidential information to its counterparts in other Member States or in third countries as part of the cooperation described above are specified in Article 131 of the Anti-Money Laundering Law. Where the other authority is not itself bound by a legal obligation of professional secrecy at least equivalent to that to which the NBB is subject, confidential information may in essence only be communicated providing a Memorandum of Understanding (MoU) is concluded beforehand on the basis of the principle of reciprocity, which limits the authorised use of the information to the AML/CFT supervision and the prudential supervision of the authority receiving the information and which prohibits its transmission to third parties without the NBB's consent.

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



# Sanctions

[Home](#) > [Financial oversight](#) > [Combating money laundering and the financing of terrori...](#)

**Administrative sanctions**

**Criminal sanctions**

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



# Administrative sanctions

Home > Financial oversight > Combating money laundering and the financing of terrori...

## Legal and regulatory framework

- Anti-Money Laundering Law: Articles 132 to 135

## Explanatory Memorandum of the Anti-Money Laundering Law

- Articles 132 to 135

## Other reference documents

- See the list of Sanctions and settlements

## Comments and recommendations by the NBB

- Comments and recommendations

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



# Anti-Money Laundering Law of 18 September 2017 - Articles 132 to 135

## Art. 132

§ 1. Without prejudice to other measures prescribed by this Law or by other legal or regulatory provisions, the supervisory authorities referred to in Article 85 or, where appropriate, the authorities designated by other laws, may, where they identify a breach of the provisions of Book II, of Article 66, § 2, second and third subparagraphs, or of Article 90, fifth subparagraph, of this Law or of their implementing decrees and regulations, of the implementing measures of Directive 2015/849, of the European Regulation on transfers of funds or of the due diligence requirements imposed by the binding provisions on financial embargoes, impose an administrative fine to the obliged entities that fall within their competence and, where appropriate, to one or more members of the statutory governing body of these entities, of their management committee, and to persons involved in their senior management in the absence of a management committee, who are responsible for the breach identified.

§ 2. Where the breach referred to in paragraph 1 has been committed by one of the obliged entities referred to in Article 5, § 1, 1° to 22, the amount of the administrative fine referred to in paragraph 1 shall, for the same deed or deeds, amount to:

1° at least EUR 10 000 and at most ten percent of the annual net turnover in the previous financial year, in case of a legal person;

2° at least EUR 5 000 and at most EUR 5 000 000, in case of a natural person.

Where the breach referred to in paragraph 1 has been committed by one of the obliged entities referred to in Article 5, § 1, 23° to 33°, the amount of the administrative fine referred to in the same paragraph 1 shall, for the same deed or deeds, amount to at least EUR 250 and at most EUR 1 250 000.

§ 3. The amount of the administrative fine referred to in § 1 shall be determined in accordance with paragraph 2, taking into account all relevant circumstances, including:

1° the gravity and the duration of the breaches;

2° the degree of responsibility of the person involved;

3° the financial strength of the person involved, as indicated in particular by the total turnover of the legal person involved or the annual income of the natural person involved;

4° any benefits or profits derived from the breaches by the person involved, insofar as they can be determined;

5° any losses to third parties caused by the breaches, insofar as they can be determined;

6° the level of cooperation of the person involved with the competent authorities;

7° any previous breaches by the person involved.

§ 4. By way of derogation from paragraph 1, the authority competent to impose an administrative fine shall be, in respect of the obliged [entity] referred to in Article 5, § 1, 1° [...] the Minister of Finance and, in respect of bpost, the Minister responsible for the latter.

§ 4 modified by Article 119 of the Law of 30 July 2018 – Belgian Official Gazette of 10 August 2018

§ 5. The Minister of Finance may impose an administrative fine in accordance with paragraphs 2 and 3 in respect of persons who benefit from the exemption referred to in Article 5, § 3 and who fail to comply with the conditions for exemption. However, where the supervisory authority competent for the category of obliged entities to which the person involved belongs, is, in accordance with Article 85, a federal public service, the administrative fine may be imposed by the minister responsible for this federal public service.

§ 6. Without prejudice to other measures prescribed by this Law or by other legal or regulatory provisions, the Minister of Finance may, where he identifies a breach of Article 58/11, third and fourth subparagraphs, of the Law of 27 June 1921 on non-profit associations, foundations and European political parties and foundations, or to Article 14/1, second and third subparagraphs of the Company Code, or to the quality of the data supplied, as referred to in the aforementioned Articles, impose an administrative fine on the administrators referred to in Article 58/11 of the aforementioned Law and in Article 14/1 of the aforementioned Code, and, where appropriate, to one or more members of the statutory body of these entities, their management committee, and to persons involved in their senior management in the absence of a management committee, who are responsible for the breach identified.

The amount of the administrative fine referred to in the first subparagraph shall be at least EUR 250 and at most EUR 50 000.

The amount of the administrative fine referred to in the first subparagraph shall be determined in accordance with the second subparagraph, taking into account all relevant circumstances set out in § 3, 1° to 7°.

## Art. 133

§ 1. Where the FSMA imposes an administrative fine pursuant to Article 132, § 1, the provisions of Chapter III, Section 5, of the Law of 2 August 2002 on the supervision of the financial sector and on financial services shall apply.

§ 2. Where the Belgian Gaming Commission imposes an administrative fine pursuant to Article 132, § 1, the provisions of Articles 15/4 to 15/7 of the Law of 7 May 1999 on games of chance, betting, gaming establishments and the protection of players shall apply.

§ 3. The administrative fine referred to in Article 132, §§ 1 and 6 shall be imposed by the supervisory authorities referred to in Article 85 or, where appropriate, the authorities designated by other laws, the Minister of Finance or the Minister responsible for bpost, pursuant to Article 132, §§ 4 and 6, after the obliged entity or person involved has been heard or at least duly convened.

§ 4. The supervisory authorities referred to in Article 85, § 1, 5° to 12° or, where appropriate, the authorities designated by other laws shall lay down the procedural rules necessary for the imposition of an administrative fine pursuant to Article 132 in respect of the obliged entities referred to in Article 5, § 1, 21°, 23° to 32°, as well as the legal remedies against such a sanction.

The rules of procedure and remedies referred to in the first subparagraph shall take effect only after their approval by the King. If the supervisory authorities concerned fail to lay down such rules of procedure and remedies or fail to amend them in the future, the King shall be empowered to enact such rules or remedies Himself or to amend them.

## Art. 134

The administrative fines imposed pursuant to this Title shall be collected by the administration of FPS Finance which is responsible for collecting and recovering non-fiscal debts, in accordance with Article 3 et seq. of the Law on State Property of 22 December 1949.

## Art. 135

§ 1. The supervisory authorities or, where appropriate, the authorities designated by other laws, the Minister of Finance and the Minister responsible for bpost shall inform the CTIF-CFI of the administrative fines they have imposed pursuant to this Title and of any appeal in relation thereto and of the outcome thereof.

§ 2. The supervisory authorities referred to in Article 85, § 1, 3° to 5° shall inform the ESAs of the administrative fines they have imposed pursuant to this Title to the obliged entities referred to in Article 5, § 1, 4° to 21°, and of any appeal in relation thereto and of the outcome thereof.

§ 3. The supervisory authorities referred to in Article 85, § 1, 1° and 5° to 13° or, where appropriate, the authorities designated by other laws, the Minister of Finance and the Minister responsible for bpost, shall nominatively publish on their official website their decisions concerning the imposition of an administrative sanction under this Title or of a supervisory measure as referred to in Chapters 4 to 7 of Title 4 immediately after the persons concerned have been informed of the decisions.

The publication must contain at least information on the type and nature of the breach and the identity of the natural or legal persons responsible.

Where the publication of the identity of the persons responsible referred to in the second paragraph or the personal data of such persons is deemed disproportionate by the supervisory authorities referred to in the first paragraph, the Minister of Finance or the Minister responsible for bpost, after a case-by-case assessment of the proportionality of the publication of such data, or where such publication would jeopardise the stability of the financial markets or an ongoing investigation, the aforementioned supervisory authorities, the Minister of Finance and the Minister responsible for bpost shall proceed as follows:

1° postponement of the publication of the decision until the reasons for non-publication cease to exist;

2° anonymous publication of the decision, if such an anonymous publication guarantees the effective protection of the personal data in question; in such a case, the publication of the relevant data may be postponed for a reasonable period of time if it is expected that at the end of this period the reasons for an anonymous publication will have ceased to exist;

3° non-publication if the possibilities referred to in 1° and 2° are considered insufficient to ensure that:

a) the stability of the financial markets will not be compromised; or

b) that the publication of the decision is proportionate to the supervisory measures, which are considered to be minor in nature.

If the decision is appealed against, such information and any subsequent information relating to the outcome of that appeal shall be published immediately on the official website referred to in the first paragraph. Any decision cancelling a previous decision must also be published.

Any information published in accordance with this paragraph shall remain on the official website referred to in the first paragraph for a period of five years after publication.

However, the personal data mentioned in the publication on the official website referred to in the first paragraph shall not be kept longer than necessary, in accordance with the applicable rules on the protection of personal data.



# Explanatory Memorandum to the Anti-Money-Laundering Law of 18 September 2017 - Articles 132 to 135

## Art. 132

As has already been indicated, the Directive (Article 59, § 1) imposes providing for administrative sanctions at least in the case of serious, reiterated and/or systematic breaches of certain requirements it lists (customer due diligence, record-keeping, suspicious transaction reporting and internal controls). The Law of 11 January 1993 has a broader scope and provides for the possibility of competent authorities delivering sanctions for every breach of certain legal requirements and of Regulation (EC) No 1781/2006 on transfers of funds (Article 40, first paragraph).

Draft Article 132, § 1 proposes not relaxing the current system and taking over this possibility of imposing a sanction from the time of the first breach, all the while extending its material scope even further by referring not only to breaches of obligations of obliged entities by virtue of Book II of the draft Law (which includes the due diligence and risk assessment obligations, record-keeping, reporting to the CTIF-CFI and internal organisation), as well as by virtue of the European legislation on the subject of funds transfers (in order to simultaneously transpose Article 15, § 1 of Regulation (EC) No 1781/2006 and 17, § 1 of Regulation (EC) No 2015/847), but also breaches of (i) due diligence requirements provided for by the binding provisions on financial embargoes, (ii) technical norms under European regulations on the subject of AML/CFT, (iii) obligations imposed on notaries and estate agents by virtue of Article 66, § 2, second and third paragraphs of the present draft in case of the sale of a property and (iv) measures provided for in Article 90, fifth paragraph of the same draft to protect persons who report infringements of the law to supervisory authorities (whistleblowing). This latter measure allows harmonisation with the provisions of the new Article 36/7/1 of the Law of 22 February 1998 establishing the Organic Statute of the National Bank of Belgium and introduced by the Law of 13 March 2016 which confers on the NBB the power to impose administrative sanctions to financial institutions under its competence in the case of breaches of the prudential legislation).

However, draft Article 132, § 1 transposes Article 58, § 4 of the Directive (a similar provision to which appears in the CRD VI transposed in Article 347 of the Banking Law from which the said Article 132, § 1 took its inspiration) and from now on provides for the possibility of sanctions, not only of the obliged entity itself, but also of the natural persons, members of the legal administrative body or the Board of Directors (or, in the absence of such a committee, the persons responsible for the day-to-day management of the firm) who are responsible for such breaches.

Draft Article 132, § 2 modulates the sanction that may be imposed by competent authorities based on whether the obliged entity being prosecuted is a financial institution (first paragraph) or not (second paragraph).

In the first case, the scale of the sanction is aligned to that provided for in Article 347 of the Banking Law: it is expressed as a range with the minimum being expressed as an absolute amount and the maximum as a percentage of the net turnover. In the second case, where the fine is imposed on a natural person, the scale of the sanction is expressed in absolute amounts.

This scale of sanctions must be applied taking into account the particularities of the sector to which the obliged entity concerned belongs. As a result, the “net turnover” jointly refers, for credit institutions to the “banking income” which is defined as the difference between the total interests and similar income, revenue from variable-yield securities, commissions earned, profit (or loss) from financial transactions and from other operating income and interests and similar charges, as well as commissions paid as defined in the Royal Decree of 23 September 1992 on the annual accounts of credit institutions, investment firms and management companies of undertakings for collective investment. In technical terms, “banking income” is calculated as the difference between the total of items I (interest

and similar products), III (income from variable-yield securities), IV (commissions earned), VI (profit or loss from financial transactions) and XIV (other operating income) and the total of items II (interest and similar charges) and V (commissions paid), in euros and other currencies, items as defined in the Royal Decree of 23 September 1992 on the annual accounts of credit institutions, investment firms and management companies of undertakings for collective investment.

For stockbroking firms, it is specified that the annual net turnover of the stockbroking firm concerned corresponds with the net operating revenue, the components of which are detailed under the commentary in Article 486 of the Banking Law as inserted by Article 72 of the Law of 25 October 2016 on the legal status and supervision of stockbroking firms and containing various provisions (Parliamentary documents, Chamber of Representatives, sess. 2015-2016, Doc 54 – 2058/001, p. 34).

However, for the insurance sector, the “net turnover” must be understood to mean, within the framework of the application of the present draft Law, as referring to the technical and financial revenue of the obliged entity.

For non-financial institutions, the scale of sanctions, expressed only in amounts, is more lenient than the preceding one and corresponds with that currently provided for, for all obliged entities, in Article 40 of the Law of 11 January 1993. The option under Article 59, § 2, e) of the Directive, which allows the upper limit of the sanction able to be imposed to be set at twice the amount of the benefit derived from the breach where that benefit can be determined, is not lifted. Establishing the amount of the fine based on a multiple of the benefit derived from the breach is not always possible and could lead to disputes as regards this latter amount, which could be of a nature so as to hinder the good resolution of the sanction procedures. It therefore seemed preferable to set the maximum amount of the fines able to be imposed in absolute amounts (EUR 5 000 000 for obliged entities in the financial sector and EUR 1 250 000 for other obliged entities). This does not however exclude that where the benefit derived from the breach can be assessed, the size of this benefit is taken into consideration when determining the fine imposed in accordance with draft Article 132, § 3.

Paragraph 3 of draft Article 132 transposes Articles 60, § 4 of the Directive. It gives a formal setting to different factors that the authorities must take into account by expressly stating them, where they are pertinent, for setting the amount of the administrative fine they impose in application of the Law.

Paragraph 4 of this draft provision attributes the sanctioning power to the Minister of Finance rather than the NBB and the Caisse des dépôts et consignations/Deposito- en Consignatiekas [the Public Trustee Office].

Draft Article 132, § 5 takes over the provisions of Article 40, third paragraph of the Law of 11 January 1993. The Directive (cf. Article 2, § 3) maintains the option previously left to the Member States of being able to exempt persons who engage in a financial activity on an occasional or very limited basis where there is little risk, from the application of all or part of the Law, under certain conditions. The draft Law empowers the King to lift this option (cf. Article 5, § 3). It is therefore useful to take over the provisions of Article 40, third paragraph of the Law of 11 January 1993 which designates the Minister of Finance as the competent authority to impose administrative fines on persons who will ultimately be designated by the King by virtue of this power where they do not comply with the conditions of exemption from which they have benefited.

Paragraph 6 of this draft Article confers the sanctioning power to the Minister of Finance as regards the central register of beneficial owners (UBO). Administrative sanctions may be imposed on directors of companies who do not comply with the obligations referred to in Article 14/1, paragraphs two and three, inserted by Article 154 of the draft Law, of the Company Code. These obligations firstly include the collection and keeping of adequate, accurate and current information on the economic interests held by the beneficial owners. This information includes at least the name, date of birth, nationality and address of the beneficial owners, as well as the nature and the extent of the economic interest held by the beneficial owners. Secondly, the companies are obliged to transfer this information to the central register of beneficial owners (UBO).

Likewise as regards non-profit organisations and foundations, this paragraph grants the Minister of Finance the power to impose administrative sanctions to administrators who do not comply with the obligations referred to in Article 58/11, third and fourth paragraphs, inserted by Article 143 of this draft Law, of the Law of 27 June 1921 on non-profit associations, foundations, and European political parties and foundations. These obligations firstly include the collection and keeping of adequate, accurate and current information on the beneficial owners. Secondly, in the cases referred to in Article 4, 27°, c), v) and vi) of this draft Law, the information must be passed on to the central register of beneficial owners.

The Minister of Finance may also impose administrative sanctions if the information transmitted to the central register of beneficial owners by companies, non-profit organisations and foundations is defective in terms of the quality of the data. The Treasury Administration must check the quality of the data because it is responsible for the content of the central register of beneficial owners as well as the appropriate, accurate and current nature of the registered information.

An administrative sanction may only be imposed after having heard the interested parties or at least after having duly summoned them. When an administrative sanction is imposed, it is additionally advisable to take into account all the pertinent circumstances as understood in § 3 of this draft Article.

## Art. 133

Article 133 covers the rules of procedure that apply if competent authorities impose administrative sanctions, where applicable by referring to other laws. As regards the NBB, such a reference is not necessary when Article 36/2 of the Law of 22 February 1998 establishing its Organic Statute is amended to expressly introduce supervision of AML/CFT within its tasks (cf. draft Article 152). From this time, the provisions of this Law establishing the rules of procedure for imposing administrative fines (Articles 36/8 et seq.), as well as the appeals that may be lodged against such fines (Article 36/21), will ipso facto apply if the NBB imposes a sanction as defined in Article 132 of this draft Law.

Apart from preventive measures aiming to put an end to the breaches identified, the Gaming Commission has the power to impose sanctions to providers of games of chance that do not comply with the provisions of Book II of the present Law, in the form of administrative fines, from a minimum of EUR 250 to a maximum of EUR 1 250 000 based on the nature of the breaches, the financial capacity of the interested party, the benefit derived etc.

In the Law of 7 May 1999 on games of chance, the Gaming Commission already has an elaborate procedure for imposing administrative fines. Draft Article 133, § 2 stipulates that this procedure may also be followed to impose administrative fines provided for in this Law. Where in the case of breaches of the law on games of chance, the Gaming Commission is obliged to proceed with collecting this fine for the Treasury with the actual collection coming under the competence of the General Administration for Collection and Debt Recovery of the Federal Public Service Finance.

## Art. 134

Draft Article 134 regulates the methods for collecting the fines imposed. It takes over and updates the last sentence of Article 40, first paragraph, 2° of the Law of 11 January 1993.

## Art. 135

Draft Article 135, § 1 takes over the obligation to report the sanctions imposed to the CTIF-CFI provided for in Article 40, second paragraph of the Law of 11 January 1993. For purposes of effectiveness, this obligation is from now on imposed as soon as the sanction is ruled on and no longer when it has become definitive, which could sometimes considerably delay transmission of the information concerned.

However, a similar reporting obligation is provided for in § 2 of the same draft provision for the supervisory authorities competent for financial institutions (NBB, FSMA and the FPS Economy) to the European Supervisory Authorities in accordance with Article 62, § 1 of the Directive.

Paragraph 3 of draft Article 135 obliges supervisory authorities, with the exception of the NBB and the FSMA (see below) of publishing forthwith any decision concerning measures and sanctions imposed for breaches of the provisions of Book II of this draft Law and its implementing Decrees and Regulations with names, and of Article 90, fifth paragraph of this draft Article, of the enforcement measures under Directive 2015/849, of the European

Regulation on transfers of funds and due diligence obligations within the meaning of the binding provisions on financial embargoes. This publication must take place on the official website of the competent supervisory authority. For the NBB and the FSMA, this publication obligation already features in their own respective legislation, especially in Article 36/1, § 6, first paragraph of the Law of 22 February 1998 establishing the Organic Statute of the National Bank of Belgium and in Article 72, § 3, fourth and seventh paragraphs of the Law of 2 August 2002 on the supervision of the financial sector and on financial services. In the case of the Caisse des dépôts et consignations/Deposito- en Consignatiekas [the Public Trustee Office], the measures and sanctions are imposed by the Minister of Finance who will therefore also take care of the publication. In the case of the limited company under public law bpost, the measures and sanctions are imposed by the Minister competent for bpost who will also take care of the publication.

Directive 2015/849 imposes a certain number of minimum requirements regarding the content of this publication. The publication must contain at least information on the type and nature of the breach and the identity of the natural or legal persons responsible.

The publication may be postponed or rendered anonymous in two cases. The first case concerns the situation in which publication of the identity or the personal data of the legal or natural persons responsible is considered disproportionate after a case-by-case assessment of the proportionality of the publication of these data. The second situation is that in which publication harms the stability of the financial markets or an investigation underway. When the reasons for the postponement or rendering anonymous cease to exist, the publication must take place in the manner provided for, i.e. at least the minimum information required as defined in § 3, second paragraph.

Where the postponement or rendering anonymous are considered insufficient to guarantee not endangering the stability of the financial markets or where the publication of the decision is proportionate given the oversight measures which are deemed minor, the option exists of not publishing.

All the information concerning an appeal lodged against a decision, as well as any subsequent information relating to the outcome of that appeal must be published immediately on the official website of the supervisory authority. Any decision cancelling a previous decision must also be published.

Any information published remains on the official website for a period of five years after publication. However, the personal data mentioned in the publication on the official website shall not be kept longer than necessary, in accordance with the applicable rules on the protection of personal data. In accordance with these regulations, these data may not be kept for longer than required for meeting the objectives for which they are handled.

# Administrative sanctions: Comments and recommendations by the NBB

Home > Financial oversight > Combating money laundering and the financing of terrori...

The NBB's Sanctions Committee may impose an **administrative fine** on financial institutions where it identifies a breach of:

- the obligations regarding governance (organisation and internal control), risk assessment, due diligence, reporting to CTIF-CFI and document retention laid down in Book II of the Anti-Money Laundering Law;
- the obligations regarding non-adverse and non-discriminatory treatment of persons making use of the external whistleblowing system, as laid down in Article 90, fifth paragraph, of the Anti-Money Laundering Law;
- the implementing measures of Directive 2015/849 (in particular the Regulatory Technical Standards and Delegated Regulations of the European Commission);
- the provisions of the European Regulation on transfers of funds; or
- the due diligence obligations laid down in the mandatory provisions on financial embargoes.

Such a fine may be imposed not only on the **financial institution** itself but also, since the entry into force of the Anti-Money Laundering Law, on **natural persons** who are members of the statutory governing body or the management committee of a financial institution, as well as on natural persons who, in the absence of a management committee, are involved in the senior management of an institution and are responsible for the breach identified (Article 132, § 1, of the Anti-Money Laundering Law).

As financial institutions are perceived by the legislator as playing a key role in the fight against ML/FT, **the amount of the administrative fine** imposed by the Sanctions Committee may, for the same deed or deeds, amount to:

- at least EUR 10 000 and at most ten percent of the annual net turnover in the previous financial year, in case of a legal person;
- at least EUR 5 000 and at most EUR 5 000 000, in case of a natural person.

The Anti-Money Laundering Law provides that the amount of the fine is determined taking into account a series of relevant circumstances listed by the Law, such as the gravity and duration of the breaches, the degree of responsibility of the person involved, his financial strength (annual income in case of a natural person) or his level of cooperation with the supervisory authorities.

The Sanctions Committee's decisions to impose an administrative sanction are **published**, in principle specifying the names of the persons involved, on the NBB's website, for a period of at least five years. By way of exception, the Sanctions Committee may decide to publish its decision without specifying the names of the persons involved where specifying the names of the persons involved is liable (cf. Article 36/11, § 6, of the Law of 22 February 1998 establishing the Organic Statute of the NBB):

- to jeopardise the stability of the financial system;
- to jeopardize an ongoing criminal investigation or proceedings;
- to be disproportionately detrimental to the interests of the persons concerned or to the institutions to which they belong.

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**





# Criminal sanctions

Home > Financial oversight > Combating money laundering and the financing of terrori...

## Legal and regulatory framework

- Anti-Money Laundering Law: Articles 136 to 138

## Explanatory Memorandum of the Anti-Money Laundering Law

- Articles 136 to 138

## Comments and recommendations by the NBB

- Comments and recommendations

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



# Anti-Money Laundering Law of 18 September 2017 - Articles 136 to 138

## Art. 136

For the purposes of this Law and its implementing Decrees and Regulations, those who hamper inspections and checks that supervisory authorities are required to carry out in the country or abroad of those who refuse to give information they are required to provide in accordance with this law or those who intentionally provide inaccurate or incomplete information, shall be punished:

1° for the obliged entities referred to in Article 5, § 1, 1° to 10°, 14°, and 17° to 22°, with the penalties referred to in Article 36/20, § 1, of the Law of 22 February 1998 determining the organic statute of the National Bank of Belgium;

2° for the obliged entities referred to in Article 5, § 1, 11° to 13°, 15° and 16°, with the penalties referred to in Article 87, § 1, of the Law of 2 August 2002 on the supervision of the financial sector and on financial services;

3° for the obliged entities referred to in Article 5, § 1, 23° to 33°, with a fine between EUR 150 and EUR 5 000.

## Art. 137

Shall be punished with a fine between EUR 250 and EUR 225 000:

1° those who breach the provisions of Article 66, § 2, first subparagraph, or of Article 67. The fine may however not exceed ten percent of the payment or gift;

2° By way of derogation from Article 136, those who intentionally impede or hinder the mission of police officials or officials designated in accordance with Article XV.2 of the Code of Economic Law when acting within the supervisory powers conferred on the Federal Public Service Economy, SMEs, Self-employed and Energy by Article 85, § 3, of this Law.

The officials designated by the Minister of Economy in accordance with Article XV.2 of the Code of Economic Law can send a warning to the offender, in accordance with Article XV.31 of the same Code or ask the offender to pay an amount barring further prosecution, in accordance with Article XV.61 of the aforementioned Code.

## Art. 138

§ 1. The provisions of Book I of the Criminal Code, including Chapter VII and Article 85, shall be applicable to the offences punishable in accordance with this title.

§ 2. Legal persons are civilly liable for the criminal fines imposed on the members of their legal administrative body, the persons in charge of the actual management or their agents in accordance with this Title.

§ 3. Any investigation as a result of an offence defined in this Title shall be reported to the competent supervisory authority in accordance with Article 85, by the judicial or administrative authority in charge of this investigation.

Any criminal proceedings as a result of an offence referred to in this title shall be reported by the Public Prosecutor's Office to the competent supervisory authority in accordance with Article 85.

§ 4. The competent supervisory authority in accordance with Article 85 is empowered to intervene at any stage of the procedure before the criminal courts dealing with an offence punished by this title, without having to demonstrate any harm. The intervention shall take place in accordance with the rules applicable to the civil party.



# Explanatory Memorandum to the Anti-Money-Laundering Law of 18 September 2017 - Articles 136 to 138

## Art. 136

Draft Article 136 provides for prosecution in the case of impeding the exercise of the tasks of the competent supervisory authorities for ensuring proper application of the present Law.

As regards the financial institutions subject to the present draft Law, the criminal sanctions applied are those that feature in Article 36/20 of the Law of 22 February 1998 establishing the Organic Statute of the National Bank of Belgium and the sanctions provided for in Article 87 of the Law of 2 August 2002 on the supervision of the financial sector and on financial services. In both cases, a prison sentence of at least one month to one year and/or a fine of EUR 250 to EUR 2 500 000 may be imposed.

As regards non-financial entities, a criminal sanction of EUR 150 to EUR 5 000 may be imposed.

The explanation for this distinction between financial and non-financial entities is two-sided. Firstly this draft Law establishes the same distinction in the provisions on administrative sanctions.

Secondly, the distinction is based on the fact that the financial institutions may have a much greater impact and a much more important role in combating ML/TF. Because of their professional knowledge and working environment, these establishments are supposed to show stricter due diligence to avoid the financial system being abused for money laundering and terrorist financing. They therefore take on a greater responsibility for lending their cooperation to the supervisory authorities. This cooperation in combating money laundering by financial institutions, and the associated responsibility, already existed since the 1980s and 1990s at the beginning of international, European and Belgian regulations and under which the starting point was and is that credit and financial institutions can be the subject of abuse and those could seriously endanger the solidity and stability of the establishment concerned and of the financial system as a whole as well as confidence therein (Parliamentary documents, Senate, session 1991 – 1992, Doc. No 468-1, p.3).

## Art. 137

As is the case in the Law of 11 January 1993 (Article 41), the system for criminal sanctions and administrative transactions by the FPS Economy is maintained as regards transactions executed in breach of the provisions of Book III on the limitation of the use of cash (cf. draft Articles 66, § 2, first paragraph and 67).

From now on, it also applies to the parties who contravene the prohibition of paying for property in cash as provided for in Article 66.

Those who make payments or donations in cash, and those who receive them, are punishable in the case of non-compliance with the restrictions provided for in Articles 66 and 67 except, in the case of Article 67, where the two parties are consumers.

The joint and several liability between the parties to the payment of the fine is therefore not necessary and disappears. This possibility had never been used and referred only to fines and not to transactions, as the acceptance of a transaction binds only the one who accepts it and not the co-authors of any breach.

The draft Article adds the possibility for the supervisory authority, the FPS Economy, to address a warning to the offender based on the methods provided for under Article 31 of the Code of Economic Law. This will especially be the case for minor breaches due to a bad interpretation of the law, in good faith, by a beginner, situations close to *force majeure*, etc.

## Art. 138

Draft Article 138 contains provisions that apply generally to cases of criminal breaches provided for by Articles 136 and 137. Paragraph 1 takes over the provision currently provided for in Article 41, third paragraph of the Law of 11 January 1993 (a similar provision to that of Articles 349 of the Banking Law and 606 of the Solvency II Law). The following paragraphs of the draft Article are inspired by Articles 350 to 352 of the Banking Law and 607 to 609 of the Solvency II Law. Paragraph 3 in particular transposes Article 62, § 2 of Directive 2015/849 and aims to avoid infringement of the “*non bis in idem*” principle where the same facts are likely to give rise to criminal prosecution and administrative sanctions. It should be noted that as regards financial institutions subject to supervision by the NBB and the FSMA, this system is supplemented by Article 36/10 of the Law of 22 February 1998 establishing the Organic Statute of the National Bank of Belgium and Article 71, § 5 of the Law of 2 August 2002 on the supervision of the financial sector and on financial services, which provide for sharing of information between these administrative and judicial authorities with a view to avoiding parallel proceedings.



# Criminal sanctions: Comments and recommendations by the NBB

[Home](#) > [Financial oversight](#) > [Combating money laundering and the financing of terrori...](#)

Irrespective of the possible application of Article 505 of the Criminal Code, the Anti-Money Laundering Law describes two offences for which criminal sanctions may be imposed on financial institutions falling under the supervisory powers of the NBB:

- any person who hinders the NBB's inspections and verifications in Belgium or abroad, who refuses to provide information he/she is required to communicate pursuant to the Anti-Money Laundering Law or who knowingly provides incorrect or incomplete information may be subject to a criminal sanction of between one month and one year and/or a fine of between 250 and 2,500,000 euros (penalties set out in Article 36/20, § 1, of the Law of 22 February 1998 establishing the organic statute of the NBB);
- anyone who infringes the provisions of Article 67 of the Anti-Money Laundering Law on the restriction of the use of cash may be subject to a criminal fine of between 250 and 225,000 euros which may not exceed 10 % of the illegal payment or donation.

The provisions of Book I of the Criminal Code, including Chapter VII and Article 85, apply to the criminal offences set out in the Anti-Money Laundering Law.

Legal persons are civilly liable for the criminal fines imposed on the members of their statutory governing bodies, on the persons in charge of the senior management or on their agents, in accordance with the Anti-Money Laundering Law.

As regards financial institutions, the NBB is empowered to intervene at any stage of the procedure before the criminal courts dealing with criminal offences, without having to demonstrate any harm. This intervention should take place in accordance with the rules applicable to the civil party.

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



## Useful links and documents

[Home](#) > [Financial oversight](#) > [Combating money laundering and the financing of terrori...](#)

### **Main reference documents**

### **Other useful links**

### **Successive versions of the AML/CFT website**

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



# Main reference documents

Home > Financial oversight > Combating money laundering and the financing of terrori...

## Contents

- At the national level
- At the European level
- At the international level
- Related documents

## At the national level

### 1.1. Belgian legislation

*Provisions currently in force:*

- Anti-Money Laundering Law of 18 September 2017 (unofficial coordinated version of 05/2019)
- Preparatory works of the Anti-Money Laundering Law of 18 September 2017 (full version)
- Anti-Money Laundering Regulation of the NBB of 21 November 2017
- Article 505 of the Criminal Code (repressive aspect)

*Earlier provisions:*

- Anti-Money Laundering Law of 11 January 1993
- Anti-Money Laundering Regulation of the CBFA of 23 February 2010

### 1.2. Circulars and communications of the NBB

*Circulars and communications currently in force:*

- 2 March 2020 - Circular NBB\_2020\_006 / Periodic questionnaire on combating money laundering and terrorist financing
- 23 January 2020 – Communication NBB\_2020\_002 containing the conclusions of the horizontal analysis of a sample of summary tables of the overall assessment of the risks of money laundering and/or terrorist financing
- 6 November 2019 – Information session on the developments and expectations of the NBB regarding AML/CFT - Presentations
- 19 June 2018 - Communication NBB\_2018\_21 / Horizontal control analysis examining a sample of transactions carried out through tied agents of different payment institutions
- 24 January 2018 - Circular NBB\_2018\_02 / Overall assessment of money laundering and terrorist financing risks
- 6 December 2016 - Horizontal letter: application of financial sanctions regime (Combating the financing of terrorism and of the proliferation of weapons of mass destruction)

*Previous circulars and communications:*

- 15 February 2019 - Circular NBB\_2019\_03 / Periodic questionnaire on combating money laundering and terrorist financing

- 15 January 2018 - Circular NBB\_2018\_01 / Periodic questionnaire on combating money laundering and terrorist financing
- 24 April 2017 - Circular NBB\_2017\_15 / Reporting on inherent risks related to money laundering and the financing of terrorism to which financial institutions are exposed
- 26 October 2016 - Circular NBB\_2016\_43 / Short-form periodic questionnaire on the prevention of money laundering and terrorist financing
- 26 October 2016 - Circular NBB\_2016\_42 / Periodic questionnaire on the prevention of money laundering and terrorist financing
- 12 July 2016 - Circular NBB\_2016\_32 / Opinion of the European Banking Authority (EBA) on the application of customer due diligence measures to customers who are asylum seekers from higher-risk third countries (EBA-Op-2016-07)
- 7 October 2015 - Circular NBB\_2015\_27 / Short-form periodic questionnaire on the prevention of money laundering and terrorist financing (annex)
- 7 October 2015 - Circular NBB\_2015\_26 / Periodic questionnaire on the prevention of money laundering and terrorist financing (annex 1 - annex 2)
- 14 October 2014 – Circular NBB\_2014\_11 / Periodic questionnaire on the prevention of money laundering and terrorist financing (annex 1 - annex 2)
- 3 April 2014 - Circular NBB\_2014\_04 / Periodic questionnaire on the prevention of money laundering and terrorist financing
- 18 December 2013 - Circular NBB\_2013\_16 / Recent developments in the prevention of money laundering
- 25 September 2013 - Circular NBB\_2013\_10 / Periodic questionnaire on combating money laundering and terrorist financing
- 25 August 2010 - Communication CBFA\_2010\_18 on the need to exercise enhanced due diligence in preventing money laundering, terrorist financing and the proliferation of weapons of mass destruction
- 6 April 2010 - Circular CBFA\_2010\_09 on customer due diligence, on preventing the use of the financial system for the purposes of money laundering and terrorist financing, and on preventing the financing of the proliferation of weapons of mass destruction
- 1 July 2009 - Communication CBFA\_2009\_27 on the need to exercise enhanced due diligence in preventing money laundering and terrorist financing, with regard to Iran, Uzbekistan, Turkmenistan and Azerbaijan

### 1.3. Financial sanctions (asset freezing and embargoes)

- See 'National financial sanctions' on the website of the Treasury

### 1.4. CTIF-CFI and FSMA

- Protocol of 17 September 2019 defining the modalities of cooperation and information exchange between the NBB and CTIF-CFI
- CTIF-CFI's information note of 26 October 2017 regarding the disclosure of information to CTIF-CFI
- General Memorandum of Understanding of 14 March 2013 for collaboration between the NBB and the FSMA to ensure the coordination of the supervision of the institutions under their respective supervision

## At the European level

### 2.1. European legislation

- Delegated Regulation 2019/758 of 31 January 2019 on the minimum action and the type of additional measures credit and financial institutions must take to mitigate ML/FT risk in certain third countries
- Regulation 2018/1672 of 23 October 2018 on controls on cash entering or leaving the Union
- RTS dated 7 May 2018 on CCP to strengthen fight against financial crime
- Delegated Regulation 2016/1675 of 14 July 2016 on high-risk third countries (for the updated annex and methodology, see the website of the European Commission – financial crime section)
- Fourth AML/CFT Directive 2015/849 of 20 May 2015 transposed into Belgian law by the Law of 18 September 2017) as modified by the fifth AML/CFT Directive 2018/843 of 30 May 2018 (unofficial coordinated version of 9 July 2018)
- Regulation 2015/847 of 20 May 2015 on information accompanying transfers of funds
- Regulation No 910/2014 of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market

- See 'European financial sanctions' on the website of the Treasury

## 2.2. European Commission

- Report from the Commission to the European Parliament and the Council of 24 July 2019 on the assessment of ML/FT risks affecting the internal market and relating to cross-border activities (Supranational Risk Assessment Report - SNRA)
  - Annex (Commission Staff Working Document)
- Report from the Commission to the European Parliament and the Council of 26 June 2017 on the assessment of ML/FT risks affecting the internal market and relating to cross-border activities (Supranational Risk Assessment Report - SNRA)
- Communication from the Commission to the European Parliament and the Council of 2 February 2016 on an Action Plan for strengthening the fight against terrorist financing

## 2.3. Joint Committee of the European Supervisory Authorities

- Joint Guidelines dated 16 December 2019 on cooperation and information exchange between competent authorities supervising credit and financial institutions ("The AML/CFT Colleges Guidelines")
- Joint Opinion dated 4 October 2019 on the risks of money laundering and terrorist financing affecting the Union's financial sector
- Opinion dated 23 January 2018 on the use of innovative solutions by credit and financial institutions
- Guidelines of 4 January 2018 on risk factors
- Joint Guidelines of 22 September 2017 under Article 25 of Regulation (EU) 2015/847 on the measures payment service providers should take to detect missing or incomplete information on the payer or the payee, and the procedures they should put in place to manage a transfer of funds lacking the required information
- Joint Opinion dated 20 February 2017 on the risks of money laundering and terrorist financing affecting the Union's financial sector
- Guidelines of 7 April 2017 on risk- based supervision

## 2.4 European Banking Authority

- Opinion dated 24 April 2019 on the nature of passport notifications regarding agents and distributors under Directive 2015/2366 (PSD2), Directive 2009/110/EC (EMD2) and Directive 2015/849 (AMLD)
- Opinion dated 12 October 2017 on issues related to the departure of the United Kingdom from the European Union
- Opinion dated 12 April 2016 on the application of customer due diligence measures to customers who are asylum seekers from higher-risk third countries or territories

## 2.5 European Insurance and Occupational Pensions Authority

- Opinion dated 11 July 2017 on supervisory convergence in light of the United Kingdom withdrawing from the European Union

# At the international level

## 3.1. FATF

### *Recommandations :*

- International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation (February 2012, updated in in June 2019)

### *Guidelines:*

- Best Practices dated October 2019 on Beneficial Ownership for Legal Persons
- Guidance dated June 2019 for a Risk-Based-Approach for the Virtual Assets and Virtual Assets Service Providers
- Guidance dated 26 October 2018 for a Risk-Based Approach for the Securities Sector
  - Highlights

- Guidance dated 25 October 2018 for a Risk-Based Approach for the Life Insurance Sector
  - Highlights
- Guidance dated 28 February 2018 on counter proliferation financing
- Guidance dated 4 November 2017 on AML/CFT measures and financial inclusion, with a supplement on customer due diligence
- Guidance dated 4 November 2017 on Private Sector Information Sharing
- Guidance dated 21 October 2016 on Correspondent Banking
- Guidance dated 23 February 2016 for a Risk-Based Approach for Money or Value Transfer Services
- Guidance dated 23 October 2015 for a Risk-Based Approach: Effective Supervision and Enforcement by AML/CFT Supervisors of the Financial Sector and Law Enforcement
- Guidance dated 27 October 2014 for a Risk-Based Approach for the Banking Sector
- Guidance dated 27 October 2014 on Transparency and Beneficial Ownership
- Guidance dated 27 June 2013 on Politically Exposed Persons

*Mutual evaluations:*

- Methodology for assessing technical compliance with the FATF Recommendations and the effectiveness of AML/CFT Systems (February 2013, updated in October 2019)
- Mutual Evaluation Report of Belgium (February 2015)
  - 3rd Enhanced Follow-up Report and Technical Compliance Re-Rating (September 2018)

### **3.2. Basel Committee**

- Guidelines dated June 2017 on Sound management of risks related to money laundering and financing of terrorism
- Guidance dated September 2016 on the application of the Core principles for effective banking supervision to the regulation and supervision of institutions relevant to financial inclusion

## Related documents

- Protection of personal data: see the website of the Data Protection Authority
- Legislation pertaining to the combat of discrimination: see the website of UNIA

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



## Other useful links

Home > Financial oversight > Combating money laundering and the financing of terrori...

### Contents

- At the national level
  - At the European level
  - At the international level
- 

### At the national level

- Checkdoc.be
- CTIF-CFI
- FSMA
- FPS Economy – Combating money laundering and terrorist financing
- Treasury – Financial sanctions
- Treasury – High-risk countries

### At the European level

- European Commission – Justice and fundamental rights – Financial crime
- Joint Committee of the European Supervisory Authorities
- EBA
- EIOPA
- ESMA
- MONEYVAL

### At the international level

- Basel Committee
  - FATF
- 

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



# Successive versions of the AML/CFT website

Home > Financial oversight > Combating money laundering and the financing of terrori...

## Contents

- Successive versions of the website
- Overview of the changes

## Successive versions of the website

### Current version:

- PDF version of 13 August 2020 (before revision of the AML/CFT website following the entry into force of the Law of 20 July 2020)

### Previous versions:

- PDF version of 21 February 2020
- PDF version of 21 October 2019
- PDF version of 26 June 2019

## Overview of the changes

### On 13 August 2020:

- Substantive changes to comments and recommendations by the NBB on the Reporting by financial institutions (see point 2 en its reference documents)
- Addition of the following NBB documents:
  - 7 April 2020 – Communication NBB\_2020\_14/ COVID-19
  - 2 March 2020 – Circular NBB\_2020\_006 / Periodic questionnaire on combating money laundering and terrorist financing

### On 21 February 2020:

- Substantive changes to comments and recommendations by the NBB on the following topics:
  - Risk-based approach and overall risk assessment (see points 3. and 4. as well as its reference documents)
  - Governance (see points 2.5., 3., 4. and 5. as well as its reference documents )
  - Performance of obligations by third parties (see points 1. and 2.)
  - Reporting by financial institutions (see points 1.1., 1.2. and 1.3. as well as its reference documents)
- Addition of the following documents:
  - FATF documents:
    - Methodology for assessing technical compliance with the FATF Recommendations and the effectiveness of AML/CFT Systems, as updated in October 2019
    - Best Practices dated October 2019 on Beneficial Ownership for Legal Persons

- Guidance dated June 2019 for a Risk-Based-Approach for the Virtual Assets and Virtual Assets Service Providers
- European Documents:
  - ESAs Joint Guidelines dated 16 December 2019 on cooperation and information exchange between competent authorities supervising credit and financial institutions (“The AML/CFT Colleges Guidelines”)
- NBB documents:
  - 23 January 2020 – Communication NBB\_2020\_002 containing the conclusions of the horizontal analysis of a sample of summary tables of the overall assessment of the risks of money laundering and/or terrorist financing
  - Presentations of the information session of 6 November 2019 on the developments and expectations of the NBB regarding AML/CFT

### On 21 October 2019:

- Substantive changes to comments and recommendations by the NBB on the following topics:
  - Governance (see point 4: introduction and point 4.1; new points 4.6 and 4.7)
  - Internal whistleblowing (see § 2)
  - Object of the identification and identity verification (see point 2.2, § 3; point 2.3.1, § 2; point 5)
  - Prohibition of disclosure (see point 1, new § 3)
  - Financial embargoes and assets freezing (see point 1, § 6; point 2.1, §§ 2 and 3; point 5.4, § 1)
  - Reporting by financial institutions to the NBB (see point 4.1)
- Addition of the following documents:
  - FATF documents:
    - Recommendations as updated in June 2019 (see page Introduction)
    - Methodology for assessing technical compliance with the FATF Recommendations and the effectiveness of AML/CFT Systems, as updated in February 2019
  - European documents
    - Delegated Regulation (EU) 2019/758 of 31 January 2019 on the minimum action and the type of additional measures credit and financial institutions must take to mitigate ML/FT risk in certain third countries (see page Belgian parent companies)
    - Report of 24 July 2019 from the Commission to the European Parliament and the Council on the assessment of ML/FT risks affecting the internal market and relating to cross-border activities (SNRA) + annex (Commission Staff Working Document) (see page Risk-based approach and overall risk assessment)
    - ESAs Joint Opinion dated 4 October 2019 on the risks of money laundering and terrorist financing affecting the Union’s financial sector (see page Risk-based approach and overall risk assessment)
    - EBA opinion dated 24 April 2019 on the nature of passport notifications regarding agents and distributors under Directive 2015/2366 (PSD2), Directive 2009/110/EC (EMD2) and Directive 2015/849 (AMLD) (see page Belgian CCPs of European payment institutions and electronic money institutions)
  - NBB documents:
    - Addition of old circulars "Periodic questionnaire" 2014\_11, 2015\_26 and 2015\_27
    - Protocol of 17 September 2019 defining the modalities of cooperation and information exchange between the NBB and CTIF-CFI (see page National cooperation)
- Minor changes to other pages of the AML/CFT website.

### On 26 June 2019:

- Online release of the English version of the AML/CFT site
- Minor changes to existing pages of the AML/CFT website.

---

**Disclaimer: This English text is an unofficial translation and may not be used as a basis for solving any dispute**



