

Combating money laundering and the financing of terrorism

- **Information and recommendations**
 - Introduction
 - Scope
 - Definitions
 - Risk-based approach and overall risk assessment
 - Organisation and internal control
 - Customer and transaction due diligence
 - Analysis of atypical transactions and reporting of suspicions
 - Transfers of funds
 - Financial embargoes and assets freezing
 - Data and document retention
 - Personal data processing and protection
 - Restriction of the use of cash
 - Supervision by the NBB
 - Sanctions
 - Useful links and documents
- **Publication of individual decisions**

- [Information and recommendations](#)
 - [Introduction](#)
 - [Scope](#)
 - [Definitions](#)
 - [Risk-based approach and overall risk assessment](#)
 - [Risk-based approach and overall risk assessment: Comments and recommendations by the NBB](#)
 - [Organisation and internal control](#)
 - [Organisation and internal control in financial institutions](#)
 - [Governance](#)
 - [Governance: Comments and recommendations](#)
 - [Risk classification](#)
 - [Policies, procedures, processes and internal control measures](#)
 - [Policies, procedures, processes and internal control measures: Comments and recommendations](#)
 - [Training and education of staff](#)
 - [Internal whistleblowing](#)
 - [Organisation and internal control in groups](#)
 - [Belgian parent companies](#)
 - [Belgian parent companies: Comments and recommendations](#)
 - [Belgian subsidiaries and branches](#)
 - [Belgian central contact points of European payment institutions and electronic money institutions](#)
 - [Belgian central contact points of European payment institutions and electronic money institutions: Comments and recommendations](#)
 - [Performance of obligations by third parties](#)
 - [Performance of obligations by third parties: Comments and recommendations by the NBB](#)
 - [Brexit](#)
 - [Customer and transaction due diligence](#)
 - [Individual risk assessment](#)
 - [Individual risk assessment: Comments and recommendations by the NBB](#)
 - [Anonymous or numbered accounts, safe-deposit boxes and contracts](#)
 - [Identification and identity verification](#)
 - [Persons to be identified](#)
 - [Persons to be identified: Comments and recommendations by the NBB](#)
 - [Object of the identification and identity verification](#)
 - [Object of the identification and identity verification: Comments and recommendations](#)
 - [Time of identification and identity verification](#)
 - [Time of identification and identity verification: Comments and recommendations by the NBB](#)
 - [Non-compliance with the identification and identity verification obligation](#)
 - [Non-compliance with the identification and identity verification obligation: Comments and recommendations by the NBB](#)
 - [Identification of the customer's characteristics and of the purpose and nature of the business relationship or the occasional transaction](#)

- [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](#)
- [Due diligence on business relationships and occasional transactions and detection of atypical facts and transactions](#)
 - [Due diligence on business relationships and occasional transactions and detection of atypical facts and transactions: Comments and recommendations by the NBB](#)
- [Special cases of enhanced due diligence](#)
 - [Identity verification over the course of the business relationship and implementation of measures as an alternative to terminating a business relationship](#)
 - [Identity verification over the course of the business relationship: Comments and recommendations by the NBB](#)
 - [High-risk third countries](#)
 - [High-risk third countries: Comments and recommendations by the NBB](#)
 - [States with low or no taxes](#)
 - [States with low or no taxes: Comments and recommendations by the NBB](#)
 - [Correspondent relationships](#)
 - [Correspondent relationships: Comments and recommendations by the NBB](#)
 - [Politically exposed persons \(PEPs\)](#)
 - [Politically exposed persons \(PEPs\): Comments and recommendations by the NBB](#)
 - [Recommended actions in the event of credible publications of mass fraud or ML/FT cases in the press](#)
- [Due diligence requirements and de-risking](#)
 - [Due diligence requirements and de-risking: Comments and recommendations by the NBB](#)
- [Due diligence requirements and compliance with other legislation](#)
- [Analysis of atypical transactions and reporting of suspicions](#)
 - [Analysis of atypical facts and transactions](#)
 - [Analysis of atypical facts and transactions: Comments and recommendations by the NBB](#)
 - [Reporting of suspicions](#)
 - [Reporting of suspicions: Comments and recommendations by the NBB](#)
 - [Prohibition of disclosure](#)
 - [Protection of reporting persons](#)
- [Transfers of funds](#)
 - [Transfers of funds: Comments and recommendations by the NBB](#)
- [Financial embargoes and assets freezing](#)
 - [Financial embargoes and assets freezing: Comments and recommendations by the NBB](#)
- [Data and document retention](#)
 - [Data and document retention: Comments and recommendations by the NBB](#)
- [Personal data processing and protection](#)
 - [Personal data processing and protection: comments and recommendations by the NBB](#)
- [Restriction of the use of cash](#)
 - [Restriction of the use of cash: Comments and recommendations by the NBB](#)
- [Supervision by the NBB](#)
 - [New institutions](#)
 - [New institutions: Comments and recommendations](#)

- [Reporting by financial institutions](#)
 - [Reporting by financial institutions: Comments and recommendations](#)
 - [Business-wide ML/TF risk assessment](#)
 - [Periodic questionnaire](#)
- [External whistleblowing](#)
 - [External whistleblowing: Comments and recommendations by the NBB](#)
- [Supervisory powers, measures and policy of the NBB](#)
 - [Supervisory powers, measures and policy of the NBB: Comments and recommendations by the NBB](#)
- [National cooperation](#)
 - [National cooperation: Comments and recommendations by the NBB](#)
- [International cooperation](#)
 - [International cooperation: Comments and recommendations by the NBB](#)
- [Sanctions](#)
 - [Administrative sanctions](#)
 - [Administrative sanctions: Comments and recommendations by the NBB](#)
 - [Criminal sanctions](#)
 - [Criminal sanctions: Comments and recommendations by the NBB](#)
- [Useful links and documents](#)
 - [Main reference documents](#)
 - [Other useful links](#)
 - [Successive versions of the AML/CFT website](#)
- [Individual preventive measures](#)

Information and recommendations

search

The most recent NBB circulars

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, safe-deposit boxes 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
 - Due diligence on business relationships and occasional transactions and detection of atypical facts and transactions
 - Special cases of enhanced due diligence
 - Due diligence requirements and de-risking
 - 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 persons

- **Transfers of funds**
- **Financial embargoes and assets freezing**
- **Data and document retention**
- **Personal data processing and protection**
- **Restriction of the use of cash**
- **Supervision by the NBB**
 - New institutions
 - Reporting by financial institutions
 - External whistleblowing
 - Supervisory powers, measures and policy 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 resolving any dispute.

Introduction

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”), since amended by the fifth AML/CFT Directive, i.e. Directive (EU) 2018/843 of 30 May 2018 (“Directive 2018/843”) and Directive 2019/2177 (see the unofficial coordinated version of 30 June 2021);
- 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 Directives;
- 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, 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 and of the Anti-Money Laundering Regulation of the NBB 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 of 18 September 2017 and of its successive amending Laws 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 (see the page “Main reference documents”), whether or not it is completed by comments and/or recommendations from the NBB.**

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 has 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 updates 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 texts relevant to the financial institutions falling under its supervisory competence (law, regulations, preparatory work, European and international guidelines, etc.) that are 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 resolving any dispute.

Scope

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 are collectively referred to as 'financial institutions' on this website.

They are the following institutions, acting in the exercise of their professional regulated activities:

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;
d) 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 an agent established in Belgium to provide services there consisting of receiving deposits or other repayable funds within the meaning of Article 4, 1) of the same Law;
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. 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;
- 6. mutual guarantee societies as referred to in the Royal Decree of 30 April 1999 on the legal status and supervision of mutual guarantee societies;
- 7. 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, (ii) credit

institutions which are governed by the law of another EEA Member State and rely on an agent established in Belgium to provide services there consisting of receiving deposits or other repayable funds, and (iii) 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 preparatory works of the Anti-Money Laundering Law (Law of 18 September 2017 and amending Laws) (see the page “Main reference documents”).

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

Definitions

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:

- “**(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
- “**AMLCO**”: see Article 1, 4° of the Anti-Money Laundering Regulation
- “**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
- “**Anti-Money Laundering Regulation of the NBB**”: Regulation of the NBB of 21 November 2017 on the prevention of money laundering and terrorist financing
- “**Atypical transaction**”: see Article 1, 6° of the Anti-Money Laundering Regulation
- “**Authentication service**”: see Article 4, 41° 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
- “**Business day**”: see Article 4, 40° of the Anti-Money Laundering Law
- “**Business relationship**”: see Article 4, 33° of the Anti-Money Laundering Law
- “**Coordinating bodies**”: see Article 4, 14° of the Anti-Money Laundering Law
- “**Correspondent relationship**”: see Article 4, 34° of the Anti-Money Laundering Law
- “**Criminal activity**”: see Article 4, 23° of the Anti-Money Laundering Law
- “**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
- “**Electronic money**”: see Article 4, 35° of the Anti-Money Laundering Law
- “**European Regulation on transfers of funds**”: see Article 4, 5° of the Anti-Money Laundering Law
- “**European Supervisory Authorities**” or “**ESAs**”: see Article 4, 11° of the Anti-Money Laundering Law
- “**Family member**”: see Article 4, 29° of the Anti-Money Laundering Law
- “**Financial Action Task Force**” or “**FATF**”: see Article 4, 10° of the Anti-Money Laundering Law
- “**Financial intelligence unit**”: see Article 4, 15° of the Anti-Money Laundering Law
- “**Games of chance**”: see Article 4, 36° of the Anti-Money Laundering Law
- “**Goods**”: see Article 4, 24° of the Anti-Money Laundering Law
- “**Group**”: see Article 4, 22° of the Anti-Money Laundering Law
- “**High-risk third country**”: see Article 4, 9° of the Anti-Money Laundering Law
- “**Implementing measures of Directive 2015/849**”: see Article 4, 4° of the Anti-Money Laundering Law
- “**International organisation**”: see Article 4, 32° of the Anti-Money Laundering Law
- “**Life insurance contract**”: see Article 4, 25° of the Anti-Money Laundering Law
- “**Managerial functions**”: see Article 4, 39° of the Anti-Money Laundering Law
- “**Managerial responsibilities**”: see Article 4, 38° of the Anti-Money Laundering Law
- “**Member State**”: see Article 4, 7° 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

- **“National Security Council”**: see Article 4, 13° of the Anti-Money Laundering Law
- **“NBB”**: the National Bank of Belgium
- **“Numbered account or contract”**: see Article 1, 7° of the Anti-Money Laundering Regulation
- **“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 a third country”**: see Article 4, 21° 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”**: see Article 4, 18° 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
- **“Occasional transaction”**: see Article 1, 5° of the Anti-Money Laundering Regulation
- **“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
- **“Professional counterparty”**: see Article 1, 8° of the Anti-Money Laundering Regulation
- **“Regulation 910/2014”**, known as the “eIDAS Regulation”: see Article 4, 5°/3 of the Anti-Money Laundering Law
- **“Senior management”**: see Article 4, 31° of the Anti-Money Laundering Law
- **“Shell bank”**: see Article 4, 37° of the Anti-Money Laundering Law
- **“Supervisory authorities”**: see Article 4, 17° of the Anti-Money Laundering Law
- **“Third country”**: see Article 4, 8° of the Anti-Money Laundering Law
- **“Trust”**: see Article 4, 26° of the Anti-Money Laundering Law

For more information on the definitions, see the preparatory works of the Anti-Money Laundering Law (Law of 18 September 2017 and amending Laws) (see the page “Main reference documents”).

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

Risk-based approach and overall risk assessment

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

Supranational risk assessment (SNRA)

- Report from the Commission to the European Parliament and the Council dated 27 October 2022 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)
- EBA Opinion dated 3 March 2021 on the risks of money laundering and terrorist financing affecting the Union's financial sector

Sectoral risk assessment

- Sectoral assessment of the money laundering risks in the Belgian financial sector subject to the supervisory authority of the National Bank of Belgium – version of 8 September 2020

Risk factors to be taken into account

- EBA Risk Factor Guidelines dated 1 March 2021

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 January 2014 on Sound management of risks related to money laundering and financing of terrorism (revised in July 2020)
- 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 resolving any dispute.

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

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 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 EBA 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) ("EBA Risk Factor Guidelines");
- 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 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;
- the sectoral assessment of the money laundering risks in the Belgian financial sector subject to the supervisory authority of the National Bank of Belgium, 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:

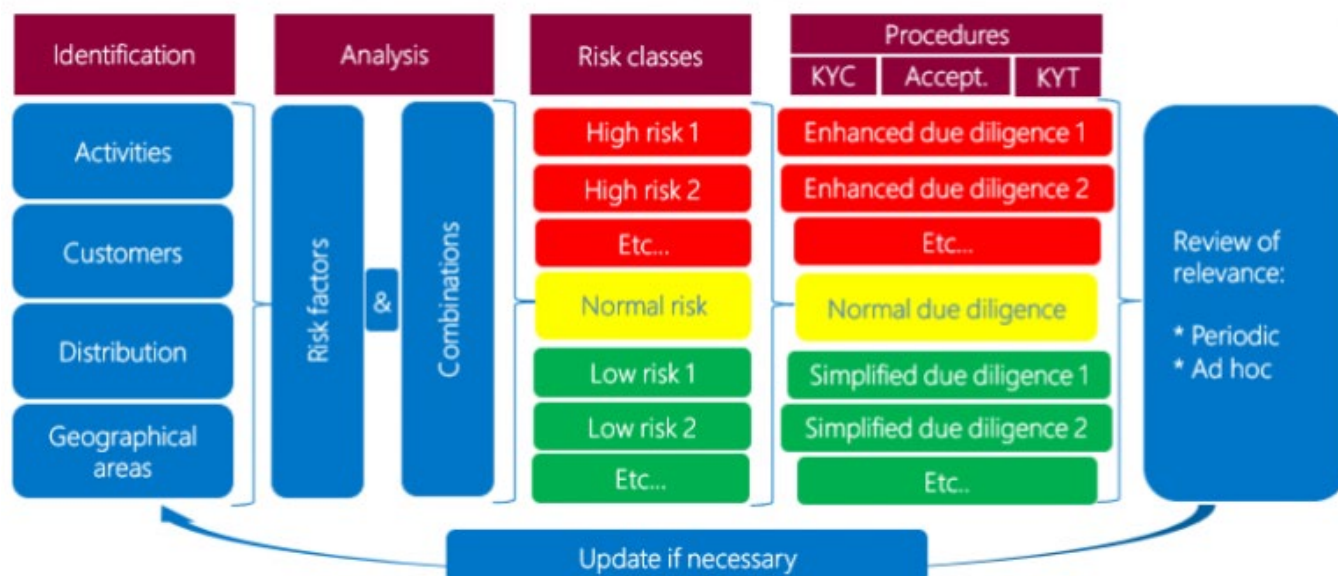
- the methodology used to perform the overall risk assessment, which is expected to include at least the key elements referred to in point 3 below;
- the manner in which this process has been integrated into the institution's broader risk management system and in its corporate governance, including the 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 obligation of due diligence on business relationships and occasional transactions, 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 EBA 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 resolving any dispute.

Organisation and internal control

- **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
 - Central contact points in Belgium of financial institutions governed by the law of another Member State
 - **Performance of obligations by third parties**
 - **Brexit**
-

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

Organisation and internal control in financial institutions

- **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 resolving any dispute.

Governance

Statutory and regulatory framework

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

Other reference documents

- EBA Guidelines of 14 June 2022 on the AMLCO function

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 resolving any dispute.

Governance: Comments and recommendations

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 statutory obligation to appoint a senior officer responsible for AML/CFTP is meant to enhance the involvement of the highest hierarchical level of 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 such prevention and, in particular, to perform at least the following tasks:

1. ensure that 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 it. In this respect, the senior officer responsible for AML/CFTP is expected to pay particular attention to (i) the coherence between the AML/CFTP procedures and the more operational procedures for each activity, and (ii) the coherence between the AML/CFTP policy and the policy implemented within the group;
2. assess, together with the management committee (or, where appropriate, senior management), whether the rule to appoint a separate AMLCO can be deviated from on the basis of the principle of proportionality (see point 5 below);
3. support the management committee (or, where appropriate, senior management) in assessing whether it is necessary to establish an AML unit to assist the AMLCO in carrying out his/her duties;
4. ensure regular reporting to the management committee (or, where appropriate, senior management) and to the board of directors on the activities carried out by the AMLCO, and provide them with sufficiently comprehensive and timely information and data on AML/CFTP risks and compliance with AML/CFTP regulations, which is necessary to enable them to perform the role and functions entrusted to them. Such information should also include arrangements between the financial institution and the AML/CFTP supervisor as well as communication with CTIF-CFI - without prejudice to the confidentiality of reports of suspicious financial transactions - and findings of the AML/CFTP supervisor regarding the financial institution, including any measures or sanctions imposed;
5. notify the management committee (or, where appropriate, senior management) and the board of directors of serious or significant AML/CFTP problems or violations and recommend measures to remedy them; and
6. ensure that the AMLCO (i) has access to all the information necessary to perform his/her tasks, (ii) has

sufficient human and technical resources and tools to be able to adequately perform the tasks assigned to him/her, 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.

The senior officer responsible for AML/CFTP serves as the main point of contact for the AMLCO within management. This person should also ensure that any AML/CFTP-related concerns of the AMLCO are properly addressed and, where this is not possible, that they are duly taken into account by the management committee or, where appropriate, senior management. Where the management committee or, where appropriate, senior management decides not to follow the AMLCO's recommendation, such decisions should be duly justified and recorded in the light of the risks and concerns raised by the AMLCO.

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 (3rd subparagraph) (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 (3rd subparagraph) (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 the AMLCO calls on these AML correspondents.

2.2. Terms and conditions for the appointment of the AMLCO

The third subparagraph of Article 9 §2 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 statutory 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 the AMLCO's 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").

The financial institution's internal procedures should ensure that the AMLCO at all times has unrestricted and direct access to all information necessary for the performance of his/her duties. The AMLCO decides what information he/she needs access to in this respect.

In case of a major incident, the AMLCO should be able to report and have direct access to the board of directors.

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 (3rd subparagraph) (2) of the Anti-Money Laundering Law, which stipulates that the AMLCO should, in particular, possess the knowledge of the Belgian statutory and regulatory framework and the availability needed to perform his/her 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. If this requirement is derogated from under the principle of proportionality, the financial institution should have the necessary systems and control measures in place to ensure that the AMLCO has access to all information and systems necessary for the performance of the latter's duties, and is available to meet with CTIF-CFI and the supervisor without delay. The financial institution should also be able to provide evidence to the supervisor that the measures it has put in place are adequate and efficient. Furthermore, 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 (3rd subparagraph) (2) of the Anti-Money Laundering Law prevent this function from being conferred

upon the AML correspondents referred to in point 2.1, 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, this person 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 statutory 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 statutory and regulatory AML/CFTP framework, and to ensure that this person 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.

The financial institution should ensure that the AMLCO is working on an ongoing basis as part of its overall business continuity management. It should consider the possibility of the AMLCO being relieved of his/her

duties and ensure the availability of a substitute possessing appropriate skills and expertise to whom the AMLCO's duties can be delegated in the event that the latter is absent for some time or his/her integrity is no longer beyond doubt.

§3. Availability

AMLCOs should have **sufficient time** to perform their 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 statutory requirements to have knowledge of the Belgian statutory 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 statutory and regulatory AML/CFTP framework, and to ensure that this person has direct contact with the branch's managers as well as the right of initiative with regard to these managers.

2.3. Tasks

As part of the second line of defence, the AMLCO is responsible for effectively steering AML/CFTP policy in the financial institution. The AMLCO's role and responsibilities should be clearly defined and documented. In particular, the AMLCO is responsible for the following tasks:

1. developing and maintaining an ML/FT risk assessment framework for the purpose of carrying out overall and individual risk assessments;
2. effectively implementing the organisational measures listed in Article 8 of the Anti-Money Laundering Law, and ensuring that they are regularly reviewed and, where necessary, amended or updated;

3. proposing a course of action in the event of changes in statutory or regulatory requirements or in ML/FTP risks, and how best to address deficiencies and shortcomings revealed by monitoring and supervision;
4. monitoring the effective implementation of AML/CFTP control measures by business units and internal units, which act as the first line of defence;
5. providing advice before employees at an appropriately high hierarchical level make a final decision on the acceptance or continuation of a business relationship with high-risk customers in accordance with the financial institution's risk-based internal AML/CFTP policies. Where these employees do not follow the AMLCO's advice, they should properly record their decision and establish how they intend to mitigate the risks raised by the AMLCO;
6. analysing atypical transactions and situations in which the due diligence obligations could not be fulfilled (in accordance with Articles 45 and 46 of the Anti-Money Laundering Law);
7. deciding, where necessary, to report suspicions to CTIF-CFI (in accordance with Article 47 of the Anti-Money Laundering Law and the provisions adopted in implementation of Article 54 of the Law) and to provide it with any other information required by application of the Law. In this regard, the AMLCO makes the autonomous decision to report to CTIF-CFI without submitting this decision to the senior officer responsible;
8. responding to requests for additional information addressed to the financial institution by CTIF-CFI (in accordance with Articles 48 and 49 of the Anti-Money Laundering Law);
9. educating and training the staff and, where applicable, the agents and distributors of the financial institution on AML/CFTP-related matters;
10. 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;
11. 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). In addition, the AMLCO should in any case bring the following to the attention of the senior officer responsible for AML/CFTP: (a) areas where AML/CFTP control measures should be implemented or improved; (b) proposals for appropriate improvements in line with point (a); (c) a progress report of major remediation programmes, at least once a year as part of the above-mentioned activity report, and information provided on an ad hoc basis or periodically - depending on improvements – on the level of exposure to ML/FTP risks and the measures taken or recommended to manage these risks effectively; (d) whether sufficient human and technical resources have been allocated to the AMLCO and, if not, whether they need to be supplemented.

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 statutory 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 CTIF-CFI). The AMLCO may combine this task with that of person responsible for the compliance function, provided that the AML unit led by this person 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 AMLCO's annual activity report is established separately from the annual activity report of the compliance function.

The NBB recommends that the AMLCO's annual activity report 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 activity report should contain 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 to respond to 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 AMLCO's annual activity report should mention 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 contain 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:
 - a. the nature, number and amount of the atypical transactions detected and transmitted to the AMLCO for analysis,
 - b. the nature, number and amount of the atypical transactions effectively analysed by or under the authority of the AMLCO,
 - c. the nature, number and amount of the reports of suspicious transactions to the CTIF-CFI (broken down by country of operation),
 - d. the number and nature of monitoring missions carried out to verify the implementation of policies, control measures and procedures by employees, agents, distributors and service providers, as well as the adequacy of monitoring resources deployed by the financial institution

- for AML/CFTP purposes,
- e. the nature and amount of the trainings provided and of the awareness-raising actions undertaken, and
 - f. 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;
 7. supervisory activities undertaken by the supervisor, including communications with the financial institution, as well reports submitted, violations identified and sanctions imposed, measures taken by the financial institution to remedy the violations identified and the current stage of such remedial action, without prejudice to any other periodic reports that may be required in the event of a supervisory activity or remedial action; and
 8. 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 AMLCO's annual activity report 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 activity 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 AMLCO's annual activity report 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 level of information provided in the annual activity report should be sufficient 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.

In order to better guarantee the quality of the activity reports produced by the AMLCOs of financial institutions and to ensure that these reports provide an effective added value for the senior management of the financial institutions to which they are addressed, in particular by avoiding that these reports are limited to referencing the content of internal policies and procedures or that they omit important information and, in general, with a view to increasing their relevance, the NBB has drawn up **an AMLCO report template:pdf - word**

The NBB invites financial institutions to adopt this template, with a view to:

- achieving an overall improvement in the quality of the AMLCO's activity report and, consequently, in the awareness of the senior management of financial institutions with regard to AML/CFT issues;
- secondarily, enabling the NBB to adopt a harmonised and coherent approach to processing the information reported to it annually in the area of AML/CFT by the financial institutions under its supervision (to this end, the NBB invites the AMLCOs of these financial institutions to provide it with a copy of their activity report in .docx file format - see the page Reporting by financial institutions).

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. This e-mail should include an organisational chart that shows the position of the respective function(s) within the financial institution and which reflects the hierarchical and functional lines of the function(s) concerned;

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

In addition to the above, more specifically for the appointment of a new senior officer responsible for AML/CFTP, the notification of this appointment should also include the following:

- the curriculum vitae of this person; and
- if the new senior officer responsible for AML/CFTP also performs another function which could give rise to a conflict of interest for that person, a description of the measures taken by the financial institution to prevent such a conflict from occurring.

In addition to the above, more specifically for the appointment of a new AMLCO, the notification of this appointment should also include the following:

- the curriculum vitae of this person;
- a justification of the appointment in the light of the conditions listed in Article 9 §2 of the Anti-Money Laundering Law; and
- if the AMLCO performs other functions or carries out other tasks within the financial institution or within the group to which it belongs, an estimate of the time actually spent on AML/CFTP tasks and an assessment of any conflicts of interest this combination of functions or tasks could give rise to.

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 not (or only to a very limited extent) exposed 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 dedicated to central contact points. 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 Anti-Money Laundering 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 (3rd subparagraph) (2) of the Anti-Money Laundering Law;
4. If the person concerned does not usually perform the 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 statutory and regulatory ML/FTP prevention framework, which are required by Article 9 §2 (3rd subparagraph) (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 financial institutions providing services in Belgium solely through (tied) agents or distributors

For

- European credit institutions and stockbroking firms that use a tied agent established in Belgium to perform investment services and/or activities there,
- European credit institutions that use an agent established in Belgium to provide services there consisting of receiving deposits or other repayable funds, and
- European payment institutions or electronic money institutions respectively providing payment services or distributing electronic money in Belgium solely through 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 persons who, at the head office of each of these institutions and in accordance with the law applicable in their country of origin:

- are responsible at the highest level for ensuring that the provisions of the Anti-Money Laundering Law and the other statutory and regulatory provisions referred to in the first subparagraph of Article 9 §1 of the Law are implemented and complied with in Belgium;
- perform the function of AMLCO, pursuant to Article 9 §2 of the Law.

With regard to the obligation to designate a central contact point (see Article 15 of the Anti-Money Laundering Law), please refer to the page dedicated to central contact points.

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:

1. deciding on the overall ML/FT risk management strategy of the financial institution concerned. The board of directors should therefore have appropriate knowledge, skills and experience to form an overall view of the policy implemented and the ML/FT risks associated with the activities performed and the business model, including knowledge of the statutory and regulatory framework for the prevention of ML/FTP;
2. validating the institution's AML/CFTP policy (see the page Policies, procedures, processes and internal control measures);
3. being informed of the results and updates of the institution's overall ML/FT risk assessment;
4. reviewing the AMLCO's activity report at least once a year and, more frequently in the interim, taking note of activities that expose the financial institution to higher ML/FTP risks;
5. assessing at least once a year the proper functioning of the compliance function, including its AML/CFTP component - inter alia on the basis of the conclusions of any internal and/or external audits performed on it - ensuring in particular the adequacy of the human and technical resources allocated to the AMLCO function.

The board of directors should have access to and consider high-quality and detailed data and information so that it is able to perform its AML/CFTP tasks effectively. At a minimum, the board of directors should have timely and direct access to the AMLCO's activity report, the report of the internal audit function, the findings and conclusions of external auditors where applicable, as well as findings of the supervisor, relevant communications with CTIF-CFI and supervisory measures or administrative sanctions imposed.

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.
 7. ensuring that any outsourcing of the AMLCO's operational tasks complies with applicable regulations (see point 1 of the page Performance of obligations by third parties), and that it receives regular reports from the service provider.

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 resolving

any dispute.

Risk classification

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 resolving any dispute.

Policies, procedures, processes and internal control measures

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

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 resolving any dispute.

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

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 on transactions and business relationships, to analyse atypical facts and transactions and report suspicions of ML/FT, as well as the obligations related to transfers of funds, embargoes and assets 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) (see the page “Main reference documents”).

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 facts and transactions and reporting of suspicions to CTIF-CFI** (see the page on this subject);
4. the measures required for compliance with the obligations related to **financial embargoes and assets freezing** and, where appropriate, with the European Regulation on **transfers of funds** (see the pages on these subjects);
5. **data and document retention and protection** (see the pages on this subject: “Data and document retention” and “Personal data processing and protection”); 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 data retention and protection (see the pages “Data and document retention” and “Personal data processing and protection”) 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 and independent sources of information” through which these data can be confirmed, and explicitly authorises the use of certain electronic identification means for this purpose; the degree of certainty required as to the identity of the persons involved is to be determined according to the risk level identified in the case concerned, based on the individual risk assessment. § 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 or the reliable and independent sources of information 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 or the reliable and independent sources of information 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 proof of registration of the relevant information in the said UBO register, which is to be collected in accordance with Article 29 of the Anti-Money Laundering Law, and the additional identification and identity verification measures to be adopted in accordance with the same Article when consulting the said 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. This requirement obviously does not apply where one of the electronic identification means of which the use is explicitly authorised by Article 27, § 1, of the Anti-Money Laundering Law is involved.

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 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 obligations to exercise due diligence on business relationships and occasional transactions. For further information, see the page "Anonymous or numbered accounts and contracts".

C. Procedure for due diligence on business relationships and occasional 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 “Due diligence on business relationships and occasional transactions and detection of atypical facts and 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 due diligence on business relationships and occasional transactions and to detect atypical facts and 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 “Due diligence on business relationships and occasional transactions and detection of atypical facts and 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 facts and 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 facts and transactions, reporting suspicions to CTIF-CFI and processing requests for information addressed by CTIF-CFI to the financial institution

The procedure for analysing atypical facts and transactions and reporting suspicions to 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 facts and transactions which staff members, agents or distributors are required to submit to the AMLCO in accordance with the procedure for due diligence on 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 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 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 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 persons in accordance with Article 57 of the Anti-Money Laundering Law.

For further information, see the pages “Analysis of atypical facts and transactions”, “Reporting of suspicions”, “Prohibition of disclosure” and “Protection of reporting persons”.

2.2.4. Procedure for monitoring transfers of funds and financial embargoes and implementing assets freezing measures

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

1) as regards the **rules on financial embargoes and assets 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 assets 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 assets 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 assets 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 data and document retention and protection

If the aspects on the data and document retention and protection 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 pages “Data and document retention” and “Personal data processing and protection”.

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 data and document retention and protection should list the information and documents to be retained, the retention period and the time when the retention period starts, as well as the modalities for the deletion of personal data at the end of the retention period. This procedure should ensure the confidentiality of the documents (storage, persons with access to them, etc.) and, to that end,

describe the terms for accessing the data contained therein, even if an external service provider is used to archive these 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 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 facts and 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 facts and 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 facts and 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 pages "Transfers of funds" and "Financial embargoes and assets 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 facts and 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 person reporting to 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 site's pages related to operational AML/CFTP obligations (for example Due diligence on business relationships and occasional transactions and detection of atypical facts and transactions, Analysis of atypical facts and transactions, Reporting of suspicions, etc.) also contain certain recommendations of the NBB on internal control and internal audit. See the 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 “Due diligence on business relationships and occasional transactions and detection of atypical facts and 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 resolving any dispute.

Training and education of staff

Statutory and regulatory framework

- 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 in turn on their technical knowledge and awareness of the critical need to prevent ML/FT transactions, both of which are the responsibility of the AMLCO (see the Governance page).

1. Education

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

2. Training

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

If the financial institution implements an awareness or training programme developed abroad, e.g. by its head office or parent company, the AMLCO should ensure that this programme is adapted to the statutory and regulatory provisions applicable in Belgium and to the institution's ML/FT typologies and specific activities.

As regards the *ratione personae* scope, training should be provided to all staff (regardless of their status) of the financial institution who are concerned by 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** should be adapted to the financial institution's organisation and take account of its

nature and size, as well as its ML/FT risk profile.

The **subject matter 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 for 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 tasked 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 risks*: training must enable them to adequately integrate AML/CFTP issues.

The training programme may include several sessions which, in accordance with the Anti-Money Laundering Law, should be 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 statutory 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 financial institution's 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 previously identified;
4. recent developments with regard to ML/FT risks in practice (typologies, risk factors, etc.);
5. the NBB reporting procedure ("external whistleblowing"); see the third subparagraph of Article 11 §1 of the Anti-Money Laundering Law.

The NBB also reminds financial institutions that training should be updated in light of any changes to the statutory and regulatory provisions and, more generally, 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 proper understanding** of the substance thereof by the staff concerned. To this end, the staff concerned can be asked to take a test after undergoing training. The financial institution should also be able to evidence to the NBB the training sessions given to staff concerned by ML/FT risks, as well as agents and distributors.

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

Internal whistleblowing

Statutory and regulatory framework

- 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 officer responsible for AML/CFTP of breaches of the Anti-Money Laundering Law on a confidential or anonymous basis and through a specific and independent 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 details (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 officer responsible for AML/CFTP.

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 officer responsible for AML/CFTP (in addition to, where applicable, the person responsible for the compliance function if this person is not the AMLCO) and (ii) the communication channels effectively ensure the confidentiality or anonymity of the whistleblowers.

Furthermore, in accordance with Article 11 (3rd subparagraph) of the Anti-Money Laundering Law, the AMLCO should, as part of his/her 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 is reflected in the level of sophistication required of the procedure to be adopted and the reporting system to be put in place, as described above. Such procedures and systems 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 resolving any dispute.

Organisation and internal control in groups

- **Belgian parent companies**
- **Belgian subsidiaries and branches**
- **Central contact points in Belgium of financial institutions governed by the law of another Member State**

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

Belgian parent companies

Statutory 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

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 resolving any dispute.

Belgian parent companies: Comments and recommendations

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 Definitions page).

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 giving rise to the risk is limited to a single entity of the group.

Thus, the parent entity governed by Belgian law which is at the head of a group should **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 statutory 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 should 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 should 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 should in particular (i) set up an 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.

To this end, the management committee should formally entrust the senior officer responsible for AML/CFTP, designated in the parent entity in accordance with Article 9 §1 of the Anti-Money Laundering Law (see point 1 of the Governance page), with the highest responsibilities at group level on AML/CFTP policy and internal control. The management committee should also appoint an AMLCO at group level. In this respect, it is the responsibility of the parent entity to determine, based on the nature, size and ML/FT risk profile of the entity and of the group, taking into account the weight of the tasks to be performed and the availability condition set out in Article 9 §2 of the Anti-Money Laundering Law, whether the group-level AMLCO function can be performed effectively by the AMLCO appointed at the parent entity level (see point 2 of the Governance page) or whether a separate group-level AMLCO should be appointed. This decision should be communicated to the Bank in accordance with the instructions in point 3 of the Governance page and, if necessary, adjusted if the underlying elements should change.

Where the management committee is informed, e.g. by members of the board of directors, the senior officer responsible for AML/CFTP or the group-level AMLCO, of supervisory activities carried out by a supervisor in group entities or of deficiencies identified in the course of such activities, it should ensure that the subsidiary or branch implements remedial measures in a timely and effective manner.

1.2. Group-level AMLCO

Group-level AMLCOs have the following tasks:

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-level 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 their coherence;
5. monitor branches and subsidiaries established in third countries for compliance with EU rules on AML/CFT, in particular where requirements to prevent ML/FT are less stringent than those in applicable EU texts;
6. establish group-wide policies, procedures and measures, particularly regarding data protection and intra-group information exchange related to AML/CFTP in accordance with national statutory provisions;
7. ensure that group entities have adequate procedures for reporting suspicious transactions and that they properly share information, including information that a suspicious transaction has been reported (without prejudice to any existing national confidentiality requirements).

There should be a direct reporting line between the AMLCO of a subsidiary or branch and the group-level AMLCO.

The group-level AMLCO should issue an activity report at least once a year and submit it to the group's management committee and board of directors. In addition to the topics mentioned in point 2.5 'Activity report by the AMLCO' of the Governance page, the group-level AMLCO's report should devote special attention to the aspects raised by the AMLCOs of the branches and subsidiaries, as mentioned in point 4 of the AMLCO activity report template. The Bank expects a single activity report to be prepared, covering topics at both the parent entity and group levels; this activity report should be prepared by the AMLCO at parent entity level and the group-level AMLCO - each in terms of their responsibilities - if these functions are performed by different persons (see point 1.1 in this regard).

The coordination at group level should not affect the legal capacity of subsidiaries and branches to meet their statutory 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 should be respected when AMLCO functions of local entities are outsourced in their entirety to the group-level 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 should 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 should 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 four aspects:

1. ML/FT risk assessment at group level;
2. customer acceptance;
3. information sharing within the group; and
4. data protection.

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 should 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 should be defined in accordance with the statutory 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.

2.2.3. Information sharing within 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 is 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 statutory obligations to report suspicions, and to ensure an appropriate follow-up of these reports within the group (cf. Article 56 §2 (1) and (2) of the Anti-Money Laundering Law).

Article 13 §1 of the Anti-Money Laundering Law specifies that, when required for the prevention of ML/FT, the following relevant information **must** be shared in particular between group entities:

- information on the identity and the characteristics of the customers;
- information on the identification of the agents and beneficial owners, where applicable;
- information relating to the purpose and nature of the business relationship;
- information on the transactions;
- and unless otherwise indicated by CTIF-CFI (or by another FIU where applicable), information on suspicious transaction reports involving the customers.

It is also recalled that Article 56 §2 (1) and (2) of the Anti-Money Laundering Law authorises, under the conditions specified therein, the disclosure of suspicious transaction reports and the sharing of information relating thereto (in particular, analyses that may lead to or have lead to identifying these transactions as suspicious) within groups of financial institutions (see the page Prohibition of disclosure). The NBB recommends to make use of this authorisation whenever relevant in order to achieve optimal effectiveness of the ML/FT prevention within the group. However, given the particularly sensitive nature of this information, it should be ensured that it is shared in accordance with terms and conditions providing satisfactory guarantees with regard to the confidentiality and use of the information shared, including guarantees to prevent disclosure thereof. Thus, this information should only be forwarded to those persons in the group who are in charge of AML/CFT and for whom this information may be useful in the performance of their tasks and responsibilities in this area, and this information should be exchanged via secure channels.

2.2.4. Data protection

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 should be defined in compliance with the statutory 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.

2.3. Internal procedures of the group

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

2.4. Implementation process at group level

To effectively coordinate the AML/CFTP policies applicable at local level, the group-level AMLCO should 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 should 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 should 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 Anti-Money Laundering 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 statutory 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 should 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 should 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 should 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 should 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 should apply **measures complementary** to those provided for locally to deal effectively with ML/FT risks. In addition, the Belgian parent company should 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 should 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, the first subparagraph of Article 38 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 should in principle require that subsidiary or branch, pursuant to the second subparagraph of Article 13 §3 of the Anti-Money Laundering Law, to implement such enhanced due diligence measures with regard to all its own local customers.

The NBB considers that the correct application of the above-mentioned statutory 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 statutory 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 statutory 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 statutory framework is likely to evolve over time, the NBB considers that parent entities should 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 statutory 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.

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 resolving

any dispute.

Belgian subsidiaries and branches

Legal and regulatory framework

- Anti-Money Laundering Law: Art. 13, § 1
- Anti-Money Laundering Regulation of the NBB: Art. 26

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 resolving any dispute.

Central contact points in Belgium of financial institutions governed by the law of another Member State

Legal and regulatory framework

- Regulatory Technical Standards on central contact points
- Anti-Money Laundering Law: Article 15
- Anti-Money Laundering Regulation of the NBB: Article 27

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 resolving any dispute.

Central contact points in Belgium of financial institutions governed by the law of another Member State: Comments and recommendations

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 (hereinafter “the Directive”), 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 3 March 2021).

To facilitate the effective implementation of the above principles, Article 15 of the Anti-Money Laundering Law requires financial institutions that are governed by the law of another EEA country and which provide financial services in Belgium “through one or more persons established in Belgium who represent the institution for that purpose” to appoint **a central contact point** (hereinafter referred to as “CCP”) **situated on Belgian territory**, “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”.

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 Directive's implementing measures, as 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 the law of 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.

Transactions that may involve cash or anonymous electronic money are particularly risky in terms of ML/FT, 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. This particularly risky nature is apparent (see the page “Main reference documents”):

- 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 in accordance with Article 6 of the Directive;
- from the EBA Risk Factor Guidelines dated 1 March 2021.

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 financial institution governed by the law of another EEA country offers financial services 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 financial institution, not the CCP, which is subject to the Anti-Money Laundering Law and which remains **responsible** for the proper performance of its legal and regulatory AML/CFTP obligations. Unlike the European financial institution concerned, which is responsible for the actions of its agents or distributors and of the CCP appointed by it 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 resolving any dispute.

Disclaimer: The content of this page is currently being reviewed and may be modified following the entry into force of the Law of 20 July 2020 containing various provisions on the prevention of money laundering and terrorist financing and on the restriction of the use of cash.

Performance of obligations by third parties

Statutory and regulatory framework

- Anti-Money Laundering Law: Articles 42 to 44
- Anti-Money Laundering Regulation of the NBB: Articles 19 to 21

Other reference documents

- BCBS Guidelines dated January 2014 on Sound management of risks related to money laundering and financing of terrorism (revised in July 2020) (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 resolving any dispute.

Performance of obligations by third parties: Comments and recommendations by the NBB

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 statutory 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 statutory 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 Governance page).

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 the page 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 the following tasks:

- the performance of ongoing supervision aimed at detecting atypical transactions or transactions carried out to or from persons or entities subject to asset freezing measures (N.B. The mere use, in this context, of external lists or databases does not formally fall under the definition of outsourcing, but constitutes a purchase of information. This use of external suppliers is without prejudice to the financial institution's compliance with its statutory AML/CFT obligations. This implies, inter alia, that the financial institution should regularly monitor the quality of the purchased product and take appropriate remedial action if the quality of the product proves to be inadequate),
- the analysis of atypical transactions in accordance with internal procedures,
- the collection of any additional information,
- the development of an opinion based on the above-mentioned analysis regarding the (non-)suspicious nature of the transaction under consideration,
- etc

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. The group's parent entity should:

- a. ensure that the relevant entities establish an inventory of instances of intra-group AML/CFT outsourcing specifying which task relates to which legal entity, and make this inventory regularly available for consultation; and

- b. ensure that intra-group outsourcing does not adversely affect the compliance of each of its subsidiaries, branches or other forms of establishment with AML/CFT obligations.

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 European financial institutions that carry out activities in Belgium through (tied) 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” to be appointed (see Article 15 of the Anti-Money Laundering Law and the page on central contact points).

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 statutory 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 on the 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 statutory and regulatory AML/CFTP obligations,
 - periodically and occasionally testing and monitoring the service provider for compliance with the obligations under the outsourcing agreement, 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 should 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 statutory 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. Regarding customer data, the AMLCO and the supervisor should have access rights to the service provider's systems/databases.
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 statutory 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 obligation of due diligence on business relationships and occasional transactions 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 statutory 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 statutory 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 (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 obligation of due diligence on occasional transactions and business relationships 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 statutory 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 statutory 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 statutory and regulatory provisions and the supervision imposed on the third party meet the equivalence conditions described above.

In contrast, Article 43 §2 of the Anti-Money Laundering Law prohibits obliged entities from using third-party business introducers established in high-risk third countries. However, the second subparagraph of §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 subparagraph of Article 43 §2 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 to verify this data, particularly, where appropriate, information obtained:

- through the use of electronic identification means such as those provided or recognised within the

- authentication service, confirming the identity of persons online, or
- through relevant trust services referred to in the eIDAS Regulation.

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 (2nd subparagraph) of the Money Laundering Law;

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

1. 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;
2. 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 statutory 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 resolving any dispute.

Brexit

Reference documents

- 22 December 2020 – Communication NBB_2020_050 / Application of Regulation (EU) 2015/847 on transfers of funds to transfers to the United Kingdom
 - 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 resolving any dispute.

Customer and transaction due diligence

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, safe-deposit boxes 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**
 - **Due diligence on business relationships and occasional transactions and detection of atypical facts and transactions**
 - **Special cases of enhanced due diligence**
 - Identity verification over the course of the business relationship and implementation of measures as an alternative to terminating a business relationship
 - High-risk third countries
 - States with low or no taxes
 - Correspondent relationships
 - Politically exposed persons (PEPs)
 - Recommended actions in the event of credible publications of mass fraud or ML/FT cases in the press
 - **Due diligence requirements and de-risking**
 - **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 resolving any dispute.

Individual risk assessment

Legal and regulatory framework

- Anti-Money Laundering Law: Article 19

Risk factors to be taken into account

- EBA Risk Factor Guidelines dated 1 March 2021

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 resolving any dispute.

Individual risk assessment: Comments and recommendations by the NBB

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 due diligence on business relationships and occasional transactions.

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 EBA Risk Factor Guidelines of 1 March 2021 (p. 37, paragraphs 3.5. and 3.6.), 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, an occasional transaction or their business. (...) 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 measures of due diligence on business relationships and occasional transactions 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 obligations of due diligence on business relationships and occasional transactions (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 “Due diligence on business relationships and occasional transactions 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.

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

Anonymous or numbered accounts, safe-deposit boxes and contracts

Legal and regulatory framework

- Anti-Money Laundering Law: Article 20
- Anti-Money Laundering Regulation of the NBB: Article 11

Comments and recommendations by the NBB

1. Accounts and safe-deposit boxes opened anonymously or under false names or pseudonyms

Article 20 of the Anti-Money Laundering Law prohibits financial institutions from opening accounts or safe-deposit boxes anonymously or under false names or pseudonyms for their customers.

As entering into a business relationship with a customer requires the latter to be identified, the anonymous opening of accounts or safe-deposit boxes, i.e. accounts or safe-deposit boxes where the identity of the account holder is not known, cannot be permitted. Likewise, no account or safe-deposit box 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 resolving any dispute.

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**

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

Persons to be identified

Legal and regulatory framework

- Anti-Money Laundering Law: Articles 21 to 25
- Anti-Money Laundering Regulation of the NBB: Article 10

Other reference documents

- EBA Risk Factor Guidelines dated 1 March 2021
- BCBS Guidelines dated January 2014 on Sound management of risks related to money laundering and financing of terrorism (revised in July 2020) (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 resolving any dispute.

Persons to be identified: Comments and recommendations by the NBB

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 (see the page “Main

reference documents".

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 150;
2. the maximum amount stored electronically does not exceed EUR 150;
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,
2. withdraws this value in cash, or
3. carries out remote payment transactions within the meaning of Article 2, 23° of the Law of 11 March 2018

if the amount redeemed, withdrawn or paid, as the case may be, exceeds EUR 50.

In these three 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 or at the time when the customer carries out remote payment transactions using electronic money** (that was previously issued without any such measures).

With regard to anonymous prepaid cards issued in third countries, the institutions referred to in Article 5, § 1, 4°, 6° and 7° of the Anti-Money Laundering Law, which offer payment services consisting in acquiring payments transactions, as referred to in point 5 of Annex I.A. of the Law of 11 March 2018, may accept payments made with such anonymous prepaid cards only if such cards comply with conditions equivalent to those laid down in the first and second paragraphs of the same Article of the Law. Where appropriate, these institutions must therefore have effective systems in place which enable them to check - at the time when the payment transaction is accepted - that these legal conditions are met and must immediately refuse the payment transaction if this should not be the case.

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 resolving any dispute.

Object of the identification and identity verification

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 (known as the “eIDAS Regulation”)
- Law of 18 July 2017 on electronic identification

Other reference documents

- Opinion of the ESAs dated 23 January 2018 on the use of innovative solutions by credit and financial institutions
- EBA Risk Factor Guidelines dated 1 March 2021
- FATF Guidance dated 4 November 2017 on AML/CFT measures and financial inclusion, with a supplement on customer due diligence
- BCBS Guidelines dated January 2014 on Sound management of risks related to money laundering and financing of terrorism (revised in July 2020) (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 resolving any dispute.

Object of the identification and identity verification: Comments and recommendations

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 in a precise, uniform and prescriptive manner the supporting documents or the reliable and independent sources of information that can be used to fulfil the obligation to verify the identity of the persons involved; although the Law explicitly authorises the use of certain electronic identification means, the degree of certainty required as to the identity of the persons involved is to be determined according to the risk level identified in the case concerned.

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, second paragraph, 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, third paragraph, 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

In accordance with Articles 26, § 1, and 27, § 1, of the Anti-Money Laundering Law, 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, and (ii) in order to have a sufficient degree of certainty as to the identity of the persons involved, 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 particular against information collected, where appropriate, through certain electronic identification means.

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 involved 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 Data and document retention) 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 in a precise, uniform and prescriptive manner the supporting documents or the reliable sources of information that may be used to verify the identification data of the person involved. It does, however, explicitly authorise checking these data against the information obtained, where appropriate:

- through electronic identification means such as those provided or recognised within the authentication service as referred to in Articles 9 and 10 of the Law of 18 July 2017 on electronic identification, confirming the identity of persons online; this may be, for example, an electronic identity card that will be read with a card reader, or a secure mobile means of identification; or
- through the relevant trust services referred to in the eIDAS Regulation; examples of such trust services are electronic signatures or advanced seals.

Therefore, each financial institution should include in its internal procedures precise rules concerning the supporting documents or the reliable and independent sources of information that it accepts for the purposes of identity verification and which must enable it to have, according to the risk level identified in the case concerned, a sufficient degree of certainty as to the identity of the persons involved.

These rules should be based on an assessment of the level of reliability of each of the supporting documents or each source of information – except, of course, where use is made of one of the electronic identification means expressly referred to in the Anti-Money Laundering Law - to ensure that this level is sufficient to achieve the objective set out in Article 27, § 1, of the said 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.

For further information on electronic identification means explicitly authorised in accordance with Article 27, § 1, of the Anti-Money Laundering Law, please refer to the explanatory memorandum of the amending Law of 20 July 2020 (see the page Main reference documents).

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. Use of innovative technological instruments other than the electronic identification means referred to in the Anti-Money Laundering Law

If a financial institution intends to make use of innovative technology other than the electronic identification means referred to in Article 27, § 1, of the Anti-Money Laundering Law to verify the identity of the persons involved in business relationships or occasional transactions, it is required to comply with Article 12, 1°, second paragraph, 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.

§ 4. 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, 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) and to the Law of 30 July 2018 on the protection of natural persons with regard to the processing of personal data. 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.

§ 5. 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.

Thus, Article 29 of the Anti-Money Laundering Law requires financial institutions, when entering into business relationships with companies incorporated in Belgium, trusts, foundations and (international) non-profit organisations or legal entities similar to *fiducies* or trusts, to collect proof of registration, in the register of beneficial owners, of information concerning the beneficial owners or to obtain an extract from such register.

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 or on an extract thereof 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. The nature of these measures must be determined according to a risk-based approach.

In low- and standard-risk situations, the NBB recommends that these additional measures at least include the reporting entity approaching the customer to obtain relevant information as to the identity of his beneficial owners, as well as supporting documents proving the identity of these persons or confirmation that the information in the UBO register is accurate, current and complete. These measures may also include consulting information published on the internet or any other available information, whether publicly available or, for example, available through external consultants for a fee.

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, where appropriate, the electronic identification means referred to in Article 27, § 1, of the Anti-Money Laundering Law.

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, first paragraph, 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.

In cases of high risk, financial institutions should also ensure that they know the customer's beneficial owners with a higher degree of certainty. Customers could thus be asked to fill in a beneficial owner

identification form and attach the necessary supporting documents (see point 3.3 below).

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 innovative technologies other than electronic identification means as referred to in Article 27, § 1, of the Anti-Money Laundering Law (see above) in high-risk situations, the NBB expects it to tighten the terms and conditions for the application of this authorisation.

With the exception of cases involving the use of electronic identification means as referred to in the Law, the financial institution should moreover 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.

When high ML/TF risks have been identified in the process of the individual risk assessment, the information and supporting documents provided by the customer regarding his beneficial owners (see point 3.2 above) should also be subject to enhanced scrutiny, including a comparison of the information thus obtained directly from the customer with that recorded in the UBO register and, to the extent possible, with information that can be obtained from other reliable and independent sources.

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 institution 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 requires the obliged entities to update the identification data they hold in the context of their business relationships, 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 Due diligence on business relationships and occasional transactions and detection of atypical facts and 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.

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

Time of identification and identity verification

Legal and regulatory framework

- Anti-Money Laundering Law: Articles 30 to 32
- Anti-Money Laundering Regulation of the NBB: Article 14

Other reference documents

- EBA Risk Factor Guidelines dated 1 March 2021
- BCBS Guidelines dated January 2014 on Sound management of risks related to money laundering and financing of terrorism (revised in July 2020) (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 resolving any dispute.

Time of identification and identity verification: Comments and recommendations by the NBB

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 150;
2. the maximum amount stored electronically does not exceed EUR 150;
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,
2. withdraws this value in cash, or
3. carries out remote payment transactions within the meaning of Article 2, 23° of the Law of 11 March 2018

if the amount redeemed, withdrawn or paid, as the case may be, exceeds EUR 50.

In these three 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 or at the time when the customer carries out remote payment transactions using electronic money (that was previously issued without any such measures).

With regard to anonymous prepaid cards issued in third countries, the institutions referred to in Article 5, § 1, 4°, 6° and 7° of the Anti-Money Laundering Law, which offer payment services consisting in acquiring payments transactions, as referred to in point 5 of Annex I.A. of the Law of 11 March 2018, may accept payments made with such anonymous prepaid cards only if such cards comply with conditions equivalent to those laid down in the first and second paragraphs of the same Article of the Law. Where appropriate, these institutions must therefore have effective systems in place which enable them to check - at the time the payment transaction is accepted - that these legal conditions are met and must immediately refuse the payment transaction if this should not be the case.

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 resolving any dispute.

Non-compliance with the identification and identity verification obligation

Legal and regulatory framework

- Anti-Money Laundering Law: Article 33 , § 1
- Anti-Money Laundering Regulation of the NBB: Article 15

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 resolving any dispute.

Non-compliance with the identification and identity verification obligation: Comments and recommendations by the NBB

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 “Due diligence on business relationships and occasional transactions 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 resolving any dispute.

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

Legal and regulatory framework

- Anti-Money Laundering Law: Article 34

Other reference documents

- EBA Risk Factor Guidelines dated 1 March 2021
- BCBS Guidelines dated January 2014 on Sound management of risks related to money laundering and financing of terrorism (revised in July 2020) (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 resolving 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

Contents

- 1. Obligation to identify the customer's characteristics and the purpose and nature of the business relationship or the occasional transaction
- 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 characteristics of the customers they have identified in accordance with the Law, 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 due diligence obligations with regard to business relationships and occasional transactions (see the page “Due diligence on business relationships and occasional transactions and detection of atypical facts and 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, please refer to the explanatory memorandum of Article 34, § 1, of the Anti-Money Laundering Law (see the page “Main reference documents”).

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, 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. 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 150;

2° the maximum amount stored electronically does not exceed EUR 150;

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,

2° withdraws this value in cash, or

3° carries out remote payment transactions within the meaning of Article 2, 23° of the Law of 11 March 2018 if the amount redeemed, withdrawn or paid, as the case may be, exceeds EUR 50.

In these three 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 or at the time when the customer carries out remote payment transactions using electronic money** (that was previously issued without any such measures).

With regard to anonymous prepaid cards issued in third countries, the institutions referred to in Article 5, § 1, 4°, 6° and 7° of the Anti-Money Laundering Law, which offer payment services consisting in acquiring payments transactions, as referred to in point 5 of Annex I.A. of the Law of 11 March 2018, may accept payments made with such anonymous prepaid cards only if such cards comply with conditions equivalent to those laid down in the first and second paragraphs of the same Article of the Law. Where appropriate, these

institutions must therefore have effective systems in place which enable them to check - at the time the payment transaction is accepted - that these legal conditions are met and must immediately refuse the payment transaction if this should not be the case.

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 “Due diligence on business relationships and occasional transactions 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 due diligence that financial institutions must exercise with regard to business relationships and occasional transactions pursuant to Article 35, § 1, of the Anti-Money Laundering Law, for more information see the page “Due diligence on business relationships and occasional transactions 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 resolving any dispute.

Due diligence on business relationships and occasional transactions and detection of atypical facts and transactions

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

Other reference documents

- Communication NBB_2018_21 / Horizontal control analysis examining a sample of transactions carried out through tied agents of different payment institutions
- EBA Risk Factor Guidelines dated 1 March 2021
- BCBS Guidelines dated January 2014 on Sound management of risks related to money laundering and financing of terrorism (revised in July 2020)

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 resolving any dispute.

Due diligence on business relationships and occasional transactions and detection of atypical facts and transactions: Comments and recommendations by the NBB

Contents

- 1. Detection of atypical facts and transactions
- 2. Updating of the data or information and of the individual risk assessment
- 3. Inability to exercise ongoing due diligence
- 4. Internal control measures

The obligation to exercise due diligence on business relationships and occasional transactions 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 all transactions carried out on an occasional basis or over the course of the business relationship, by a customer identified pursuant to Article 21, § 1, of the Law; this obligation includes 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, in the case of business relationships – on which due diligence must be exercised on an ongoing basis - 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 obligation to exercise due diligence on business relationships and occasional transactions, 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 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 EEA 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 or on an occasional basis that appear complex or that are unusually large, as well as transactions conducted in an unusual pattern or that do not have an 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 occasional 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. complex or unusually large transactions);
- 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 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 threats, retaliatory measures 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 (see the page "Protection of reporting persons").

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 due diligence obligation is that financial institutions must keep up to date the data or information they hold, in the context of their business relationship, pursuant to their obligation to identify and verify the identity of the customer and their obligation to identify the characteristics of the customer as well as the purpose and nature of the business relationship.

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 carried out over the course of a business relationship 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 over the course of a business relationship may imply also updating the individual risk assessment and, where appropriate, adapting the extent or modalities of the ongoing 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. Inability to exercise ongoing due diligence

Article 35, § 2 of the Anti-Money Laundering Law describes the consequences of the inability to fulfil the due diligence obligation.

As this obligation must be fulfilled either with respect to an occasional transaction which is planned to be carried out, or throughout a business relationship, the Anti-Money Laundering Law distinguishes between future customers (planned occasional transactions or new business relationships) and existing customers (existing business relationships).

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 occasional 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 on an occasional basis where the financial institution has, in advance, reason to believe that it will not be able to meet its (ongoing) due diligence obligation with respect to the business relationship or the transaction 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 and continuously 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 obligation of due diligence on business relationships and occasional transactions 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 business relationships and occasional transactions are consistently complied with and that the processes for implementing the 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 resolving any dispute.

Special cases of enhanced due diligence

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

- General commentary on cases of enhanced due diligence
- **Identity verification over the course of the business relationship and implementation of measures as an alternative to terminating a business relationship**
- **High-risk third countries**
- **States with low or no taxes**
- **Correspondent relationships**
- **Politically exposed persons (PEPs)**
- **Recommended actions in the event of credible publications of mass fraud or ML/FT cases in the press**

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

Identity verification over the course of the business relationship and implementation of measures as an alternative to terminating a business relationship

Legal and regulatory framework

- 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 resolving any dispute.

Identity verification over the course of the business relationship: Comments and recommendations by the NBB

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 “Due diligence on business relationships and occasional transactions 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 resolving any dispute.

High-risk third countries

Legal and regulatory framework

- Anti-Money Laundering Law: Article 38

Other reference documents

- EBA Risk Factor Guidelines dated 1 March 2021
- Commission Delegated Regulation (EU) 2016/1675 of 14 July 2016 on high-risk third countries, as amended by Delegated Regulation 2022/229 of 7 January 2022 (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 resolving any dispute.

High-risk third countries: Comments and recommendations by the NBB

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 EBA Risk Factor Guidelines dated 1 March 2021 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 resolving any dispute.

States with low or no taxes

Legal and regulatory framework

- Anti-Money Laundering Law: Article 39

Other reference documents

- EBA Risk Factor Guidelines dated 1 March 2021

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 resolving any dispute.

States with low or no taxes: Comments and recommendations by the NBB

Contents

- 1. Target situations
- 2. Enhanced due diligence measures
- 3. Reporting to the AMLCO
- 4. Internal control measures

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, § 1/2, third paragraph, of the Income Tax Code 1992. These are 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 is regularly updated, 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 “Due diligence on business relationships and occasional transactions 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 “Due diligence on business relationships and occasional transactions 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 resolving any dispute.

Correspondent relationships

Legal and regulatory framework

- Anti-Money Laundering Law: Article 40

Other reference documents

- EBA Risk Factor Guidelines dated 1 March 2021
- BCBS Guidelines dated January 2014 on Sound management of risks related to money laundering and financing of terrorism (revised in July 2020) (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 resolving any dispute.

Correspondent relationships: Comments and recommendations by the NBB

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 aforementioned 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°, 4° to 7°, 9° to 14° and 16° to 22°, of the Anti-Money Laundering Law establishes a cross-border correspondent relationship involving the execution of payments **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**. These measures must be taken prior to establishing a business relationship. 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 (see the page "Main reference documents").

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 5, § 1, 1°, 4° to 7°, 9° to 14° and 16° to 22°, 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 as referred to in Article 5, § 1, 1° and 3° to 22° of the Law 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.

The concept of "shell bank" is defined in 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 resolving any dispute.

Politically exposed persons (PEPs)

Legal and regulatory framework

- Anti-Money Laundering Law: Article 41 and Annex IV

Other reference documents

- EBA Risk Factor Guidelines dated 1 March 2021
- BCBS Guidelines dated January 2014 on Sound management of risks related to money laundering and financing of terrorism (revised in July 2020) (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 resolving any dispute.

Politically exposed persons (PEPs): Comments and recommendations by the NBB

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 who are exposed to particular risks because of the (political, judicial or administrative) prominent public functions they hold or have held. While the Law of 11 January 1993 limited the notion of PEPs to foreign residents, the Anti-Money Laundering Law also includes PEPs residing in Belgium. Thus, the distinction according to whether the PEP resides in Belgium, in an EEA Member State or in a third country is no longer made. It should also be noted that the notion of PEP refers to prominent public functions and not to middle-ranking or more junior functions.

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.

In order to facilitate the practical application of this definition and to enhance legal certainty with regard to the identification of politically exposed persons in the European Union, Directive 2015/849 also requires each EEA Member State (i) to issue and keep up to date a list indicating the exact functions which it considers to be prominent public functions in accordance with its national laws, regulations and administrative provisions, and (ii) to request each international organisation accredited on its territory to issue and keep up to date a list of prominent public functions at that international organisation. Those lists may be made public and must be sent to the European Commission, which will issue, based on the lists received from all the Member States and its own list, a single list of the functions concerned and make it public.

The list of the exact functions thus qualified by Belgium as prominent public functions is set out in Annex IV of the Anti-Money Laundering Law.

Pursuant to Article 41, § 4, of the Law, in conjunction with the definition in Article 4, 28°, **the following persons in particular must therefore be considered as PEPs**: natural persons who hold or have held one of the public functions:

- listed in Annex IV of the Anti-Money Laundering Law, and
- mentioned in the single list published by the European Commission (functions which qualify as prominent public functions in other Member States and international organisations).

The decision as to whether a customer, an agent of the customer or a beneficial owner of the customer is a politically exposed person in a third country should be based solely on the definition in Article 4, 28°, of the Law.

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, although some of them are accurately listed in its Annex IV, 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 or in Annex IV thereto 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, § 1, of the Anti-Money Laundering Law stipulates that financial institutions should have “*appropriate risk management systems, including adequate risk-based procedures, to determine whether the customer with whom they establish or have a business relationship or for whom they carry out an occasional transaction, an agent of the customer or a 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. In particular, any use of this data for commercial purposes is prohibited (see Article 41, § 4, third paragraph, of the Anti-Money Laundering Law); 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 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 "Due diligence on business relationships and occasional transactions and detection of atypical facts and transactions"), 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, third paragraph, 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, at the latest at the time of the payment of benefits or at the time of the partial or total transfer of the insurance policy 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 “due diligence on occasional facts and transactions), 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 resolving any dispute.

Recommended actions in the event of credible publications of mass fraud or ML/FT cases in the press

In the event of credible publications of mass fraud or ML/FT cases in the Belgian and/or international press, financial institutions and in particular their AMLCO should thoroughly analyse these publications and assess whether they themselves or certain customers or business relationships are affected by the fraud or ML/FT cases.

If this proves to be the case, financial institutions should take the published information into account when applying their risk-based approach (see the page Risk-based approach and overall risk assessment), in particular by updating the data or information available to them in the context of their business relationships and, where appropriate, by also carrying out a new individual risk assessment on the basis of the published information (see in particular point 2 of the page Due diligence on business relationships and occasional transactions and detection of atypical facts and transactions).

Furthermore, affected financial institutions should detect and analyse atypical facts and transactions in view of the published information (see the pages Due diligence on business relationships and occasional transactions and detection of atypical facts and transactions and Analysis of atypical facts and transactions).

Finally, where necessary, financial institutions should report (additional) suspicions to CTIF-CFI (see the page Reporting of suspicions).

The NBB further requests financial institutions to inform it proactively and without delay of any involvement in such publications. The institutions concerned should indicate which specific actions they have taken or will take in this respect (mentioning any “lessons learnt” where appropriate). They should also notify the NBB of the results of internal investigations and analyses.

Due diligence requirements and de-risking

Reference documents

- EBA statement dated 27 April 2022 on financial inclusion in the context of the invasion of Ukraine
- Circular NBB_2022_03 of 1st February 2022 / Prudential expectations in relation to the "de-risking" phenomenon
- EBA Opinion and report dated 5 January 2022 on de-risking and its impact on access to financial services
- Circular NBB_2016_32 of 12 July 2016 / 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)

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 resolving any dispute.

Due diligence requirements and de-risking: Comments and recommendations by the NBB

Contents

- 1. Implications of the overall risk assessment and customer acceptance policy
- 2. Individual risk assessment and refusal to enter into a business relationship on grounds related to ML/FT
- 3. Updating individual risk assessments and terminating existing business relationships
- 4. The cost of due diligence
- 5. The risk of administrative remedial measures, administrative sanctions and civil or criminal convictions

Since the entry into force of the Anti-Money Laundering Law, the NBB has noted an increase in the number of de-risking actions by financial institutions under its remit that allege reasons related primarily to AML/CFT.

“De-risking” is defined here as the decision in principle, taken a priori by a financial institution, to refuse to enter into business relations with potential customers or to terminate existing business relations with current customers on the grounds that these potential or existing customers belong to a category of persons which the financial institution alleges is linked to excessive ML/FT risks, inter alia in view of its risk appetite or the AML/CFT system it has put in place. The NBB notes that a significant number of undertakings and professionals from various sectors have been confronted with this phenomenon. At present, the NBB observes that de-risking is mainly practised by financial institutions from the banking sector, but it cannot be ruled out that this phenomenon may also spread within the other financial sectors supervised by the NBB.

While decisions not to enter into or terminate a business relationship, or not to carry out a transaction, may be consistent with the requirements of the Anti-Money Laundering Law, de-risking entire categories of customers without due regard to individual customers’ risk profiles is a sign of ineffective ML/FT risk management and can have a significant impact.

In its capacity as the supervisory authority designated by Article 85, § 1, 3°, of the Anti-Money Laundering Law, the NBB is of the opinion that financial institutions under its supervision must effectively implement mechanisms to prevent and manage ML/FT risks.

The NBB also recognises that the business relations between a financial institution and its customers are essentially governed by the principle of contractual freedom which, barring legal exceptions, does not allow a party (in this case, a financial institution) to be obliged to enter into a contractual relationship to which it has not freely consented. The NBB wishes to point out that the scope of these comments and recommendations is limited to such de-risking as results from inadequate implementation by financial institutions of their obligations under the applicable legal and regulatory provisions on AML/CFT.

Entities under the NBB’s supervision are reminded that effective application of the anti-money laundering law and regulations does not exempt them from complying fully and simultaneously with other mandatory or public-order legislation that is also binding on them (see the page Due diligence obligations and compliance with other legislation). This is the case e.g. with the legislation on combating discrimination, Article VII

55/12 of the Code of Economic Law, which grants payment institutions objective, non-discriminatory and proportionate access to the payment account services of credit institutions, as well as the provisions of Book VII, Title 3, Chapter 8, of the Code of Economic Law on access to payment accounts and the basic banking service.

The NBB also stresses that financial institutions are expected to assume their specific responsibility for the economic development of society as effectively as possible, without prejudice to the legal and regulatory provisions applicable to them.

Although some financial institutions may have tried to justify their restrictive and defensive behaviour in the context of implementing their procedure for accepting new customers or terminating existing business relationships by their desire to strictly manage the reputational risk to which they are exposed, it should be noted that these very behaviours might damage their reputation if, as a result, they were to be accused of not fully or satisfactorily assuming their specific societal responsibilities, or even of promoting discriminatory behaviour in the exercise of their activities, of hindering economic development and financial inclusion, of participating in the destabilisation of the financial system or of disregarding some of their legal public-order obligations.

Moreover, where financial institutions adopt such restrictive and defensive behaviours, they may fail to contribute effectively to the prevention of ML/FT, instead rejecting out of any control transactions that may be related to ML/FT issues.

The NBB therefore expects financial institutions under its jurisdiction to take great care in defining and implementing balanced AML/CFT policies which, while ensuring effective implementation of the obligations set out in or under the Anti-Money Laundering Law, also enable them to comply with all their other legal public-order or mandatory obligations and to fulfil all their specific societal responsibilities.

On the basis of Article 86, § 2, 1°, of the Anti-Money Laundering Law, the NBB hereby addresses a number of comments and recommendations to financial institutions under its remit to assist them in achieving this balance.

These comments and recommendations take full account of the statements issued by the FATF on 23 October 2014, 26 June 2015 and 23 October 2015 dealing specifically with de-risking, as well as the various sets of Guidance in which it clarified the scope of the risk-based due diligence obligations of financial institutions and took a position on the issue of de-risking.

Reference is made in particular to the following sets of Guidance:

- Guidance dated 4 November 2017 on AML/CFT measures and financial inclusion, with a supplement on customer due diligence
- 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 27 October 2014 for a Risk-Based Approach for the Banking Sector
- 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

These comments and recommendations also take full account of the European Banking Authority (EBA) publications on de-risking:

- EBA Opinion and Report dated 22 January 2022 on de-risking and its impact on access to financial services ;
- Pre-existing provisions in EBA instruments that help to address the main drivers of de-risking decisions (see the list on pages 29 et seq. of the above-mentioned EBA Report).

The NBB urges financial institutions to take note of these publications and to take them into account when implementing their legal obligations to prevent ML/FT.

1. Implications of the overall risk assessment and customer acceptance policy

It appears that some financial institutions have tried to justify their refusal to enter into business relations with a number of customers on the grounds that their customer acceptance policy would prohibit entering into business relations with persons in the category to which the potential customer concerned belongs. In this respect, note should be taken of the following.

Pursuant to Article 7 of the Anti-Money Laundering Law, the entities under supervision, including financial institutions, are required to implement the AML/CFT measures required by the Law in a differentiated manner, depending on their assessment of ML/FT risks, in particular due diligence measures with respect to transactions and business relationships.

In order to do so, the entities under supervision are required to carry out an “overall risk assessment” in accordance with Article 16 of the Anti-Money Laundering Law, taking into account risk factors relating to customers, products and services offered, distribution channels and relevant geographical areas (see the page Risk-based approach and overall risk assessment).

It is therefore not only appropriate but also mandatory that, on the basis of their overall risk assessment, entities should classify according to ML/FT risks the various categories of customers to whom they offer their financial services and products, taking into account their general characteristics (natural persons or legal entities, residence in Belgium or abroad, economic sector of activity, sources of income or wealth, etc.). This classification of customers, combined with that resulting from other risk factors relating inter alia to the financial products or services requested, the distribution channel used or the geographical areas to which the customers or their transactions are linked, must enable them to establish, in accordance with Article 4 of the Anti-Money Laundering Regulation of the NBB, an appropriate risk classification to take into account the characteristics of all the activities conducted.

The aim of risk classification is to ensure that financial institutions are able to apply appropriate due diligence measures in each specific situation (see the page Risk classification). Based on the overall risk assessment, the risk classification provides the basis for each financial institution to define risk-differentiated policies, procedures, processes and internal control measures as required by Article 8 of the Anti-Money Laundering Law (see the page Policies, procedures, processes and internal control measures).

In particular, according to the NBB's recommendations, financial institutions' AML/CFT policies should include a “customer acceptance policy” which “[i]n terms of principles, (...) 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 may be envisaged that acceptance of certain categories of customers with high ML/FT risks may be conditional on the implementation of specific risk mitigation measures. Risk mitigation measures may include (but are not limited to):

- providing the financial institution with better guarantees as to the honesty of the customer's approach in general (e.g. the customer's formal commitment to respect labour and social law in Belgium or the communication of an extract from the criminal record which must be free of any recent conviction for one of the crimes underlying the ML/FT, as listed in the Anti-Money Laundering Law);
- providing the financial institution with guarantees of honesty and transparency in the conduct of the customer's transactions (e.g. by requiring documentation of the transactions, such as a copy of the invoice to be paid, or even a document from the customer's auditor certifying that they have carefully examined the transaction in question and have not detected any indication of ML/FT);
- adapting, without prejudice to other applicable legal provisions, the offer of products and services to high-risk customers by limiting or excluding from such offer those products and services identified in the overall risk assessment as being most likely to be used for ML/FT purposes;
- facilitating the understanding and management of ML/FT risks through organisational measures (e.g. by centralising the management of business relationships with certain categories of customers in a centre of expertise).

In the context of these same recommendations, the NBB made a point of emphasising 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.”* The NBB also specifies that this policy should include, inter alia, the listing of general criteria for allocating customers to the various risk categories, and the principles for the differentiated allocation of the power to decide to enter into the business relationship or to carry out the transaction requested by the customer to persons of an appropriate hierarchical level in relation to each risk category. (See point 2.1.2. of the NBB’s Comments and Recommendations on Internal Control Policies, Procedures, Processes and Measures).

The NBB thus confirms that it is not appropriate, nor is it consistent with AML/CFT legal and regulatory requirements, for a financial institution's customer acceptance policy to exclude all business relationships with potential or existing customers on the basis of general criteria such as, inter alia, their belonging to a particular economic sector or a link to a high-risk country (without prejudice to any other legal provisions that may be applicable or measures to implement binding financial embargo provisions).

Thus, for example, the NBB considers that it would be inappropriate and inconsistent with AML/CFT legal and regulatory provisions for the customer acceptance policy of a “generalist” credit institution, whose service offering includes the provision of payment accounts to all of its customers, to prohibit a priori the provision of this service to certain categories of natural or legal persons on the basis of their

membership of a particular economic sector.

The NBB therefore urges financial institutions whose acceptance policy includes such provisions to repeal them as soon as possible.

2. Individual risk assessment and refusal to enter into a business relationship on grounds related to ML/FT

It appears that some financial institutions have tried to justify their refusal to enter into business relationships with certain customers by alleging that the Anti-Money Laundering Law prohibits them from entering into such business relationships where there is a high risk of ML/FT.

The NBB emphasises that the Anti-Money Laundering Law does not formulate such a prohibition, but instead requires a financial institution to implement enhanced due diligence measures in situations where it identifies high ML/FT risks. In this respect, one should bear in mind the following.

In accordance with Article 19 of the Anti-Money Laundering Law, financial institutions are required to carry out an “individual risk assessment” as soon as they enter into a business relationship with a customer or when the customer requests them to carry out an occasional transaction of EUR 10,000 or more. This individual risk assessment should enable the financial institution concerned to determine, in accordance with its customer acceptance policy, the scope and intensity of the due diligence measures implemented, according to the ML/FT risks specifically associated with the customer concerned.

As a reminder, the due diligence measures required are as follows:

- To identify and verify the identity of the customer and, where applicable, of their agent(s) and beneficial owner(s);
- To assess the characteristics of the customer and the purpose and proposed nature of the business relationship or occasional transaction; and
- To exercise continuous due diligence with regard to the business relationship and the customer's transactions.

Certain de-risking decisions may have originated from an inadequate interpretation of the scope of these due diligence requirements, in particular in the context of correspondent banking activities or with regard to payment institutions. As the FATF itself has pointed out (see Guidance dated 21 October 2016 on Correspondent Banking, p. 3), the NBB confirms in this respect that where the customer is another financial institution, the due diligence obligations relate to that financial institution in its capacity as customer, and do not include implementing due diligence measures in respect of the customers of that client financial institution (“KYCC”). In this regard, reference is made to the commentary on Article 23 of the Anti-Money Laundering Law in its preparatory works, which explicitly states that “[w]here transactions are intended to enable a financial institution to effectively provide its own customers with the products and services it offers, these transactions are to be considered as transactions for the financial institution's own account, and not for the account of its customers. In this case, the latter do not have the possibility of determining any of the terms and conditions of these transactions. This is the case, for example, where a credit institution takes out interbank loans to finance its loan portfolio or where it uses the clearing and settlement services provided by another financial institution to ensure the proper execution of the services it offers to its customers in the area of payments or securities transactions.” (Chambre des représentants / Kamer van volksvertegenwoordigers,

2016-2017, DOC 54 2566/001, p. 109. See on the AML/CFT site: Explanatory Memorandum to the Anti-Money Laundering Law, Article 23, point A3: Articles 21 to 25).

The absence of a systematic legal obligation on KYCC does not preclude the examination of atypical transactions carried out by the client financial institution in accordance with Article 45 of the Anti-Money Laundering Law in order to determine whether they are suspicious of being related to ML/FT (e.g. due to a significant and unanticipated increase in the amount of the transactions carried out by the client financial institution, the counterparties or beneficiaries of such transactions, their country of establishment, etc.). In this case, the client financial institution may be asked for additional information on the transactions of its customers underlying the detected atypical transaction in accordance with § 1, second subparagraph, of Article 45 of the Anti-Money Laundering Law. In this respect, reference is made to the page Analysis of atypical facts and transactions. Attention is drawn to the commentary on this provision in the explanatory memorandum to the Anti-Money Laundering Law, which states that “[n]evertheless, the information available to [the institution] in this way may be insufficient to enable it to decide whether there are suspicions of ML/FT. In this case, the second subparagraph of § 2 requires the entity under supervision to take (at the initiative of its AMLCO) such additional measures to those already applied in the context of ongoing due diligence as are necessary to be able to assess whether or not such transactions or activities seem suspicious.” (Chambre des représentants / Kamer van volksvertegenwoordigers, 2016-2017, DOC 54 2566/001, p. 155. See on the AML/CFT site: Explanatory Memorandum to the Anti-Money Laundering Law, Articles 45 and 46).

Concerns have also been expressed that when, conversely, a Belgian financial institution maintains correspondent banking relationships as a client of a foreign correspondent institution, the latter may refuse or terminate the business relationship on the grounds that the Belgian institution accepts to serve customers with a high ML/FT risk profile, and that this Belgian institution may thereby lose its access to the currency market of the third country concerned. However, the NBB notes that, much more than the risk profile of the client institution's customers, it is the quality and effectiveness of the due diligence measures implemented by this client institution, taking into account the risk profile of its customers, that are analysed by the correspondent bank (for example by using the Wolfsberg Group Correspondent Banking Due Diligence Questionnaire, which focuses extensively on the ML/FT prevention measures implemented by the client bank), with the aim of ensuring as much as possible that any criminal financial flows are identified and reported by the client bank to the competent local authorities before being injected into the correspondent banking relationship.

In order to properly implement all due diligence requirements on the basis of the risks, and in addition to the risk criteria identified in general by the overall risk assessment and reflected in the customer acceptance policy, the individual risk assessment should enable the financial institution to take into account characteristics that are specific to the customer (e.g. where the customer is a professional who is himself exposed to the risk of being used by third parties for ML/FT purposes, the quality of the measures the customer has implemented themselves to manage and reduce this risk), the product or service requested (e.g. the particular terms or conditions requested by the customer), the distribution channel (e.g. the particular circumstances surrounding the request to enter into a business relationship) or any links with risky geographical areas (e.g. the nature and intensity of these links). This individual risk assessment should either confirm the level of risk that is determined on the basis of the risk criteria that have been identified generally for all customers, or lower or raise the level of risk where specific information so requires.

Article 19, § 2, second subparagraph, of the Anti-Money Laundering Law specifies that where the individual risk assessment associated with a business relationship leads the financial institution to identify high risks, the institution is obliged to take enhanced due diligence measures.

For more details on the individual risk assessment, please refer to the page Individual Risk Assessment, and in particular to the EBA Guidelines of 1 March 2021 on ML/TF risk factors and the NBB's Comments and Recommendations published there.

In this context, the NBB notes that the Anti-Money Laundering Law only provides for a prohibition on entering into or continuing the business relationship in a limited number of cases, namely:

- Where entities under supervision cannot fulfil their obligations to identify and verify the identity of the customer, or, where applicable, of the customer's agents or beneficial owners (Article 33, § 1, first subparagraph, of the Anti-Money Laundering Law),
- Where entities under supervision cannot fulfil their obligation to assess the characteristics of the customer and the purpose and nature of the business relationship (Article 34, § 3, first subparagraph, of the Anti-Money Laundering Law), and
- Where they have reason to consider that they will not be able to satisfy:
 - their obligation to scrutinise the transactions carried out during the business relationship and, if necessary, the origin of the funds, or
 - their obligation to update the identification data of the customer and of any agents and beneficial owners of the customer, as well as other information collected which is necessary to assess the characteristics of the customer and the purpose and nature of the business relationship

(Article 35, § 2, first subparagraph, of the Anti-Money Laundering Law).

Consequently, the NBB is of the opinion that the refusal to enter into a business relationship on the basis of the Anti-Money Laundering Law is only required by the above-mentioned legal provisions in situations where the financial institution concerned can justify that it is unable to comply with the due diligence obligations concerned.

However, these prohibitions do not apply merely because the financial institution's individual risk assessment has determined that high ML/FT risks are associated with the business relationship, so that enhanced due diligence measures are required by law.

Where the financial service or product for which the financial institution is solicited by the customer is consistent with the financial institution's habitual range of financial services and products, the financial institution must, pursuant to Article 8 of the Anti-Money Laundering Law, have the appropriate AML/CFT organisation and internal control mechanisms in place with respect to its "business model". This internal AML/CFT scheme must enable it to adequately manage all ML/FT risk situations that may arise in the context of the activities covered by its business model, including high-risk situations. In this context, the NBB considers that the mere fact that the implementation of enhanced measures requires the financial institution to perform additional or more intensive work than in the case of more ordinary risks in order to meet its due diligence obligations does not mean that the situation is so impossible for the financial institution that it must refuse to enter into a business relationship.

On the other hand, where the business relationship requested by the customer is not consistent with the ordinary offer of financial services or products that fall within its business model or commercial strategy, the effective exercise of the above-mentioned due diligence obligations may require substantial changes to its organisation and internal control measures. Where such changes are not justified in the light of the financial institution's business model, the NBB considers that the failure to meet the above due diligence requirements may be due to the fact that the financial institution cannot reasonably be expected to have the appropriate

organisation and internal control mechanisms to manage the ML/FT risks that are specific to this business relationship situated outside its business model.

The NBB would also like to point out that where a financial institution is obliged to refuse a customer's request to enter into a business relationship in application of the above-mentioned articles of the Anti-Money Laundering Law, it is also obliged to examine, in accordance with Article 46 of the Law, whether the reasons for the failure to comply with the due diligence obligations are such as to give rise to a suspicion of ML/FT and whether CTIF should be informed. In this respect, reference is made to Article 33, § 1, second subparagraph, Article 34, § 3, second subparagraph, and Article 35, § 2, second subparagraph, of the Anti-Money Laundering Law.

In view of the above, the NBB considers that the provisions of Articles 33, § 1, first subparagraph, 34, § 3, and 35, § 2, of the Anti-Money Laundering Law should only be invoked to justify the refusal to enter into a business relationship requested by the customer in cases where the entity under supervision can justify that it is proven impossible for it to fulfil the due diligence obligations imposed by the Anti-Money Laundering Law.

The NBB also recommends that in such cases, in accordance with Article 24 of the Anti-Money Laundering Regulation of the NBB, the entity should carefully establish and keep in its records: (i) the individual risk assessment and the justification for the impossibility of fulfilling the legal due diligence obligations on which the refusal to enter into a business relationship is based, and (ii) an analysis of the causes of this impossibility that led to determining whether or not CTIF should be informed.

3. Updating individual risk assessments and terminating existing business relationships

As noted in some cases of refusal to enter into a business relationship, it appears that some financial institutions have tried to justify the termination of existing business relationships with certain customers by alleging that the Anti-Money Laundering Law prohibits them from maintaining such business relationships where it is revealed in the course of the business relationship that high ML/FT risks are associated with it.

As is well known, Article 35, § 1, first subparagraph, 2°, of the Anti-Money Laundering Law requires updating the identification data and information relating to the characteristics of the customer and the purpose and nature of a relationship as held by a financial institution, in particular where elements relevant to the individual risk assessment referred to in Article 19 of the Law have been modified. The individual risk assessment must be updated whenever events occur that may have such significant influence on the risks associated with the business relationship that the due diligence measures implemented might no longer be adequate and sufficient in view of the new level of risks. The NBB has also considered that, in order to ensure the current relevance of individual risk assessments, internal procedures may usefully provide for a periodic review of these assessments and the information held on which they are based, where this is appropriate to the activities carried out (see the pages Due diligence on business relationships and occasional transactions and detection of atypical facts and transactions: Comments and recommendations by the NBB, 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, and Individual risk assessment: Comments and recommendations by the NBB).

Where the individual risk reassessment leads to an increase in the level of risk that the financial institution

associates with the business relationship, the Anti-Money Laundering Law requires the financial institution to also increase the level of due diligence it exercises in respect of that business relationship.

As in the case of entering into a business relationship, the Anti-Money Laundering Law does not however require the financial institution to terminate the business relationship if the level of risk is higher than previously assessed, except in cases where the financial institution:

- cannot fulfil its obligation to update and verify the identification data of the customer or, where applicable, of their effective authorised representatives or beneficial owners (Article 33, § 1, first subparagraph, of the Anti-Money Laundering Law),
- cannot fulfil its obligation to update its assessment of the characteristics of the customer and the purpose and nature of the business relationship (Article 34, § 3, first subparagraph, of the Anti-Money Laundering Law), or
- has reason to believe that it will not be able to satisfy:
 - its obligation to scrutinise the transactions carried out during the business relationship and, if necessary, the origin of the funds, or
 - its obligation to subsequently update the identification data of the customer and of any authorised representatives and beneficial owners, as well as other information collected which is necessary to assess the characteristics of the customer and the purpose and nature of the business relationship

(Article 35, § 2, first subparagraph, of the Anti-Money Laundering Law).

The comments made above regarding the impossibility of fulfilling the relevant obligations in the case of entering into a business relationship are equally applicable.

However, the NBB would like to point out that where a suspicious transaction report has been sent to CTIF, the financial institution must update the individual risk assessment of the customer concerned by the report, in accordance with Article 22 of the Anti-Money Laundering Regulation of the NBB. In this context, the analysis of the intensity of the suspicion of money laundering or terrorist financing, of the amount or frequency of the suspicious transactions, may lead the financial institution to consider that the enhanced due diligence measures that it could implement with regard to the customer concerned would not allow it to sufficiently protect itself from the risk of being involuntarily involved in future money laundering or terrorist financing transactions by the customer, and to decide to terminate the business relationship with the customer.

In view of the above, the recommendations made by the NBB in the previous chapter apply, *mutatis mutandis*, where a financial institution terminates a business relationship due to its inability to fulfil its due diligence obligations.

4. The cost of due diligence

It appears that some financial institutions have sought to justify their refusal or termination of business relationships with certain customers by invoking the costs of performing the due diligence required by the Anti-Money Laundering Law, particularly where high ML/FT risks are associated with the business relationship. As a rule, the cost of AML/CFT controls is covered by the ordinary fees that financial institutions charge their customers for the provision of their financial services and products. Their pricing policy does not necessarily differentiate between the different levels of ML/FT risk associated with business

relationships, as reflected in the risk classification.

In this respect, although the implementation of AML/CFT due diligence is intended to reduce the potential future costs that ML/FT risks are likely to generate if they materialise, and which may be extremely heavy or even unbearable for financial institutions, the NBB is aware that, like all internal control measures of any kind, the implementation of the due diligence measures required by the Anti-Money Laundering Law generates an immediate cost which increases where, due to a high level of ML/FT risks, the law requires an increased level of due diligence. The NBB therefore does not rule out that, in compliance with any other legislation that may be applicable, the additional cost of implementing additional due diligence measures may be objectively reflected in the charges that financial institutions apply to their customers.

On the other hand, the NBB is not of the opinion that it would be legitimate for a financial institution to de-risk categories of customers on the grounds that the pricing of the products and services provided would be insufficient to cover the costs incurred by the exercise of due diligence required by the Anti-Money Laundering Law.

In view of the above, it could be accepted that financial institutions, to the extent legally permitted, take into account the objectively assessed cost of the due diligence measures required by the Anti-Money Laundering Law in pricing the financial services and products they offer to their customers. The NBB considers that it may be legitimate to apply differentiated charges according to the nature and level of due diligence required, provided that such differentiation can be objectively justified in such a way that it cannot be qualified as discriminatory or prohibitive.

5. The risk of administrative remedial measures, administrative sanctions and civil or criminal convictions

It appears that some financial institutions have also tried to justify their refusal to enter into business relations with certain customers or their decision to terminate them by invoking the risk of being subject to administrative remedial measures as listed in Articles 93 and 94 of the Anti-Money Laundering Law or to administrative sanctions as defined in Article 132 of the Law, or even criminal sanctions based on Article 505 of the Criminal Code in the event that the customer uses the financial relationship to carry out ML/FT transactions. Where suspicious transaction reports are sent to CTIF and the funds concerned are frozen as a result, there is also a risk that the customer will file a claim for compensation if the report to CTIF was not made in good faith.

It should be stressed, however, that when considering whether to impose the above-mentioned administrative measures or to initiate an administrative sanction procedure against a financial institution, the NBB will take into account, in accordance with the positions adopted in this respect by the FATF (see in particular its statement of 23 October 2015 and the 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), the fact that the risk-based approach that financial institutions are legally obliged to implement does not strictly ensure that they cannot be misused for ML/FT purposes.

Consequently, administrative remedial measures are not systematically imposed or administrative sanction procedures initiated whenever the NBB finds that the due diligence obligations required by the Anti-Money Laundering Law have only been imperfectly implemented in the context of particular business relationships, or in every case where suspicious transactions have not been detected and reported to CTIF. In the face of

such findings, the NBB will determine whether it is necessary and appropriate for it to take serious measures of this nature on the basis of an assessment of the seriousness of the established facts. Criteria shall be taken into account for this purpose such as the amounts involved, the repetitive nature of the breaches or the fact that the breaches are the result of clear and inexcusable negligence or a known serious deficiency in the internal organisation that has not been remedied, or, a fortiori, when they are the result of a deliberate act.

Administrative measures or sanction procedures may be justified in particular if the NBB has serious indications that the breaches observed result in the financial institution not being able to cooperate effectively in the prevention of ML/FT as required by law.

With regard to the risk of criminal sanctions based on Article 505 of the Criminal Code, the NBB wishes to stress that it has no competence in criminal matters and cannot, in particular, give an opinion on the conditions under which a financial institution, its directors or employees may be prosecuted and sentenced under this article of the Criminal Code as perpetrators, co-perpetrators or accomplices in a criminal money laundering offence.

The NBB also notes that in cases where suspicious transaction reports have been sent to CTIF, the civil and criminal immunity granted by Article 57 of the Anti-Money Laundering Law is not absolute, but subject to the condition that the suspicious transaction report has been sent “in good faith”. The interpretation of this notion is not a matter for the NBB, but for the Courts of law. Where this condition is not met, the risk of a claim for compensation or prosecution and criminal sanction cannot be excluded. Nevertheless, the NBB considers that Article 57 of the Anti-Money Laundering Law, like Article 37 of Directive 2015/849 of 20 May 2015 and FATF Recommendation 21, which it transposes, aims to provide security for entities under supervision that report suspicions in good faith, by protecting them from possible prosecution, particularly judicial prosecution, including prosecution based on the money laundering transactions they have reported.

It should also be recalled in this respect that, in civil law, the case law indicates that “good faith” as referred to above presupposes in particular that the atypical transactions by customers have been the subject of a specific analysis, as required by Article 45 of the Anti-Money Laundering Law, which effectively takes into account all the information held by the financial institution or which results from such additional measures to those referred to in Articles 19 to 41 of the Law as are necessary to support this analysis, and which the financial institution is required to implement, pursuant to the same Article 45 of the Law.

The NBB wishes to bring back to mind that the best way for financial institutions to avoid the risk of serious administrative measures or sanctions for breaches of the Anti-Money Laundering Law, or even the risk of criminal prosecution for assisting money laundering transactions by its customers, and the risk of claims in civil courts due to reports made to CTIF without due analysis, is to ensure the effective implementation of appropriate and effective money laundering prevention measures, including and especially in cases where high ML/FT risks are identified.

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

Due diligence requirements and compliance with other legislation

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

See the page “Personal data processing and protection”.

3. Basic banking services

Financial institutions should take into account the impact of the legislation regarding 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 resolving any dispute.

Analysis of atypical transactions and reporting of suspicions

- **Analysis of atypical facts and transactions**
- **Reporting of suspicions**
- **Prohibition of disclosure**
- **Protection of reporting persons**

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

Analysis of atypical facts and transactions

Legal and regulatory framework

- Anti-Money Laundering Law: Articles 45 and 46
- Anti-Money Laundering Regulation of the NBB: Articles 16 to 18

Other reference documents

- Guidelines of CTIF-CFI of 15 August 2020 for obliged entities referred to in Article 5 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 regarding the reporting 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 resolving any dispute.

Analysis of atypical facts and transactions: Comments and recommendations by the NBB

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 “Due diligence on business relationships and occasional transactions and detection of atypical facts and 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 proceeds of 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 trafficking in narcotic drugs and psychotropic substances;
- d. illicit trafficking in goods and merchandise, and weapons, including anti-personnel mines and/or submunitions;
- e. smuggling of 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 crime."

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. Laundering of the proceeds of 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 laundering of the proceeds of 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, § 1/2, third paragraph, of the Income Tax Code 1992. In this respect, see the page “States with low or no taxes”.

See also the page “Due diligence on business relationships and occasional transactions and detection of atypical facts and transactions” for a list of indicators of atypical transactions that may lead to suspicions of serious fiscal fraud.

§2. Laundering of the proceeds of social fraud

The list of predicate offences in the Anti-Money Laundering law has been updated to include social fraud and computer crime.

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.

The NBB invites financial institutions to consult CTIF-CFI's activity reports on this subject.

§ 3. Laundering of the proceeds of computer crime

The concept of "computer crime" is used in the Anti-Money Laundering Law to cover, on the one hand, offences where a computer system is the target of the criminal activity, i.e. acts directed against a computer system or the data it contains (e.g. unauthorised access to a computer system, also known as hacking), and, on the other hand, offences where a computer system is used merely as a tool to commit a criminal activity (e.g. the distribution of paedophile images via computer networks).

The NBB invites financial institutions to consult CTIF-CFI's activity reports on this subject.

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 due diligence on business relationships and occasional transactions (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 the section “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 transactions** that meet at least one of the following conditions: (i) they are complex, (ii) they are unusually large, (iii) they are conducted in an unusual pattern, and (iv) they do not have an 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 on 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”.

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 the principle set out in Article 47, § 1, second paragraph, 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 recommends that the **internal audit function** 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 resolving any dispute.

Reporting of suspicions

Legal and regulatory framework

- Anti-Money Laundering Law: Articles 47 to 54
- Anti-Money Laundering Regulation of the NBB: Article 22

Other reference documents

- Guidelines of CTIF-CFI of 15 August 2020 for obliged entities referred to in Article 5 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 regarding the reporting 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 resolving any dispute.

Reporting of suspicions: Comments and recommendations by the NBB

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 invites financial institutions to consult the guidelines of CTIF-CFI regarding the reporting of information to it.

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 referred to in Article 5, § 1, of the Anti-Money Laundering Law, i.e. to financial institutions governed by Belgian Law and to Belgian branches of foreign financial institutions, as well as to certain financial institutions governed by the law of another EEA Member State which are subject to the Belgian Anti-Money Laundering Law on the grounds that they offer services in Belgium through (tied or independent) agents or distributors. In this respect, please refer to the page "Scope".

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, information should in principle be reported and submitted to CTIF-CFI by the **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 financial institutions that use agents or distributors in Belgium and which meet the criteria outlined on the page dedicated to central contact points, 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 the guidelines of CTIF-CFI regarding the reporting of information to it.

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

A reporting of suspicions should contain at least the following information:

- 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 immediately 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 persons;
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 persons".

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 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 recommends that the internal audit function 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.

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

Prohibition of disclosure

Legal and regulatory framework

- Anti-Money Laundering Law: Articles 55 and 56

Other reference documents

- Guidelines of CTIF-CFI of 15 August 2020 for obliged entities referred to in Article 5 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 regarding the reporting 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 Article 55, § 1, second paragraph, of the Anti-Money Laundering Law, read in conjunction with Article 56, § 2, 2°, of the same Law, the prohibition of disclosure also applies to communication of information or intelligence by Belgian financial institutions to their branches and subsidiaries established in third countries if no adequate measures have been taken to ensure that these branches or subsidiaries effectively apply a group policy in accordance 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 Article 56, § 1, 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 “Personal data processing and protection”.

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 or that a money laundering or terrorist financing analysis is being, or may be, carried out with respect to a particular customer, provided that 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.

2.4. Information sharing with tied and exclusive agents

Tied and exclusive agents of financial institutions subject to the supervision of the NBB exercise their professional activities within the framework of a mandate. Consequently, such agents cannot be considered as third parties vis-à-vis the obliged entity for which they carry out a mandate. The prohibition of disclosure laid down in Article 55 of the Anti-Money Laundering Law is therefore not applicable to financial institutions in their relationship with tied and exclusive agents.

This does not necessarily mean, however, that tied and exclusive agents have the right to be informed by the

financial institution for which they carry out a mandate of all analyses or reportings to CTIF-CFI regarding transactions carried out by customers for whom these agents act on behalf of the financial institution, or of the precise reason for terminating a customer relationship or refusing a transaction.

In concrete terms, such information may only be transmitted by an obliged entity to its tied and exclusive agents if that is necessary for the proper implementation, by these agents, of the mandate entrusted to them to apply the internal AML/CFT procedures of the financial institution. Purely commercial considerations on the part of the agent (e.g. protection of his turnover) should therefore be regarded as insufficient justification for obtaining such information.

If this information were to be communicated to the agent, he would in any case be prohibited from transmitting it to the customer or to third parties, pursuant to Article 55 of the Anti-Money Laundering Law. Any violation of this prohibition should be considered as serious professional misconduct on the part of the agent.

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

Protection of reporting persons

Legal and regulatory framework

- Anti-Money Laundering Law: Articles 57 to 59

Other reference documents

- Guidelines of CTIF-CFI of 15 August 2020 for obliged entities referred to in Article 5 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 regarding the reporting of information to CTIF-CFI

Comments and recommendations by the NBB

1. Exemption from liability for reporting persons

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 person 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 persons

Article 58 of the Anti-Money Laundering Law aims to protect reporting persons 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.

3. Protection of judicial authorities

The protection of AMLCOs who report suspicious transactions and of the financial institutions that employ them is further strengthened by Article 59 of the Anti-Money Laundering Law, which provides that the authorities competent for investigations and prosecutions, such as CTIF-CFI or the Public Prosecutor's Offices, should take specific measures to ensure that reporting persons are legally protected from any threats, retaliatory measures or hostile actions.

Reporting persons that would be exposed to such threats, retaliatory measures or hostile actions or to adverse or discriminatory employment actions for having reported a suspicion of ML/FT, internally or to CTIF-CFI, may furthermore file a complaint with the competent authorities, without prejudice to the additional possibility offered to this entity to make use of the reporting mechanism set up by the NBB pursuant to Article 90 of the Anti-Money Laundering Law (external whistleblowing).

For more information on this subject, please refer to the Explanatory Memorandum of the Anti-Money Laundering Law (see the page “Main reference documents”) and to the page “External whistleblowing”.

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

Transfers of funds

Legal and regulatory framework

- Regulation (EU) 2015/847 of 20 May 2015 on information accompanying transfers of funds (unofficial coordinated version of 1 January 2020)
- 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 resolving any dispute.

Transfers of funds: Comments and recommendations by the NBB

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.

Furthermore, the financial institution is expected, in accordance with Articles 8, § 2, and 12, § 2, of Regulation 2015/847 to inform the NBB of cases where a PSP **repeatedly fails** to provide the required information on the payer or the payee, and of the measures it has taken as a result thereof. In order to assess when a PSP should be considered to be ‘repeatedly failing’ to provide the required information, please refer to the quantitative and qualitative criteria laid down in the ESAs Joint Guidelines (see points 47 et seq.). These guidelines also list the information to be provided, where appropriate, to the competent supervisory authorities. This information should be communicated to the NBB's AML/CFT supervision team at the following e-mail address: supervision.ta.aml@nbb.be. The NBB itself will subsequently inform the EBA.

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 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 behinds 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 identification of PSPs or IPSPs that **repeatedly fail to provide the required information** and the measures to be taken with regard to these service providers.

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 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 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.

Financial embargoes and assets freezing

Legal and regulatory framework

- Anti-Money Laundering Regulation of the NBB: Article 23

Other reference documents

- FATF Guidance dated June 2021 on proliferation financing risk assessment and mitigation
- 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 resolving any dispute.

Financial embargoes and assets freezing: Comments and recommendations by the NBB

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 types of 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 Due diligence on business relationships and occasional transactions 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. It applies to financial institutions governed by Belgian law (i.e. which are established in Belgium). Parent companies under Belgian law that are at the head of a group as defined in Article 4, 22°, of the Anti-Money Laundering Law should also ensure that all other institutions of this group take into account the national list of the Member State or third country where they are established. This provision is subject to any intragroup outsourcing agreements stipulating that the parent company will carry out the screening for each of these institutions.

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 outgoing 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 (N.B.: the NBB also considers it useful that the

monitoring system allows for the detection of the originators of incoming financial transactions. If it appears that the originator (and only the originator) of the incoming financial transaction is included on an official list of sanctions applicable in Belgium, the execution of the incoming financial transaction would not lead to assets being made available to such a person or entity and therefore would not infringe the rules on financial embargoes and assets freezing; however, from the perspective of ML/FT prevention, such a transaction should be considered as atypical or even suspicious and a review of the risk profile of the customer and related persons may be required, where appropriate accompanied by a reporting of suspicions to CTIF-CFI - see point 5.4. below).

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 his 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).

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-CFI (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.

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

Data and document retention

Statutory and regulatory framework

- Anti-Money Laundering Law: Articles 60 to 63
- Anti-Money Laundering Regulation of the NBB: Article 24

Other reference documents

- See the reference texts on the website of the Data Protection Authority
- Guidelines of CTIF-CFI of 15 August 2020 for obliged entities referred to in Article 5 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 regarding the reporting 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 resolving any dispute.

Data and document retention: Comments and recommendations by the NBB

Contents

- 1. Document retention modalities
- 2. Procedure

1. Document retention modalities

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, as referred to in Article 27, including:

- a. where applicable, information obtained through electronic identification means provided or recognised within the authentication service as referred to in Articles 9 and 10 of the Law of 18 July 2017 on electronic identification, confirming the identity of persons online;
- b. where applicable, information obtained through relevant trust services referred to in Regulation 910/2014.

The aforementioned documents and information are kept **for a period of ten years from the end of the business relationship with the customer or from the execution of the occasional transaction;**

2° the documents describing the measures taken to comply with the verification obligation in the case referred to in the third subparagraph of Article 23 §1 of the Anti-Money Laundering Law, including the information on any difficulties that arose during the verification process. These documents are kept **for a period of ten years from the end of the business relationship with the customer or from the execution of the occasional transaction;**

3° without prejudice to compliance with any other legislation 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 execution of the transaction;**

4° the written report on the analysis of atypical transactions, which may result in reporting to CTIF-CFI, as well as the report drawn up in case the due diligence requirements cannot be fulfilled, **for a period of ten years from the execution of the underlying transaction** (according to the same terms and conditions as set out in point 3° 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 (see the second subparagraph of Article 60 of the Anti-Money Laundering Law). This period is also reduced to seven years for information and documents regarding business relationships ended or transactions concluded up to 5 years prior to the date of entry into force of the Anti-Money Laundering Law (see Article 62 §2 of the Law). It should be noted that, by complying with this 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 I.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 provided that these documents have not been modified or altered in the meantime. Financial institutions considering making use of this derogation should specify in advance, in their internal 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 statutory 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.

In accordance with Article 62 §1 of the Anti-Money Laundering Law, financial institutions are obliged to delete personal data at the end of the aforementioned retention periods.

2. Procedure

In order to apply the rules set out in point 1 above in practice, the NBB expects financial institutions to develop a document retention procedure (see also the page Policies, procedures, processes and internal 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 resolving any dispute.

Personal data processing and protection

Legal and regulatory framework

- Anti-Money Laundering Law: Articles 64 and 65

Other reference documents

- See the reference texts on the website of the Data Protection Authority

Comments and recommendations by the BNB

- Comments and recommendations

Personal data processing and protection: comments and recommendations by the NBB

Contents

- 1. Introduction and processing purposes
- 2. Derogation from common law
- 3. Internal policies and procedures

1. Introduction and processing purposes

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, at assisting in monitoring, detecting and examining customer transactions involving sums likely to be derived from a criminal activity falling under the concept of money laundering or to participate in the financing of terrorism, or at detecting 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.

2. Derogation from common law

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. This provision derogates from the general rules 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 (usually referred to as the “General Data Protection Regulation” or “GDPR”), on the ground that the participation of financial institutions in AML/CFT is a public interest task and that the processing of these data is based on, and necessary for the fulfilment of, the legal obligations imposed on these financial institutions.

As regards the application of the general rules on personal data protection, please refer to the website of the Data Protection Authority and, in particular, to its recommendations in this area.

As regards the application of these rules in the specific context of AML/CFT, please refer to the comments on the processing of personal data by obliged entities set out on page 97 et seq. of the Explanatory Memorandum of the Amending Law of 20 July 2020 (see the page “Main reference documents”).

3. Internal policies and procedures

Financial institutions should ensure that their customer acceptance policies and their internal procedures are compatible with the applicable provisions of the GDPR, while also taking into account the special provisions laid down in this regard in Articles 64 and 65 of the Anti-Money Laundering Law.

Restriction of the use of cash

Legal and regulatory framework

- Anti-Money Laundering Law: 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 resolving any dispute.

Restriction of the use of cash: Comments and recommendations by the NBB

Contents

- 1. General rule for restricting the use of cash
- 2. Exceptions
- 3. Extension of the rule to postal deposits
- 4. Proof
- 5. Sanctions
- 6. 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 section of the Anti-Money Laundering Law (Articles 66 and 67). This section 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 section 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. 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**, or its equivalent in another currency, as part of one or several transactions that seem to be related”.

1.1. Scope

1.1.1. *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.

1.1.2. *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.

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.

Finally, pursuant to Article 67, § 3, third paragraph, of the Anti-Money Laundering Law, “the set of amounts mentioned in an official or unofficial accounting, that do not relate to one or more specific debts” should be irrefutably presumed to be carried out or received as part of linked transactions. This refers to the situation where an accounting is so non-transparent that it is impossible to attribute amounts, which are often less than EUR 3 000, to specific debt payments; in that case, these payments are considered as a single payment and are subject as a whole to the cash limit of EUR 3 000.

2. Exceptions

2.1 Exemption for obliged entities for which cash transactions are considered inherent to their activities

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], nor to their customers 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 for 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, credit institutions governed by the law of another EEA Member State which rely on a tied agent established in Belgium to provide investment services and/or perform investment activities there, and credit institutions governed by the law of another EEA Member State which rely on an agent established in Belgium to provide services there consisting of receiving deposits or other repayable funds;
- 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 EEA Member State that carry out their activities in Belgium through agents or distributors; and
- stockbroking firms governed by Belgian law, Belgian branches of European or non-European stockbroking firms, and stockbroking firms governed by the law of another EEA Member State which rely on a tied agent established in Belgium to provide investment services and/or perform investment activities there.

Conversely, the restriction on cash transactions applies in particular to:

- life insurance companies governed by Belgian Law and Belgian branches of European or non-European life insurance companies;
- central securities depositories, and
- mutual guarantee societies.

2.2 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”, thus **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 by other means than 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.

2.3 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. Apart from the exceptions provided for in the Law (particularly public auctions or sales/purchases of old jewels, for which payment or receipt in cash is still authorised up to EUR 3 000), Article 67, § 2, second paragraph, of the Anti-Money Laundering Law prohibits any payment carried out or received in cash of:

- the purchase/sales price of copper cables, when the buyer is a professional;
- the purchase/sales price of old or precious metals, when both seller and buyer are professionals; however, when the seller is a consumer and the buyer is a professional, the payment or receipt, in cash, of the purchase/sales price of the same goods is allowed, but subject to a maximum limit of EUR 500 (and to an obligation for the professional buyer to identify the selling consumer).

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 paragraph, 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, please refer to the Explanatory Memorandum of the Anti-Money Laundering Law (see the page “Main reference documents”).

3. Extension of the rule to postal deposits

In order to prevent the misuse of postal deposits for the purpose of circumventing the maximum limit of EUR 3 000 on cash payments and donations, the Anti-Money Laundering Law extends this restriction to postal deposits made on bank accounts held by financial institutions established in Belgium (a restriction which is generally already applied in practice) or on postal current accounts. Furthermore, these deposits may only be made by consumers (see Article 67, § 4, of the Anti-Money Laundering Law). For more information on this subject, please refer to the Explanatory Memorandum of the Anti-Money Laundering Law (see the page “Main reference documents”).

4. 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, please refer to the Explanatory Memorandum of the Anti-Money Laundering Law (see the page “Main reference documents”).

5. 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, please refer to the Explanatory Memorandum of the Anti-Money Laundering Law (see the page “Main reference documents”).

6. 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, third 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 in the context of their customer and transaction due diligence obligation.

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

Supervision by the NBB

- **New institutions**
 - **Reporting by financial institutions**
 - **External whistleblowing**
 - **Supervisory powers, measures and policy of the NBB**
 - **National cooperation**
 - **International cooperation**
-

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

New institutions

Legal and regulatory framework

- Anti-Money Laundering Law: Article 91

Comments and recommendations by the NBB

- Comments and recommendations

New institutions: Comments and recommendations

Any institution that submits a request for authorisation to the NBB which, when granted, will subject it to the Anti-Money Laundering Law and, more specifically, to the NBB's AML/CFTP supervision, is required to provide the NBB at least two months before the start of its commercial activities in Belgium with the following documents and information in the authorisation file:

- information on the overall risk assessment (also called business-wide risk assessment) required by Article 16 of the Anti-Money Laundering Law, which makes it possible to identify and properly manage or, where appropriate, limit the inherent ML/FT risks to which the financial institution will be exposed in Belgium. The expected content and form of this reporting are specified on the page "Reporting by financial institutions";
- the organisation put in place within the institution for AML/CFTP matters (particularly with regard to the functioning of the three lines of defence model, the hierarchical lines or the reporting lines);
- the AML/CFTP policies and procedures, in line with local requirements, that will apply to the activities in Belgium (see the page "Policies, procedures, processes and internal control measures"), including the different SLAs that could be concluded for outsourcing AML/CFT tasks (see the page "Performance of obligations by third parties");
- the necessary information on the person designated as senior officer responsible for AML/CFTP and the person designated as AMLCO (see the page "Governance"), including at least:
 - the curriculum vitae of these persons;
 - an organisational chart that shows the position of these functions within the financial institution and which reflects their hierarchical and functional lines;
 - if the senior officer responsible for AML/CFTP also performs another function which could give rise to a conflict of interest for that person, a description of the measures taken by the financial institution to prevent such a conflict from occurring;
 - if the AMLCO performs other functions or carries out other tasks within the financial institution or within the group to which it belongs, an estimate of the time actually spent on AML/CFTP tasks and an assessment of any potential conflicts of interest this combination of functions or tasks could give rise to;
 - if a single person serves as both the senior officer responsible for AML/CFTP and as the AMLCO, the justification for applying the principle of proportionality;
- the schedule for the launch of the activities in Belgium and information on the planned business model and volume of business.

If the institution intends to simultaneously or within a short time frame open subsidiaries, branches or other types of establishments in other EEA Member States or in third countries, the file should also include the policies and procedures at group level, including the process applied by the entities of the group for assessing the risks to which they are exposed, as well as a description of the methods used by the Belgian institution to monitor the compliance of their branches, subsidiaries or other types of establishments with these policies and procedures (see the page "Belgian parent companies").

Financial institutions governed by the law of another EEA Member State or of a third country that have undertaken to establish a subsidiary or branch in Belgium should provide proof that the AML/CFTP policy drawn up at group level which is applicable in the subsidiary or branch has been reviewed for compliance with Belgian legal and regulatory requirements (see the page "Belgian subsidiaries and branches"). In addition, the NBB considers that the AMLCO of a branch in Belgium should be appointed among employees

that are physically based in that branch (see point 2.2.2. of the page “Governance” and point 3. of the page “Belgian subsidiaries and branches”).

Finally, financial institutions governed by the law of another EEA Member State or of a third country that are established on Belgian territory in a form other than a branch or subsidiary in order to offer financial services or products there, should refer to the page “Central contact points”.

Reporting by financial institutions

Legal and regulatory framework

- Anti-Money Laundering Law: Article 91

Comments and recommendations by the NBB

- Circular NBB_2023_01 / Periodic questionnaire on combating money laundering and terrorist financing
- Circular NBB_2022_04 of 15 February 2022 concerning the prudential expectations regarding the AMLCO activity report
- 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 resolving any dispute.

Reporting by financial institutions: Comments and recommendations

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 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 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, measures and policy of 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 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 complete the questionnaire aimed at credit institutions.

Circular NBB_2023_01 / Periodic questionnaire on combating money laundering and terrorist financing

- Questionnaire credit institutions pdf - word
- Questionnaire life insurance companies pdf - word
- Questionnaire stockbroking firms pdf - word
- Questionnaire payment institutions and electronic money institutions pdf - word
- 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 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.

The answers to the questionnaire must be submitted to the NBB through OneGate by **15 May of each year.**

The electronic form in which the requested information must be provided is available in OneGate **from 1 April 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. 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.

2.4 Procedure for answering the questionnaire

a) Answering the questions

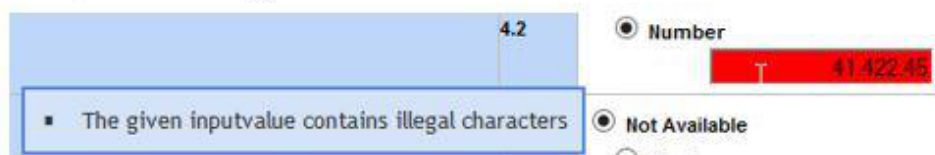
In the electronic form that will be available in OneGate, each financial institution should provide the necessary information by selecting in the drop-down menu, for each question, the answer that best suits its organisation (e.g. 'yes', 'no' or 'not applicable').

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.

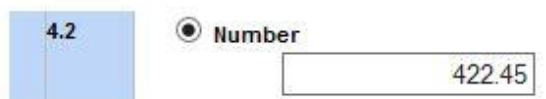
Please note:

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 page Governance. The NBB invites financial institutions to use the activity report template prepared by it, which is available on the same page.

Each financial institution is expected to send a copy of the aforementioned activity report to the NBB in accordance with the rules below.

3.2 Deadline for submission

The copy of the AMLCO's activity report should be sent to the NBB **no later than 15 May of the year following the year to which it relates**. Life insurance companies, however, should respect the reporting dates laid down in the eCorporate 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 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 which do not conduct activities in Belgium or are not (or only to a very limited extent) exposed 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). 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 the page 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 resolving any dispute.

Business-wide ML/TF risk assessment

- Overview
- Example
- Questionnaire

Periodic questionnaire

Circular NBB_2022_06 / Periodic questionnaire on combating money laundering and terrorist financing

- Questionnaire credit institutions pdf - word
- Questionnaire life insurance companies pdf - word
- Questionnaire stockbroking firms pdf - word
- Questionnaire payment institutions and electronic money institutions pdf - word
- Indicative list of countries presenting a higher risk of money laundering or terrorist financing (annex 1 to the above-mentioned questionnaires)

External whistleblowing

Statutory and regulatory framework

- 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 resolving any dispute.

External whistleblowing: Comments and recommendations by the NBB

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 are required to 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, on a confidential or anonymous basis and through a specific and independent channel, of any breaches of the Anti-Money Laundering Law (see the page Internal whistleblowing on this website), the NBB has also set up a whistleblowing system for external reporting of 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. 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 Scope page.

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 statutory 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 this person having reported a breach. The Bank may impose an administrative sanction on any financial institution that violates this prohibition.

The NBB uses the information supplied in the breach report exclusively for the purpose of performing its statutory 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, and 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 resolving any dispute.

Supervisory powers, measures and policy of the NBB

Statutory and regulatory framework

- Anti-Money Laundering Law: Articles 7 and 85 to 98/1

Other reference documents

- EBA Guidelines dated 16 December 2021 on risk-based supervision
- FATF Guidance dated March 2021 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 resolving any dispute.

Supervisory powers, measures and policy of the NBB: Comments and recommendations by the NBB

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
- 4. Risk-based supervisory methodology and policy

1. Role of the NBB in AML/CFT

The provisions governing the NBB's competence in the area of AML/CFT are laid down in Articles 85 to 98/1 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 administrative sanctions where a financial institution violates a legislative or regulatory provision whose compliance is monitored by the NBB (see the page Administrative sanctions).

2. Supervisory powers and measures of the NBB

The NBB's supervisory powers and measures in the area of AML/CFT are specified in Articles 91 to 98/1 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 Anti-Money Laundering Law and to verify the appropriate nature of the management structures, the administrative organisation, the internal control and the ML/FT risk management policies;
- task the statutory auditor or accredited auditor for the financial institution with preparing special

reports relating to compliance by the latter (including any branches it may have abroad) with the applicable AML/CFT provisions or relating to the enforcement of the NBB's orders;

The NBB may thus rely on the cooperation of the statutory auditor or accredited auditor of the financial institution (or of an ad hoc accredited auditor that the NBB appoints if the institution concerned is not required to appoint one), in particular for monitoring the proper implementation of an action plan drawn up following an on-site inspection or recommendations issued following a specific or horizontal supervisory action, or for confirmation that the information which the institution is required to communicate to it is complete, correct and established in accordance with the relevant rules.

It should also be noted that, like the laws organising prudential supervision, the Anti-Money Laundering Law provides that inspection reports, any special reports which may be requested from the statutory auditor or accredited auditor and, more generally, all documents coming from the NBB which it specifies are confidential may not be disclosed by the financial institutions without the NBB's express authorisation, under penalty of the sanctions provided for in Article 458 of the Criminal Code.

Where the NBB's controls lead to the identification of shortcomings on the part of a financial institution, the NBB may order it:

- to comply with specific AML/CFT obligations imposed on it pursuant to the applicable provisions (for example, due diligence requirements provided for in Book II of the Anti-Money Laundering Law, or obligations imposed by the binding provisions relating to financial embargoes);
- to comply with a requirement imposed by the NBB pursuant to the aforementioned provisions (for example, ad hoc or regular communication of information or documents of any kind);
- to comply with the requirements imposed by the NBB as conditions to a decision taken pursuant to the same provisions (for example, the requirement that the AMLCO of the financial institution has his position in the organisation chart of this financial institution modified in order to satisfy the obligation of independence referred to in Article 9 of the Anti-Money Laundering Law, or follows a specific training course in order to satisfy the obligation of expertise laid down in the same Article 9);
- to make the necessary adjustments, or 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 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. The Anti-Money Laundering Law provides that the amount of the penalty is determined, where appropriate, taking into account a series of relevant circumstances listed therein, such as the gravity and the duration of the breaches, the degree of responsibility of the financial institution involved, its financial strength, or its level of cooperation with the supervisory authorities.

Finally, if the NBB finds that the situation has not been remedied by the deadline it has set, the Anti-Money Laundering 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 urgent cases, or where the seriousness of the facts so justifies, the NBB may take such

measures without previously issuing an order, provided that the financial institution has been able to defend its case.

The Anti-Money Laundering Law provides that the aforementioned measures taken by the NBB (as well as any appeals in relation thereto and the outcome thereof) are, on the one hand, brought to the attention of the EBA and, on the other hand, **published**, in principle specifying the name of the institution concerned, on the NBB's website for a period of at least five years. This publication should include at least information on the type and nature of the breach, as well as the identity of the natural and legal persons responsible. In view of the specific nature of certain measures imposed by the NBB, the decision whether or not to publish, or to publish anonymously, is taken by the NBB taking into account the proportionate nature of the publication as well as the risk for the financial institution concerned and for the stability of the financial markets.

Finally, where the NBB, in the context of its supervisory mission at a financial institution, identifies any breaches of the provisions of the Anti-Money Laundering Law relating to the limitation of the use of cash which are subject to the criminal sanctions provided for in Article 137 (1) of the Law and which falls within the supervisory competence of the FPS Economy, it notifies the latter as soon as possible.

In order to ensure the consistency between AML/CFT supervision and general prudential supervision, most of the provisions of the Anti-Money Laundering Law conferring the supervisory and enforcement powers referred to above 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 and with the European Central Bank acting as the prudential supervisory authority under the Single Supervisory Mechanism, in order to maintain the overall consistency of the supervisory actions with regard to each of the financial institutions subject to supervision.

4. Risk-based supervisory methodology and policy

In accordance with Articles 7 and 87 of the Anti-Money Laundering Law, the NBB is required to implement a risk-based approach in the exercise of its AML/CFT supervisory powers.

Based on its practical experience with risk-based supervision in this area, as well as the EBA Guidelines dated 16 December 2021 on risk-based supervision and various guidance documents published by FATF in this area, including the FATF Guidance of March 2021 on risk-based supervision, the NBB has developed a risk-based AML/CFT supervisory policy. The purpose of this supervisory policy is:

- to base the exercise of its supervisory powers on an assessment of the level and nature of the ML/FT risks associated with each financial institution subject to supervision, taking into account its specific characteristics ("risk profiles");
- to implement differentiated off-site and on-site supervisory actions for each financial institution according to the risk profile assigned to it;
- to ensure consistency between the off-site supervisory actions, on the one hand, and the controls carried out on site (inspections), on the other;
- to provide a framework for implementing the principle of equal treatment of financial institutions with regard to supervision, notwithstanding the differentiation of individual supervisory actions according to risk.

The NBB's supervisory policy thus clarifies the objectives of the supervision and defines, in general terms, the differentiated risk-based supervisory actions to be taken to achieve those objectives.

The principles underlying this supervisory policy can be summarised as follows.

This policy is based primarily on an individual assessment of the ML/FT risks to which each financial institution is exposed ("risk profiles").

In order to provide a frame of reference allowing a consistent attribution of the individual risk profiles to all the financial institutions falling within its supervisory powers, the NBB has carried out a sectoral risk assessment (SRA) aimed at determining in a generic manner the level of ML/FT risk associated with the various categories of financial institutions falling within its powers. In order to achieve an adequate level of granularity in this document, the NBB has carried out this exercise by distinguishing between the risks associated with the various financial activities carried out by the institutions subject to its supervision. This sectoral risk assessment also enables the NBB to contribute, through its assessment of the vulnerability to money laundering risks of the various categories of financial institutions subject to its supervision, to the national assessment of money laundering risks carried out by the body tasked with coordinating the fight against the laundering of money of illicit origin.

While the sectoral risk assessment constitutes an important frame of reference, the assignment of an adequate risk profile to each financial institution also requires full account to be taken of the specific characteristics of each of them. To this end, the attribution of the risk profile is based on the analysis of all available information concerning each financial institution, in particular the information obtained from each financial institution through the periodic AML/CFT questionnaire and its overall risk assessments and the AMLCO's annual report. Information relating to the results of previous supervisory actions, both off-site and on-site (inspections), information obtained, where applicable, from other AML/CFT supervisory authorities or from the competent prudential supervisory authorities in the framework of both national and international cooperation, information that may be communicated by CTIF-CFI, or any other relevant information that may be obtained from reliable external sources, are also taken into account.

The analysis of all this information aims at measuring, on the one hand, the inherent risks that appear to be associated with the activities carried out by each financial institution (taking into account risk factors relating to the characteristics of the customers, the products and services offered, the distribution channels used, and the geographical areas with which the financial institution comes into contact through its activities. On the other hand, the analysis aims to assess the measures taken to reduce and manage these risks, both in terms of their compliance with applicable statutory and regulatory requirements and in terms of their effectiveness and efficiency.

This process leads to an individual assessment of residual ML/FT risks, which results in the attribution to each financial institution of the risk profile ("High Risk", "Medium High Risk", "Medium Low Risk" or "Low Risk") that is deemed to be the most appropriate. It should be noted that these risk profiles are attributed according to a methodology that ensures consistency, not only within each sector subject to supervision (credit institutions, life insurance companies, stockbroking firms, payment institutions and electronic money institutions), but also at the cross-sectoral level.

To allocate these risk profiles, the NBB has developed IT tools for collecting and analysing information, that it refines whenever necessary.

Based on the risk-based supervisory policy adopted by the NBB, each of the four risk profiles that can be attributed to financial institutions is associated with a differentiated level of supervision ("Intensive", "Reinforced", "Ordinary" or "Light"). Each of these levels of supervision leads to the application of off-site supervisory measures that are differentiated in terms of their intensity, their frequency, and the nature and objective of the supervision.

Intensity of supervision

The risk profile assigned to each financial institution determines the degree of verification of information and the intensity of the supervision that will be exercised. Thus, the higher the level of risk, the more intrusive the supervisory methods should be.

On the other hand, in the case of financial institutions with a "medium high" or "high" level of risk, supervisory actions may give rise to additional requests for more detailed information. For example, these financial institutions may be asked to provide the NBB with samples of individual customer files or samples of their transactions to enable it to carry out spot checks.

Depending on the needs, the desk-based supervision is supplemented by meetings with management, compliance officers, AMLCOs or other members of staff, and/or by an on-site control (other than inspections) in order to analyse the information and ensure the relevance of the findings and the adequacy of the recommended remedial measures and their implementation schedule.

Differentiating the intensity of supervision according to the risk profile also makes it possible to shortlist financial institutions with the highest risks with a view to formal on-site inspections.

Frequency of supervision

Without prejudice to supervisory actions to be carried out outside the ordinary supervisory schedule due to event-driven situations, the frequency of supervisory actions will vary according to the risk profile.

Nature and purpose of supervision

With regard to financial institutions with a "low" or "medium low" risk, standardised supervisory actions will generally be carried out in order to provide an overall assessment of the level of compliance and effectiveness of the AML/CFT mechanisms implemented. However, if this overall assessment of the situation reveals that the risk that the financial institution subject to supervision could be used for money laundering or terrorist financing purposes is higher than initially thought, more targeted supervisory actions will be taken.

These standardised actions are essentially based on the use of the risk assessment and supervisory tools which the NBB has developed itself. It should be noted that the identification of vulnerabilities through this standardised approach leads to the adoption of specific remedial measures, and may also result in a change in the risk profile allocated to the financial institution concerned.

In the case of financial institutions with a “medium high” or “high” level of risk, a standardised assessment of the overall situation of the financial institution should be carried out, but it should be supplemented by targeted and thematic actions, and/or actions focusing on specific, individualised points of attention, specifically taking into account the individual characteristics of each financial institution, in particular the activities carried out, the characteristics of the customers, the size, the complex internal organisation structure, etc. Such actions typically cover clearly delineated topics.

Depending on the needs, these supervisory actions may concern either financial institutions that can be grouped in a single cluster (based on the similarities in the most significant risks they are exposed to), or individual financial institutions.

With regard to targeted and thematic inspections, carrying out parallel missions at several similar financial institutions may reinforce the validity of the conclusions of the respective missions by comparing their situation with that of all the institutions included in the cluster (benchmarking). This supervisory technique may also help to ensure equal treatment of financial institutions in the context of risk-based supervision. It also enables the NBB to refine, if necessary, the information it publishes on its website dedicated to AML/CFT, for example by publishing the general conclusions of its thematic mission ("lessons learned", "good practices", etc.), or by amending its recommendations for the purpose of clarification or greater precision. The risk-based supervisory policy confirms that such actions should be implemented as a priority with regard to those financial institutions under supervision that present a “high” or “medium high” level of risk. The topics to be examined as part of this type of supervision will be selected on the basis of their relevance to the institutions included in the cluster or to the financial sector as a whole, taking into account the developments within this sector, the emergence of new forms of risks or vulnerabilities, or an upward reassessment, in the light of experience, of the impact of pre-existing risks or vulnerabilities.

In addition to "standardised" and "thematic" supervisory actions, financial institutions with a “medium high” or “high” level of risk are also subject to "individualised" actions to deepen the knowledge of the risks and vulnerabilities that are specific to them individually, to identify any shortcomings and weaknesses in their measures to manage and mitigate these risks and vulnerabilities, and to ensure that these shortcomings and weaknesses are adequately addressed.

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

National cooperation

Legal and regulatory framework

- Anti-Money Laundering Law: Articles 120/2, 120/3 and 121 to 121/2

Other reference documents

- EBA Guidelines dated 16 December 2021 on cooperation and information exchange between prudential supervisors, AML/CFT supervisors and financial intelligence units under Directive 2013/36/EU
- Memorandum of Understanding for collaboration of 17 June 2021 regarding the platform for a public-private partnership on the prevention of money laundering and terrorist financing (“AML platform”)
- 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

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

National cooperation: Comments and recommendations by the NBB

Contents

- 1. Provisions common to national and international cooperation
- 2. Provisions specific to national cooperation

Book IV of the Anti-Money Laundering Law includes a Title 5, inserted by the Law of 20 July 2020, which is devoted to the cooperation between the relevant authorities and defines the limits of the professional secrecy to which they are bound, in particular by lifting it where it could constitute an obstacle to cooperation. Similarly, Article 36/13 of the Law of 22 February 1998 establishing the organic statute of the National Bank of Belgium sets out the exceptions to the NBB's obligation of professional secrecy which are applicable in the context of its mission to prevent money laundering and terrorist financing. Book IV, Title 5 of the Anti-Money Laundering Law comprises three chapters: the first containing provisions common to the two following chapters (Articles 120/2 and 120/3), the second one pertaining to national cooperation (Articles 121 to 121/2) and the last one to international cooperation (see the page International cooperation).

1. Provisions common to national and international cooperation

Article 120/2 of the Anti-Money Laundering Law defines a number of concepts used in Title 5. This provision should be read in conjunction with Article 4, 17° of the Anti-Money Laundering Law, which in particular defines the concept of “supervisory authorities” as the authorities referred to in Article 85 of the Law. On the basis of this definition, Article 120/2 specifies two categories of supervisory authorities in particular: the “financial supervisory authorities” (1°), on the one hand, and the “supervisors” (7°), on the other. This distinction is theoretical in Belgium: both terms refer to the same authorities, namely the NBB, the FSMA and the FPS Economy. They will sometimes be qualified as supervisors and sometimes as financial supervisory authorities, depending on whether reference is made to their competence to supervise compliance with anti-money laundering provisions, or with rules of a financial nature, also known as “prudential” rules when referring to the rules supervised by the NBB.

Article 120/3 of the Law introduces a principle of finality for the financial supervisory authorities in relation to the way they use the confidential information of which they become aware in their capacity as AML/CFT supervisory authority. The same principle is also expressed in Article 36/12/4 of the Law of 22 February 1998 establishing the organic statute of the National Bank of Belgium.

The EBA Guidelines dated 16 December 2021 on cooperation and information exchange between prudential supervisors, AML/CFT supervisors and financial intelligence units under Directive 2013/36/EU detail the ways in which these authorities should cooperate and exchange information in the context of supervision covering, inter alia, authorisation, and the monitoring of the conduct of business, including risk assessment and the imposition of measures and sanctions such as withdrawal of authorisation.

2. Provisions specific to national cooperation

The national cooperation and exchange of information among (Belgian) supervisory authorities and between (Belgian) supervisory authorities and CTIF-CFI have their legal basis in Article 121 of the Anti-Money

Laundering Law (which was included in the Law from its inception). 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 in particular:

1. CTIF-CFI;
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, § 2, 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 information useful for the exercise of the powers conferred upon them by or pursuant to the Law.

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 a Memorandum of Understanding (MoU). 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 on the previous page).

In addition, on 17 June 2021, the professional associations representing the financial sector, the supervisory authorities (including the NBB), CTIF-CFI and the Treasury signed a Memorandum of Understanding for collaboration to create a platform for a public-private partnership on the prevention of money laundering and terrorist financing (the so-called “AML platform”). This platform is intended to increase the efficiency of AML/CFTP by facilitating the exchange of information and consultation between its participants. However, it is without prejudice to any pre-existing consultation structures and channels, in particular (i) the AML/CFT coordination bodies referred to in the Anti-Money Laundering Law, which are comprised exclusively of public authorities (including the NBB) and whose main purpose is to prepare the “national risk assessment” required by the Law, and (ii) the usual modes of bilateral consultation, particularly the consultation between the NBB and the professional associations of the financial sector. The AML platform is tasked, among other things, with proposing guidelines and providing feedback on the implementation of the legal AML/CFTP requirements, in particular those related to the detection and reporting of suspicious transactions.

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

International cooperation

Legal and regulatory framework

- Anti-Money Laundering Law: Articles 120/2, 120/3 and 130 to 131/5

Other reference documents

- EBA Guidelines dated 16 December 2021 on cooperation and information exchange between prudential supervisors, AML/CFT supervisors and financial intelligence units under Directive 2013/36/EU
- Joint Guidelines dated 16 December 2019 on cooperation and information exchange between competent authorities supervising credit and financial institutions (“The AML/CFT Colleges Guidelines”)
- 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 resolving any dispute.

International cooperation: Comments and recommendations by the NBB

Contents

- 1. Provisions common to national and international cooperation
- 2. Provisions specific to international cooperation

Book IV of the Anti-Money Laundering Law includes a Title 5, inserted by the Law of 20 July 2020, which is devoted to the cooperation between the relevant authorities and defines the limits of the professional secrecy to which they are bound, in particular by lifting it where it could constitute an obstacle to cooperation. Similarly, Article 36/13 of the Law of 22 February 1998 establishing the organic statute of the National Bank of Belgium sets out the exceptions to the NBB's obligation of professional secrecy which are applicable in the context of its mission to prevent money laundering and terrorist financing. Book IV, Title 5 of the Anti-Money Laundering Law comprises three chapters: the first containing provisions common to the two following chapters (Articles 120/2 and 120/3), the second one pertaining to national cooperation (see the page National cooperation) and the last one to international cooperation (Articles 130 to 131/5).

1. Provisions common to national and international cooperation

Article 120/2 of the Anti-Money Laundering Law defines a number of concepts used in Title 5. This provision should be read in conjunction with Article 4, 17° of the Anti-Money Laundering Law, which in particular defines the concept of “supervisory authorities” as the authorities referred to in Article 85 of the Law. On the basis of this definition, Article 120/2 specifies two categories of supervisory authorities in particular: the “financial supervisory authorities” (1°), on the one hand, and the “supervisors” (7°), on the other. This distinction is theoretical in Belgium: both terms refer to the same authorities, namely the NBB, the FSMA and the FPS Economy. They will sometimes be qualified as supervisors and sometimes as financial supervisory authorities, depending on whether reference is made to their competence to supervise compliance with anti-money laundering provisions, or with rules of a financial nature, also known as “prudential” rules when referring to the rules supervised by the NBB.

Article 120/3 of the Law introduces a principle of finality for the financial supervisory authorities in relation to the way they use the confidential information of which they become aware in their capacity as AML/CFT supervisory authority. The same principle is also expressed in Article 36/12/4 of the Law of 22 February 1998 establishing the organic statute of the National Bank of Belgium.

The EBA Guidelines dated 16 December 2021 on cooperation and information exchange between prudential supervisors, AML/CFT supervisors and financial intelligence units under Directive 2013/36/EU detail the ways in which these authorities should cooperate and exchange information in the context of supervision covering, inter alia, authorisation, and the monitoring of the conduct of business, including risk assessment and the imposition of measures and sanctions such as withdrawal of authorisation.

2. Provisions specific to international cooperation

2.1. Anti-Money Laundering Law

2.1.1. Cooperation between Belgian and foreign supervisory authorities

Article 130 of the Anti-Money Laundering Law first sets out the general principle of cooperation and information exchange between the Belgian and foreign supervisory authorities competent with regard to AML/CFT. This principle is then illustrated in different situations where the Belgian supervisory authorities, including the NBB, are required in particular to cooperate with foreign supervisory authorities.

For instance, the following applies in particular 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, § 2, 1°, 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, § 2, 2°, 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, 3°, 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, 3°, 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 supervisory 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 is required, in its capacity as AML/CFT supervisory authority, to exchange information with foreign AML/CFT supervisory authorities as part of the cooperation described above are specified in Article 131 of the Anti-Money Laundering Law. Where the foreign supervisory authority is not itself bound by a legal obligation of professional secrecy at least equivalent to that to which the NBB is subject, the NBB may in essence only share information on the condition that a Memorandum of Understanding (MoU) is concluded beforehand on the basis of the principle of reciprocity. This Memorandum should prohibit the authority receiving the information shared by the NBB from using it for purposes other than AML/CFT supervision and from transmitting this information to third parties without the NBB's consent.

However, this condition does not apply to the cooperation between the NBB and the AML/CFT financial supervisory authorities of another EEA Member State, for which Directive 2018/843 has introduced a harmonised professional secrecy regime. Information sharing between these authorities is subject only to the condition that the authority receiving the information does not transmit it to a third-country authority without the consent of the authority that transmitted the information to it (in this case the NBB). Conversely, a financial supervisory authority of a Member State that has received information from the NBB may share this information with a financial supervisory authority of another Member State without the NBB's consent.

2.1.2. International cooperation between financial supervisory authorities and supervisors

Article 131/1, § 1, of the Anti-Money Laundering Law establishes the obligation for competent AML/CFT financial supervisory authorities, including the NBB, to cooperate with foreign supervisors competent for the “prudential” supervision of financial institutions (including the European Central Bank) and to exchange with them all information (including confidential information) useful for the exercise of their respective supervisory powers.

Article 131/1, § 2, of the Anti-Money Laundering Law introduces the same obligation for Belgian supervisors, including the NBB in its capacity as prudential supervisor, i.e. the obligation to cooperate and exchange all useful information with foreign AML/CFT financial supervisory authorities.

The conditions under which the NBB is required, in its capacity as AML/CFT supervisory authority, to exchange information with foreign supervisors are specified in Article 131/2 of the Anti-Money Laundering Law. Where the foreign supervisor is not itself bound by a legal obligation of professional secrecy at least equivalent to that to which the NBB is subject, the NBB may in essence only share information on the condition that a Memorandum of Understanding (MoU) is concluded beforehand on the basis of the principle of reciprocity. This Memorandum should prohibit the supervisor receiving the information from using it for purposes other than prudential supervision and from transmitting this information to third parties without the NBB's consent.

However, this condition does not apply to the cooperation between the NBB and the supervisors of another EEA Member State competent for the supervision of certain financial institutions (credit institutions, stockbroking firms and insurance companies), for which European directives relating specifically to the supervision of these institutions have introduced a harmonised professional secrecy regime. Information sharing between these authorities is subject only to the condition that the authority receiving the information does not transmit it to a third-country authority without the consent of the authority that transmitted the information to it (in this case the NBB). Conversely, a supervisor of a Member State that has received information from the NBB may share this information with a supervisor of another Member State without the NBB's consent.

2.1.3. International cooperation between supervisory authorities and the authorities responsible for the supervision of financial markets

Articles 131/3 and 131/4 impose and organise, in a similar way as in the above-mentioned Articles, cooperation between the AML/CFT supervisory authorities, including the NBB, and the authorities responsible for the supervision of financial markets of the other EEA Member States. Here, too, the principle applies that the authorities concerned should exchange all information useful for the exercise of their respective tasks.

2.1.4. International cooperation between supervisory authorities and the ESAs

Article 36/13, § 1, 8°, of the Law of 22 February 1998 establishing the organic statute of the National Bank of Belgium provides that the NBB may, by way of derogation from its professional secrecy obligation, communicate confidential information received in the exercise of its AML/CFT supervisory tasks (as referred to in Article 36/2, § 2, of that Law), within the limits of European Union law, to the European Securities and Markets Authority, the European Insurance and Occupational Pensions Authority and the European Banking Authority. This exception to the NBB's professional secrecy enables it, in particular, to provide the EBA with confidential information, including nominative information, as required by the European regulations defining its AML/CFT tasks.

It should also be noted that, pursuant to Article 131/5 of the Anti-Money Laundering Law, the NBB is required to inform the ESAs (in particular the EBA) of cases where it is itself informed, by a financial institution subject to the Anti-Money Laundering Law which has a subsidiary, branch or other form of establishment in a third country, that the law of this third country does not permit the implementation within those establishments of the AML/CFT policies and procedures in force at group level, including the policies and procedures on data protection and intra-group information sharing for AML/CFT purposes. In such a situation (as referred to in Article 13, § 3, third paragraph, of the Law), the NBB and the ESAs should cooperate in finding a solution.

2.2. ESAs joint guidelines on AML/CFT colleges

The establishment of “AML/CFT colleges” aims to create a permanent structure for enhanced cooperation and information sharing between European and third-country authorities responsible for the AML/CFT supervision of the same financial institution operating on a cross-border basis. These AML/CFT colleges are intended to provide AML/CFT supervisory authorities with a forum where they can work together to improve their understanding of the ML/FT risks associated with the financial institution concerned, exchange information to inform each other on the supervisory approach to be adopted and coordinate their supervisory actions where necessary.

As such, the NBB should henceforth, in its capacity as AML/CFT supervisory authority:

- periodically organise AML/CFT colleges for the groups of financial institutions for which it is the “lead supervisor”; and
- participate in other AML/CFT colleges of which it is a permanent member.

The relevant ESAs are also invited to participate in the colleges as permanent members. In addition, cooperation is foreseen with the prudential supervisors of the Member States concerned, who are invited to participate in the AML/CFT colleges as observers.

For more information on this subject, particularly the conditions for establishing an AML/CFT college, please refer to the ESAs Joint Guidelines on AML/CFT colleges.

Where the conditions for setting up an AML/CFT college are not met, competent authorities should ensure cooperation and information exchange on a bilateral basis.

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

Sanctions

- **Administrative sanctions**
- **Criminal sanctions**

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

Administrative sanctions

Legal and regulatory framework

- 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 resolving any dispute.

Administrative sanctions: Comments and recommendations by the NBB

The NBB's Sanctions Committee may impose an **administrative fine** on financial institutions where it identifies:

1° a breach of:

- the provisions of the Anti-Money Laundering Law (e.g. provisions of Book II of the Law which impose obligations in relation to governance, risk assessment, due diligence, reporting to CTIF-CFI and document retention, or provisions aimed at protecting the members of staff and the representatives of a financial institution who have reported a breach of the Law to the NBB through external whistleblowing from any adverse or discriminatory treatment or breach of contract as a result of this reporting) or of its implementing decrees or regulations, in particular the Anti-Money Laundering Regulation of the NBB;
- 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;

2° non-compliance with a requirement imposed by the NBB pursuant to the provisions referred to in point 1° (e.g. where the NBB, pursuant to the provisions of the Anti-Money Laundering Law from which it derives its supervisory powers - see the page "Supervisory powers, measures and policy of the NBB" - requires a financial institution to communicate specific information to it on a monthly basis and the institution fails to do so);

3° non-compliance with a requirement set by the NBB as a condition to a decision taken pursuant to the provisions referred to in point 1° (e.g. where the NBB makes the granting of an authorisation subject to a condition and this condition is not complied with).

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:

- a maximum of EUR 5 000 000 or, if this amount is higher, ten percent of the annual net turnover of the previous financial year, in case of a legal person (the concept of "turnover" being defined in the Anti-Money Laundering Law and specified in the preparatory works of the Law);
- a maximum of EUR 5 000 000, in case of a natural person.

The Anti-Money Laundering Law provides that, where the offence has resulted in a profit for the financial institution concerned or enabled it to avoid a loss, the maximum amount of the fine may be increased to twice the amount of this profit or loss. This possibility is without prejudice to the aforementioned maximum

amounts; in other words, setting the maximum amount of the fine at twice the profit made or the loss avoided may not result in a maximum fine of less than the maximum of EUR 5 000 000 or 10 percent of the annual net turnover of the previous financial year (where the application of this percentage results, for legal persons, in an amount exceeding EUR 5 000 000). This also applies when the fine is imposed on a natural person.

Furthermore, the Law provides that the amount of the fine is determined taking into account a series of relevant circumstances listed in it, such as the seriousness 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.

Any administrative sanction imposed by the Sanctions Committee (as well as any possible appeal against it and the outcome of such an appeal) will moreover be communicated by the NBB to CTIF-CFI on the one hand and the ESAs on the other. The same applies to the settlements that the NBB is authorised to conclude on the basis of the aforementioned Law of 22 February 1998.

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

Criminal sanctions

Legal and regulatory framework

- Anti-Money Laundering Law: Articles 90/1 and 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 resolving any dispute.

Criminal sanctions: Comments and recommendations by the NBB

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 EUR 250 and EUR 2 500 000 (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 EUR 250 and EUR 225 000 which may not exceed 10 % of the illegal payment or donation.

The criminal offences set out in the Anti-Money Laundering Law are subject to the provisions of Book I of the Criminal Code, including Chapter VII and Article 85.

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 pursuant to 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.

It should also be noted that Article 90/1 of the Anti-Money Laundering Law requires the NBB to inform the Public Prosecutor when it detects one of the above-mentioned offences in the exercise of its supervisory powers in relation to a financial institution.

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

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 resolving any dispute.

Main reference documents

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 02/2023)
- Anti-Money Laundering Regulation of the NBB of 21 November 2017
- Article 505 of the Criminal Code (repressive aspect)

Preparatory works of the Anti-Money Laundering Law (relevant for financial institutions):

- Amending Law of 20 July 2020
 - Explanatory Memorandum and Comments on the Articles
 - Draft Law
- Amending Law of 2 May 2019 (relevant extracts)
 - Comments on the Articles
 - Law Proposal
- Amending Law of 30 July 2018 (relevant extracts)
 - Comments on the Articles
 - Draft Law
- Anti-Money Laundering Law of 18 September 2017
 - Explanatory Memorandum and Comments on the Articles
 - Draft Law

Earlier provisions:

- Anti-Money Laundering Law of 11 January 1993
- Anti-Money Laundering Regulation of the CBFA of 23 February 2010

1.2. Sectoral risk assessment

- Sectoral assessment of the money laundering risks in the Belgian financial sector subject to the supervisory authority of the National Bank of Belgium – version of 8 September 2020

1.3. Circulars and communications of the NBB

Circulars and communications currently in force:

- 26 January 2023 - Circular NBB_2023_01 / Periodic questionnaire on combating money laundering and terrorist financing
- 15 February 2022 – Circular NBB_2022_04 / Prudential expectations regarding the AMLCO activity report
- 1 February 2022 - Circular NBB_2022_03 / Prudential expectations in relation to the "de-risking" phenomenon
- 8 June 2021 – Circular NBB_2021_12 / Due diligence obligations regarding the repatriation of funds from abroad and taking into account of tax regularisation procedures when applying the Anti-Money Laundering Law
- 7 April 2020 – Communication NBB_2020_14 / COVID-19
- 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:

- 22 February 2022 - Circular NBB_2022_06 / Periodic questionnaire on combating money laundering and terrorist financing
- 9 March 2021 - Circular NBB_2021_007 / Periodic questionnaire on combating money laundering and terrorist financing
- 22 December 2020 – Communication NBB_2020_050 / Application of Regulation (EU) 2015/847 on transfers of funds to transfers to the United Kingdom
- 15 September 2020 - Communication NBB_2020_36 / Law of 20 July 2020 containing various provisions on the prevention of money laundering and terrorist financing and on the restriction of the use of cash
- 2 March 2020 - Circular NBB_2020_006 / Periodic questionnaire on combating money laundering and terrorist financing
- 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

1.4. Financial sanctions (asset freezing and embargoes)

- See 'National financial sanctions' on the website of the Treasury

1.5. Miscellaneous

- Memorandum of Understanding for collaboration of 17 June 2021 regarding the platform for a public-private partnership on the prevention of money laundering and terrorist financing (“AML platform”)
- Guidelines of CTIF-CFI of 15 August 2020 for obliged entities referred to in Article 5 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 regarding the reporting of information to CTIF-CFI
- 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, as amended by Delegated Regulation 2022/229 of 7 January 2022 (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 (transposed into Belgian Law by the Law of 20 July 2020) and directive 2019/2177 (unofficial coordinated version of 30 June 2021)
- Regulation 2015/847 of 20 May 2015 on information accompanying transfers of funds (unofficial coordinated version of 1 January 2020)
- 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 27 October 2022 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 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”)
- Opinion dated 23 January 2018 on the use of innovative solutions by credit and financial institutions
- 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
- Guidelines of 7 April 2017 on risk- based supervision

2.4 European Banking Authority

- Guidelines of 14 June 2022 on the AMLCO function
- Statement dated 27 April 2022 on financial inclusion in the context of the invasion of Ukraine
- Opinion and report dated 5 January 2022 on de-risking and its impact on access to financial services
- Guidelines dated 16 December 2021 on risk-based supervision
- Guidelines dated 16 December 2021 on cooperation and information exchange between prudential supervisors, AML/CFT supervisors and financial intelligence units under Directive 2013/36/EU
- Opinion dated 3 March 2021 on the risks of money laundering and terrorist financing affecting the Union's financial sector
- Risk Factors Guidelines dated 1 March 2021
- 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

Recommendations:

- International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation (February 2012, updated in March 2022)

Guidelines:

- Updated Guidance dated October 2021 for a Risk-Based-Approach for the Virtual Assets and Virtual Assets Service Providers
- Guidance dated June 2021 on proliferation financing risk assessment and mitigation
- Guidance dated March 2021 on Risk-Based Supervision
- 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 2021)
- 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 January 2014 on Sound management of risks related to money laundering and financing of terrorism (revised in July 2020)
- 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

- Personal data protection: see the website of the Data Protection Authority
- Anti-discrimination legislation: see the website of UNIA

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

Other useful links

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
 - High-risk countries

At the European level

- European Commission – Justice and fundamental rights – Financial crime
- Joint Committee of the European Supervisory Authorities
- EBA
 - Q&A Tool
- 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 resolving any dispute.

Successive versions of the AML/CFT site

Contents

- Successive versions of the site
- Overview of the changes

Successive versions of the site

Current version:

- PDF version of 28 March 2023

Previous versions:

- PDF version of 27 September 2022
- PDF version of 8 June 2022
- PDF version of 21 December 2021
- PDF version of 4 March 2021
- PDF version of 13 August 2020 (before revision of the AML/CFT site following the entry into force of the Law of 20 July 2020)
- PDF version of 21 February 2020
- PDF version of 21 October 2019
- PDF version of 26 June 2019

Overview of the changes

On 28 March 2023:

- Addition of the following documents:
 - European documents:
 - Report from the Commission to the European Parliament and the Council of 27 October 2022 on the assessment of ML/FT risks affecting the internal market and relating to cross-border activities (SNRA) + Annex (Commission Staff Working Document) (see the page “Risk-based approach and overall risk assessment”)
 - EBA Guidelines of 14 June 2022 on the AMLCO function
 - Changes to comments and recommendations by the NBB on the following topics:
 - Page “Governance” (points 1.2, 2.2.1, 2.3, 2.5, 6.1 and 6.2; see in particular the new version of the AMLCO activity report template in point 2.5)
 - Page “Training and education of staff” (point 2: new second paragraph)
 - Page “Internal whistleblowing” (first and third paragraphs)
 - Page “Belgian parent companies” (points 1.1 and 1.2)
 - Page “Performance of obligations by third parties” (points 1.1 and 1.2, eighth paragraph)
 - Page “Data and document retention” (point 1)
 - Page “Supervisory powers, measures and policy of the NBB” (point 2, fifth and eighth

- paragraphs)
- Page “External whistleblowing” (first paragraph)

On 24 March 2023:

- Replacement of the Protocol of 17 September 2019 defining the modalities of cooperation and information exchange between the NBB and CTIF-CFI by its updated version of 10 March 2023 (see page National cooperation)

On 30 January 2023:

- Addition of the following document:
 - Circular NBB_2023_01 / Periodic questionnaire on combating money laundering and terrorist financing

On 27 September 2022:

- Addition of the following document:
 - FATF:
 - Recommendations as updated in March 2022
- Addition of comments and recommendations by the NBB on the following topic:
 - Recommended actions in the event of credible publications of mass fraud or ML/FT cases in the press
- Changes to comments and recommendations by the NBB on the following topics:
 - Page “Governance” (point 2.5)
 - Page “Object of the identification and identity verification” (point 2.3.2, a), fifth paragraph, point 3.2 and point 3.3.2)
 - Page “Financial embargoes and assets freezing” (point 3.1.2)
 - Page “Reporting by financial institutions” (points 2.2, 3.1 and 3.2)
 - Page “Supervisory powers, measures and policy of the NBB” (point 4)
 - Page “National cooperation” (point 1)
 - Page “International cooperation” (point 1)

On 8 June 2022:

- Addition of the following documents:
 - FATF document:
 - Guidance dated March 2021 on Risk-Based Supervision
 - European documents:
 - EBA Statement dated 27 April 2022 on financial inclusion in the context of the invasion of Ukraine
 - Commission Delegated Regulation (EU) 2022/229 of 7 January 2022 on amending Delegated Regulation 2016/1675 of 14 July 2016 on high-risk third countries

- EBA Opinion and report dated 5 January 2022 on de-risking and its impact on access to financial services
- EBA Guidelines dated 16 December 2021 on risk-based supervision
- EBA Guidelines dated 16 December 2021 on cooperation and information exchange between prudential supervisors, AML/CFT supervisors and financial intelligence units under Directive 2013/36/EU
- Addition of comments and recommendations by the NBB on the following topic:
 - Due diligence requirements and de-risking
- Changes to comments and recommendations by the NBB on the following topic:
 - Page “Performance of obligations by third parties” (point 1.1, § 6)

In February 2022:

- Addition of the following NBB documents:
 - 22 February 2022 - Circular NBB_2022_06 / Periodic questionnaire on combating money laundering and terrorist financing
 - 15 February 2022 – Circular NBB_2022_04 concerning the prudential expectations regarding the AMLCO activity report
 - 1 February 2022 - Circular NBB_2022_03 / Prudential expectations in relation to the "de-risking" phenomenon

On 21 December 2021:

- Addition of the following documents:
 - FATF documents:
 - Updated Guidance dated October 2021 for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers
 - Guidance dated June 2021 on Proliferation Financing Risk Assessment and Mitigation
 - International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation (February 2012, updated in June 2021)
 - Methodology for Assessing Technical Compliance with the FATF Recommendations and the Effectiveness Of AML/CFT Systems (February 2013, updated in November 2020)
 - European documents:
 - Most recent unofficial consolidation of the Fourth AML/CFT Directive 2015/849 (30 June 2021)
 - EBA Opinion dated 3rd March 2021 on the risks of money laundering and terrorist financing affecting the Union’s financial sector
 - EBA Guidelines dated 1 March 2021 on risk factors
 - Miscellaneous:
 - Memorandum of Understanding for collaboration of 17 June 2021 regarding the platform for a public-private partnership on the prevention of money laundering and terrorist financing (“AML platform”)
- Addition of the following NBB document:

- 8 June 2021 – Circular NBB_2021_12 / Due diligence obligations regarding the repatriation of funds from abroad and taking into account of tax regularisation procedures when applying the Anti-Money Laundering Law
- Addition of comments and recommendations by the NBB on the following topic:
 - New institutions
- Changes to comments and recommendations by the NBB on the following topics:
 - Page “Governance” (points 3 and 5)
 - Page “Restriction of the use of cash”
 - Page “Reporting by financial institutions” (point 4.1)
 - Page “National cooperation” (addition of the final paragraph)
- Minor changes to other pages of the AML/CFT site

On 12 July 2021:

- Addition of the following NBB document:
 - Addition of the most recent unofficial consolidation of the Anti-Money Laundering Law of 18 September 2017 (06/2020)

On 17 March 2021:

- Addition of the following NBB document:
 - 9 March 2021 – Circular NBB_2021_007 / Periodic questionnaire on combating money laundering and terrorist financing

On 4 March 2021:

- Changes following the entry into force of the Law of 20 July 2020:
 - Addition of the most recent unofficial consolidation of the Anti-Money Laundering Law of 18 September 2017
 - Replacement, on each page, of the references to the provisions of the Anti-Money Laundering Law and of the Anti-Money Laundering Regulation of the NBB with a link to the unofficial consolidation of the Law and to the Regulation
 - Replacement, on each page, of the section “Explanatory Memorandum of the Anti-Money Laundering Law” with references to the preparatory works of the relevant laws amending the Anti-Money Laundering Law on the page “Main reference documents”
 - Other substantive changes to comments and recommendations by the NBB on the following topics:
 - Introduction (see point 3)
 - Scope (see §§ 1 and 3)
 - Definitions
 - Governance (see points 2.3 and 5.6)
 - Policy, procedures, processes and internal control measures (see points 2.2.2.A.2 and 2.5)
 - Belgian parent companies (see points 2.2.3, 2.2.4, 2.3 and 3.2)
 - Performance of obligations by third parties (see point 2.2.3)
 - Anonymous or numbered accounts, safe-deposit boxes and contracts (see point 1)
 - Persons to be identified (see points 2.2 and 2.3)
 - Object of the identification and identity verification (see introduction; points 1, 2.3.2,

- 3.3.2, 5)
 - Time of identification and identity verification (see points 2.2.2 and 2.2.3)
 - Identification of the customer's characteristics and of the purpose and nature of the business relationship or the occasional transaction (see points 1.1, 2.2 and 2.3)
 - Due diligence on business relationships and occasional transactions and detection of atypical facts and transactions (see introductory §§, points 1.1.1, 1.2, 1.5, 2.1, 2.2, 3, 3.1, 3.3 and 4)
 - Correspondent relationships (see point 3, first and third paragraph; point 4)
 - Politically exposed persons (PEPs) (see points 1.1, 1.2, 3, 3.1 and 4)
 - Due diligence requirements and compliance with other legislation (see point 2)
 - Analysis of atypical facts and transactions (see points 2.1.1.A; 2.1.1.B, § 2 and addition of § 3; point 2.2, ninth paragraph)
 - Reporting of suspicions (see point 2.1, first paragraph, 2.2, 2.5.1, first paragraph)
 - Protection of reporting persons (addition of point 3)
 - Data and document retention (deletion of point 2 on personal data protection, which is now covered on a separate page devoted to personal data processing and protection)
 - Restriction of the use of cash (see point 2.1.1.c; addition of the final paragraph of point 2.1.2; point 2.2; addition of point 2.3)
 - Supervisory powers, measures and policy of the NBB (see points 1 and 2)
 - National cooperation (see addition of §1 and point 1; point 2)
 - International cooperation (see addition of §1 and point 1; point 2)
 - Administrative sanctions
 - Criminal sanctions (addition of the final paragraph).
- Minor changes:
 - Adaptation of references to statutory and regulatory provisions
 - Replacement of the concept of “ongoing due diligence” with “due diligence on business relationships and occasional transactions”
- Other changes:
 - Page “Prohibition of disclosure” (see point 2.3; addition of point 2.4)
 - Page “Transfers of funds” (see point 2.2)
 - Page “Financial embargoes and assets freezing” (see point 2.3)
 - Page “Supervisory powers, measures and policy of the NBB” (see point 3; addition of the risk-based supervisory policy in point 4)
 - Addition of a link to the EBA’s “AML Q&A Tool” (page “Other useful links”)
 - Addition of the following documents:
 - Sectoral assessment of the money laundering risks in the Belgian financial sector falling under the supervisory competences of the NBB (version of 8 September 2020)
 - Communication of the NBB of 22 December 2020 on the application of Regulation (EU) 2015/847 on transfers of funds to transfers to the United Kingdom
 - Communication of the NBB of 15 September 2020 on the Law of 20 July 2020 containing various provisions on the prevention of money laundering and terrorist financing and on the restriction of the use of cash
 - Guidelines of CTIF-CFI of 15 August 2020 for obliged entities referred to in Article 5 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 regarding the reporting of information to CTIF-CFI
 - FATF Recommendations (revised in October 2020)
 - BCBS Guidelines dated January 2014 on Sound management of risks related to money

laundering and financing of terrorism (revised in July 2020)

- Regulation 2015/847 of 20 May 2015 on information accompanying transfers of funds (unofficial consolidation of 1 January 2020)
- Minor changes to other pages of the AML/CFT site.

On 13 August 2020:

- Substantive changes to comments and recommendations by the NBB on the Reporting by financial institutions (see point 2 and 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 to Virtual Assets and Virtual Asset 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 site

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

Publication of individual decisions

According to the Anti-Money Laundering Law of 18 September 2017, the NBB's Board of Directors may decide to publish, nominatively or not, the decisions it has taken pursuant to Articles 93, 94 and/or 95 of the same Law.

- 16 November 2022

Publication of the decision of the National Bank of Belgium of 11 October 2022 regarding X, adopted pursuant to Article 93, § 1, 1°PDF