Sectoral assessment of the risks of money laundering and terrorist financing in Belgian financial institutions subject to the supervisory authority of the National Bank of Belgium

JULY 2023

Table of Contents

Executive summary

On 24th October 2023, the National Bank of Belgium (hereinafter "the Bank") adopted, pursuant to the exercise of its supervisory powers under the Act of 18 September 2017 on the prevention of money laundering and terrorist financing and on restriction of the use of cash (hereinafter the "AML Act"), a new version of its assessment of money laundering and terrorist financing risks to Belgian financial institutions that fall under its supervision[1].

The purpose of this assessment is to evaluate the various money laundering and terrorist financing ("ML/FT") risks to which financial institutions subject to supervision by the Bank are exposed.

Such an assessment has many benefits. More precisely:

1. it formalises and articulates the knowledge acquired by the Bank's supervisory staff in the exercise of their duties in this area and enables the Bank to refine its risk-based approach and better guide supervision by allocating supervisory resources appropriately. It should be noted that, in accordance with international standards, risk-based supervision requires sufficient knowledge of the ML/FT risks associated with the supervised sectors. It is therefore necessary for the Bank to carry out a sectoral risk assessment;
2. it complements the national money laundering risk analysis. It will therefore be transmitted to CTIF-CFI, the body responsible for coordinating the national assessment. The latter is carried out further to Recommendation 1 of the Financial Action Task Force (FATF), which states that countries should identify, assess and understand their ML/FT risks and adopt a risk-based approach to mitigate the risks identified;
3. it helps financial institutions identify the risks to which they are exposed and enables them to refine their risk-based approach.

The Bank goes beyond an assessment of "sectoral" risks (i.e., those to which all credit institutions, insurance companies, payment and electronic money institutions, and stockbroking firms are exposed) and also focuses on nineteen services and activities identified as potentially presenting a risk to the individual institutions the Bank is responsible for supervising.

The first step involved an assessment of the risk inherent in each service or activity, i.e. the risk of the service or activity in question being used for ML/FT purposes due to its nature and objective characteristics. The level of vulnerability of each financial institution, taking into account all risk mitigation measures, was then determined. Finally, the residual risk of each service or activity was assessed, based on the level of inherent risk in conjunction with the level of vulnerability.

For its analysis, the Bank relied on numerous information sources, as well as the findings of its supervisory work in recent years.

The new version of the sectoral risk assessment:

1. is a **deeper** analysis of money laundering risks.

    - Some new cross-cutting risks are identified, while others are analysed in greater detail. For example, certain specificities of the situation in Belgium that could have an impact on ML/FT risk are identified.
    - New developments are covered including:
        - the acceleration of digitalisation processes, which is impacting the ways in which financial products and activities are distributed;
        - the possible consequences of Brexit for the financial sector, with the establishment in Belgium of several institutions playing an important role on the market and, in some cases, having an innovative business model;

1 The first version was adopted on 8 September 2020.

  - the growing importance of new services (virtual IBANs) which can be vectors for new ML/FT typologies (i.e. techniques and trends, etc. in relation to ML/FT);
  - the impact of the Port of Antwerp's activities on ML/FT risks.
- The present assessment analyses nineteen financial services, compared with thirteen in the previous version. Acquiring services, trade finance, foreign exchange transactions, guarantee and pledge services, factoring, clearing and custodial services are now analysed separately.
- Various public information sources were used to compile the analysis of money laundering risks. These include reports produced by the Financial Action Task Force (FATF), European Banking Authority (EBA) and the Belgian FIU (CTIF-CFI).

2. an **initial** sectoral **assessment** of risks in relation to the fight against terrorist financing.

- It was decided to analyse money laundering and terrorist financing risks concomitantly, given the similarities presented by these two types of risk and their typologies.
- For its assessment of terrorist financing risks, the Bank relied on various public information sources, including reports issued by the IMF, Europol, Eurojust, CTIF-CFI and the State Security Service. Participation in various workshops on combating the financing of terrorism organised under the aegis of the European Commission also proved useful.
- Five main terrorist threats to the sector have been identified:
  - Islamic fundamentalism
  - Right-wing extremism
  - Left-wing extremism and anarchism
  - Terrorism linked to the political situation in a foreign country
  - Other forms of terrorism
- For each financial service or activity, an analysis was carried out of the terrorist financing risks, identifying the inherent risks and vulnerabilities.

The Bank's sectoral assessment of money laundering and terrorist financing risks will be updated every two years.

It is available on the Bank's website.

Summary of money laundering risks

	Inherent risk	**Score (out of 5)**	**Vulnerabilities**	**Score (out of 5)**	**Residual risk**	**Score (out of 5)**
Payment activities	High	4	High	4	High	4
Money remittance	High	4.5	High	4	High	4.5
Acquiring activities	Moderate	2	Moderate	2	Moderate	2
Payment initiation services	Low	1.5	Moderate	2.5	Moderate	2
Account information services	None	0	None	0	None	0
Electronic money activities	Moderate	2.5	Significant	3	Moderate	2.5
Private banking	Significant	3.5	High	4	High	4
Retail banking	Moderate	2.5	Moderate	2.5	Moderate	2.5
Corporate banking	Significant	3	Moderate	2	Moderate	2.5
Trade finance	Significant	3	Significant	3	Significant	3
Manual exchange services	High	4	Significant	3	Significant	3.5
Guarantee and pledge services	Low	1.5	Low	1.5	Low	1.5
Factoring	Moderate	2	Moderate	2	Moderate	2

Correspondent banking	High	4	Significant	3	Significant	3.5
Clearing/custody/central securities depository activities	Moderate	2.5	Moderate	2	Moderate	2
Investment advice (private banking)	Significant	3.5	High	4	High	4
Investment advice (no funds held)	Moderate	2	Moderate	2	Moderate	2
Life insurance	Moderate	2	Low	1.5	Low	1.5
Life insurance (investment products)	Significant	3	Moderate	2.5	Moderate	2.5

Summary of risks relating to the financing of terrorism

	Inherent risk	**Score (out of 5)**	**Vulnerabilities**	**Score (out of 5)**	**Residual risk**	**Score (out of 5)**
Payment activities	High	4	High	4	High	4
Money remittance	High	4	High	4	High	4
Acquiring activities	Low	1.5	Low	1.5	Low	1.5
Payment initiation services	Low	1.5	Low	1.5	Low	1.5
Account information services	None	0	None	0	None	0
Electronic money activities	Significant	3	Significant	3	Significant	3
Private banking	Low	1.5	Moderate	2	Low	1.5
Retail banking	High	4	High	4	High	4
Corporate banking	Moderate	2	Moderate	2	Moderate	2
Trade finance	Moderate	2	Moderate	2	Moderate	2
Manual exchange services	High	4	Significant	3	Significant	3.5
Guarantee and pledge services	Low	1.5	Low	1.5	Low	1.5
Factoring	Low	1.5	Low	1.5	Low	1.5
Correspondent banking	High	4	Significant	3	Significant	3.5
Clearing/custody/central securities depository activities	Moderate	2	Moderate	2	Moderate	2
Investment advice (private banking)	Low	1.5	Significant	3	Moderate	2
Investment advice (no funds held)	Low	1.5	Significant	3	Moderate	2
Life insurance	Low	1.5	Low	1.5	Low	1.5
Life insurance (investment products)	Low	1.5	Low	1.5	Low	1.5

List of abbreviations

AISP	Account Information Service Provider
AML/CFT Act	Act of 18 September 2017 on the prevention of money laundering and terrorist financing and on the restriction of the use of cash
AML/CFT	Anti-money laundering and combating the financing of terrorism
CTIF-CFI	Belgian FIU
EBA	European Banking Authority
ECB	European Central Bank
EEA	European Economic Area
EU	European Union
FATF	Financial Action Task Force
FBI	Federal Bureau of Investigation
FSMA	Financial Services and Markets Authority
IBAN	International Bank Account Number
IMF	International Monetary Fund
ML/FT	Money laundering and terrorist financing
NBB	National Bank of Belgium
NRA	National analysis of money laundering risks
OCAM/OCAD	Coordination Unit for Threat Analysis
PEP	Politically Exposed Person
PISP	Payment Initiation Service Provider
PSD2	Payment Services Directive
UBO	Ultimate Beneficial Owner

1 PURPOSE

This document presents a sectoral assessment of the risks of money laundering and terrorist financing (hereinafter "ML/FT") in the Belgian financial institutions subject to the supervisory authority of the National Bank of Belgium (hereinafter “the NBB”). This sectoral risk assessment is intended to serve as a guide for the NBB in conducting its checks on anti-money laundering and combating the financing of terrorism (AML/CFT) in accordance with its risk-based approach, and therefore supplements the risk-based supervision policy it has adopted. This assessment of the risks associated with the Belgian financial sector and, more specifically, with the institutions for which the NBB is the supervisory authority pursuant to the Act of 18 September 2017 on the prevention of money laundering and terrorist financing and on the restriction of the use of cash (hereinafter "the AML/CFT Act") also provides input for the national assessment of money laundering risks, which is discussed later in this text[2].

This sectoral risk analysis will also be useful to the entities under supervision when drawing up their overall risk assessment. Article 16 of the AML/CFT Act specifies that they must take into account all relevant information available to them. The conclusions of this analysis, which are also based on supervisory actions, will provide them with a useful sectoral overview.

This document is in part an updated version of the first sectoral assessment of money laundering risks carried out in 2020, but now also includes an analysis of terrorist financing risks.

The methodology adopted aims to formalise the expertise developed by NBB staff and to provide the basis for refining sectoral assessments of ML/FT risks, a process that will keep pace with developments in the financial sector.

This analysis is based in particular, though not exclusively, on the following [3]:

- the European Commission’s supranational ML/FT risk assessment of 27 October 2022 (COM(2022)554 final) and its annexes;
- the national analysis of money laundering risks adopted on 3 February 2023 by the Ministerial Committee for coordinating the fight against money laundering of illicit proceeds;
- FATF Guidance “National Money Laundering and Terrorist Financing Risk Assessment”, 2013;
- FATF Report “Professional Money Laundering” 26th July 2018;
- the EBA Guidelines of 1 March 2021 on ML/FT risk factors;
- Joint Opinion of the European Supervisory Authorities of 4 October 2019 on the risks of money laundering and terrorist financing affecting the European Union’s financial sector (JC2019 59), updated by the EBA Opinion of 3 March 2021 on the risks of money laundering and terrorist financing affecting the Union’s financial sector;
- the EBA Report “Risk assessment on ML/TF risks associated with payment institutions”, 16th June 2023;
- the annual reports of the Belgian Financial Intelligence Processing Unit (CTIF-CFI);
- the results of the control actions carried out by the NBB in its capacity as competent national authority under the AML/CFT Act;
- the national assessment of terrorist financing risks of 2017 (restricted document);
- IMF paper “Countering the financing of terrorism: Good practices to enhance effectiveness”, 12th May 2023;
- Europol Reports “European Union Terrorism Situation and Trend Report”, 2022 and 2023;
- Eurojust Report on Money Laundering, 2022;

---

2 Belgian Official Gazette of 6 October 2017 – Chamber of Representatives (www.lachambre.be) documents 54-2566.

3 The main documents can be found on the Bank’s AML/CFT website : Main reference documents | nbb.be

- The annual reports of the Belgian State Security Service 2021 and 2021;
- Egmont paper "Counterterrorism in Belgium: Key challenges and policy options", 2016;
- RUSI Europe - Project CRAAFT Report "Bit by Bit: Impacts of New Technologies on Terrorism Financing Risks", 5th April 2022.

2 METHODOLOGY

An overall assessment of the financial sector without identification of the different characteristics implying specific risks and vulnerabilities would have little added value.

The methodology used therefore aims to identify - within the various categories of institutions subject to the NBB's supervision – specific activities which are central to their different business models and which have characteristics corresponding to specific and potentially differentiated levels of inherent risks, vulnerabilities and residual risks.

Owing to difficulties in accessing precise aggregate data per activity, it is not easy to draw fully documented general conclusions at the end of the assessment. The expertise gained through the (on-site and off-site) controls carried out allows the NBB to make an expert judgment, resulting in a series of sufficiently substantiated conclusions which highlight the risks associated with the institutions' activities, as well as their vulnerabilities in terms of compliance with statutory and regulatory anti-money laundering provisions.

A methodology is being developed for the updating of the analysis.

2.1 ACTIVITIES COVERED

As per 31 December 2022, there are 209 institutions subject to the NBB's AML/CFT supervision, broken down as follows:

- Credit institutions governed by Belgian law: 30
- Branches of credit institutions established in a European Economic Area (EEA) Member State: 45
- Branches of credit institutions established outside the EEA: 5
- Stockbroking firms governed by Belgian law: 12
- Branches of stockbroking firms established in an EEA Member State: 10
- Life insurance companies governed by Belgian law: 25
- Branches of life insurance companies established in an EEA Member State: 9
- Payment and electronic money institutions governed by Belgian law: 39
- Branches and central points of contact of payment and electronic money institutions established in an EEA Member State: 32
- Central securities depositories: 2

For this assessment, 19 activities pursued by four groups of institutions subject to the NBB's supervision were identified, ensuring the desired degree of granularity.

For payment institutions, the activities set out in PSD2 are considered but specific sections are devoted to:

- payment and money remittance activities;
- electronic money activities;
- acquiring activities;
- payment initiation services;
- account information services.

For credit institutions, the following activities were identified as sufficiently distinct to be analysed individually:

- private banking,
- corporate banking and trade finance,
- retail banking, factoring, guarantee and pledge services,
- correspondent banking,
- clearing and settlement,
- custody and central securities depository activities.

It should be noted that these activities may be conducted by institutions of varying size and nature, from large universal banks offering the whole spectrum of financial activities to institutions specialising solely in one particular activity.

For insurance companies, a distinction is made between long-term life insurance products and life insurance as an investment product, partly because of the differences between the types of products and the associated risks, and partly because these products are occasionally offered by different institutions prone to specific vulnerabilities.

A section is devoted to the investment advice offered by stockbroking firms.

Although the NBB is not the competent authority in this area, this assessment also addresses the exposure of financial institutions to ML/FT risks associated with virtual assets, taking into account that financial institutions may be used by their customers to carry out transactions involving virtual assets or to hold virtual assets for their customers.

This non-exhaustive list of activities covered may be modified in subsequent updates of this sectoral risk assessment and the related methodology.

2.2 ACTIVITIES AND RISKS NOT COVERED

This analysis does not cover risks relating to transactions that Belgian or foreign customers might effect via institutions operating in Belgium under the freedom to provide services within the EEA without the intervention of an agent/distributor. Such institutions do not fall within the supervisory scope of the NBB, but within that of the supervisory authority of their Member State of origin. However, they may present non-negligible ML/FT risks to the financial activities of Belgian customers if these risks are not adequately taken into account by the authorities of that Member State.

This analysis also does not cover or measure the risks posed by illicit activities conducted by unauthorised persons or institutions, which consequently evade the supervisory powers of the NBB and any other national or foreign supervision authority[4].

2.3 NATIONAL ANALYSIS OF MONEY LAUNDERING RISKS

The national analysis of money laundering risks adopted on 3 February 2023 inter alia sheds light on the scale and certain characteristics of money laundering and terrorist financing in Belgium.

It shows that money laundering in Belgium represented around €12.7 billion in 2019. Belgium's central position within the European Union and the fact that it is home to a large number of European institutions and international organisations, constitute risk factors.

According to the Federal Police, the number of reports ("PV's") for money laundering registered in the General National Database (Banque de données nationale générale / Algemene Nationale

4 In Belgium, the FSMA is competent to initiate proceedings for activities carried out without authorisation.

Gegevensbank) increased from 856 in 2017 to 1,133 in 2018. Reports were mainly filed in three arrondissements: Antwerp, Brussels and Halle-Vilvoorde.

Another source of information on money laundering offences is CTIF-CFI, which bases its work on suspicious transaction reports it receives from entities subject to the AML/CFT Act (95%) and from other competent authorities (5%). It should be noted that CTIF-CFI cannot investigate on its own initiative transactions that were not first reported to it by obliged entities. It therefore does not have a comprehensive view of all money laundering offences committed in Belgium. Between 2017 and 2022, CTIF-CFI referred around a thousand cases per year to the judicial authorities.

The financial flows in these cases averaged around €1.5 billion per year. This figure should be treated with caution, however, as CTIF-CFI works on the basis of serious indications, which must then be confirmed with a conviction by the judicial authorities.

Over the past ten years (from 2009 to 2019), convictions have been handed down in 633 cases referred by CTIF-CFI to the judicial authorities, and fines and seizures have been imposed totalling more than €300 million.

Criminal activities

The national analysis of money laundering risks describes the main criminal activities observed in Belgium that need to be taken into account to identify products, services and channels that could be used for ML/FT purposes. These activities include, in order of importance, illicit drug trafficking, tax fraud, social security fraud, scams, theft, and human trafficking and smuggling.

Furthermore, the predicate offences to money laundering identified by CTIF-CFI also give an indication of the main criminal activities in Belgium.

Five criminal activities stand out in CTIF-CFI's statistics: serious tax fraud (organised or otherwise), illicit trafficking in goods and merchandise, social fraud, organised crime and scams. These five activities account for almost 90% of the amounts reported by CTIF-CFI to the judicial authorities.

Illicit drug trafficking is a major criminal activity in Belgium (as evidenced by the numerous drug seizures in recent years), but, given the use of money laundering techniques to avoid the financial system (such as offsetting or the cross-border transport of cash), transactions resulting from this type of crime are now less visible in CTIF-CFI's statistics.

Risks and vulnerabilities

The national analysis shows that the financial sector has long been subject to strict rules and prudential supervision by the NBB and the FSMA, including with regard to the prevention of money laundering. The level of vulnerability of an activity sector is highly dependent on its implementation of effective AML measures. If properly implemented, these measures should reduce the level of money laundering risk in that sector. Risks and vulnerabilities are therefore closely related concepts.

For example, when it comes to assessing the level of risk that financial institutions are likely to pose themselves, independently of their vulnerability to money laundering risks, it should be noted that they are subject to strict rules and prudential supervision that includes measures to verify the professional integrity and adequate expertise of their shareholders, managers and persons responsible for key functions (particularly the internal audit and compliance functions). This supervisory power is exercised directly by the European Central Bank (ECB), within the framework of the Single Supervisory Mechanism, in respect of the largest credit institutions (the systemically important banks), and by the NBB, under the supervision of the ECB, in respect of less significant credit institutions.

Prudential supervisory measures, combined with the specific control measures provided by the institutions' AML systems, can reduce the money laundering risk posed by them. However, these measures cannot eliminate this risk completely.

2.4 TRANSVERSAL RISK FACTORS

Certain traditional transversal risk factors, such as the use of cash or the scope of the risk associated with distribution methods, have long been known.

However, since money laundering activities continue to evolve in line with the transformation of financial activities and the associated regulatory, preventive and repressive framework, the financial sector is now also faced with the following new transversal money laundering risk factors:

- The consequences of the Brexit;
- FinTech[5];
- new technologies;
- virtual assets;
- legislative developments and divergences between Member States and divergences in ML/FT supervisory practices.

2.4.1 CONSEQUENCES OF THE BREXIT

Brexit had a major impact, especially between 2016 and 2021. Many applications for authorisation submitted to the NBB during that time were prompted by the partial or total relocation to Belgium of activities previously carried out in the EU from the United Kingdom. In Belgium, this mainly affected the payment and electronic money sectors. Several players, including global market leaders, have chosen to establish their activities in Belgium and apply for a European passport to carry out their activities from Belgium in the EEA. An examination of the quality of their AML/CFT systems revealed shortcomings mainly arising from the very intensive and insufficiently controlled outsourcing of AML/CFT-related tasks and functions to other entities of the group established outside the European Union. This often results in a lack of substance of the entities authorised in Belgium, as they remain dependent on other group entities.

2.4.2 FINTECH

FinTech is experiencing significant growth in Belgium, bringing with it innovative products and services. The promoters of these new entities are primarily or even exclusively IT-based and lack adequate and sufficiently detailed understanding of the AML/CFT constraints related to the marketing of their new products. This may constitute a significant risk and requires supervisors to adapt both their controls and the statutory and regulatory framework. The use by financial institutions of external service providers without sufficiently assessing the extent to which their services meet AML/CFT requirements exposes them to significant risk. In addition, the growing number of FinTech applications providing services to customers of credit institutions means that transactions are more opaque and less traceable.

Most players on the Belgian market use external technological solutions and third-party databases, mainly to identify or analyse customer profiles and transactional activities. This technology market is relatively limited, and the potential concentration of the data market raises questions about:

- the quality of the data thus used by a large number of players;
- the lack of analysis of individual cases or specific alerts;
- the increase in de-risking actions on the part of certain institutions.

---

5 FinTech refers to technology-based financial innovation that can lead to new business models, applications, processes or products with a material impact on financial markets and institutions and the provision of financial services.

2.4.3 VIRTUAL ASSETS

Virtual assets can be attractive to criminals because they offer greater discretion and anonymity than other means of payment. As from 1 May 2022, the activities of certain virtual asset service providers have been regulated in Belgium and subject to FSMA's supervision, to the exclusion of any formal competence devolved to the NBB vis-à-vis these providers. Nevertheless, financial institutions subject to the NBB's supervision may be used by criminals to introduce funds derived from virtual asset transactions into the financial system. In addition, customers of financial institutions may hold virtual assets, which entail specific risks if they are converted into legal tender and the proceeds are inserted into the financial system[6].

In addition, credit institutions may have business relationships with customers that are virtual asset service providers. In particular, companies that operate bitcoin ATMs (BTMs) and collect vast amounts of cash wish to introduce the proceeds of their activity into the financial system.

Furthermore, customers of financial institutions may be (unwittingly) involved in fraudulent crypto-currency transactions or fall victim to fraud, for example:

- customers who accept an offer from a fake platform to invest in crypto-currencies and who make a transfer from their bank accounts to an IBAN account belonging to fraudsters;
- customers who buy crypto-currencies through their bank account on a crypto-currency trading platform, after which they are asked to transfer these crypto-currencies from their digital wallet to a fake platform, while in reality they end up in the fraudsters' crypto wallet;
- customers who receive funds derived from fraud (e.g. ransomware) or other illicit activities (e.g. sale of drugs);
- customers who are active in crypto mining[7] operations and who receive the proceeds of these activities on their account in Belgium.

This type of fraud is on a steady rise but, as not all victims file complaints, it is still difficult to estimate its scale at this stage.

The emergence of new challenges linked to **technological innovation**, the increasing integration of financial flows in the single market and the "extraterritorial" nature of the activities of certain institutions make it even more important to strive for greater uniformity in national legislation and in the practices of the national authorities responsible for AML/CFT supervision.

It should also be pointed out that financial institutions may have stakes in virtual assets, which may give rise to a prudential risk that is outside the scope of this analysis. However, prudential reporting shows that the exposure to virtual assets of financial institutions active in Belgium was extremely limited at the end of 2022. Credit institutions operating in Belgium are required to report their exposure to crypto assets to the NBB. At present, only two credit institutions have concrete plans to develop activities in this area, while some other banks are at a more exploratory stage.

2.4.4 LEGISLATIVE DEVELOPMENTS AND DIVERGENCES BETWEEN MEMBER STATES AND DIVERGENCES IN ML/FT SUPERVISION PRACTICES

Certain regulatory changes can lead to situations that make the supervisory activities more complex. Reference can be made in this regard to recent developments in instant payments. In addition,

---

6 See the FATF Guidance of 28 October 2021 for a risk-based approach to virtual assets and virtual asset service providers.

7 A "miner" is a person or entity that participates in a decentralized virtual currency network by running special software to solve complex algorithms in a "proof of work" or other proof system used to validate transactions in the virtual currency system.

certain differences in territorially applicable legislation may be exploited to facilitate money laundering operations.

The emergence of these new risks was confirmed by a 2023 EBA Report[8], to which the NBB contributed.

These new risk factors, which result from changes to the sector in terms of its players and the design of its products, concern all financial activities in varying degrees and ultimately create more opportunities to carry out money laundering operations.

For instance, new conditions exist today which often make money laundering harder to detect or identify than before (e.g. virtual IBANs).

2.4.5 THE COVID-19 HEALTH CRISIS

Contrary to initial fears, the Belgian financial sector does not seem to have been impacted by the emergence of new types of crime specific to the Covid crisis. The fear that counterfeit medicines or vaccines would be distributed or counterfeit medicines ordered, does not seem to have materialised to any significant extent in Belgium. This is undoubtedly due to the fact that, once available on the international market, vaccines and any treatments were gradually made available to as many people as possible in an orderly fashion and often free of charge. On the other hand, it is undeniable that the Covid crisis and the related lockdowns and restrictions have accelerated the development and use of digitalisation and new technologies in the financial sector. This has provided criminals with new opportunities for phishing and fraud.

2.4.6 CHANGES TO THE FINANCIAL SECTOR AND BUSINESS MODELS

Changes to the financial sector influence the business models of financial institutions, as well as the general knowledge they may have about customers and their characteristics (see also point 2.4.11).

As more products are offered to customers in Belgium, the significant increase in competition on markets with low profitability may occasionally lead institutions to increase their risk-taking. The European Commission[9] specifically mentions the pressure on risk appetite models and the danger this represents for financial activity as one of the four major vulnerabilities in terms of money laundering risks.

At the same time, the increase of financial activities further complicates and may even limit institutions' acquisition of knowledge about the activities and characteristics of their customers. For instance, an institution may be less able to detect an atypical transaction by a customer if it only has information on that customer in connection with a limited activity: thus, in principle, an institution offering only one specific type of financial product or service naturally has less information on its customers' characteristics than an institution which has gained more detailed knowledge of its customer via a transversal and more inclusive commercial approach.

8 EBA Report on ML/FT risks associated with payment institutions (EBA/REP/2023/18)

9 Report from the Commission to the European Parliament and the Council of 24 July 2019 on the assessment of recent alleged money laundering cases involving EU credit institutions (COM (2019)373).

2.4.7 INTRODUCTION OF THE REGISTER OF BENEFICIAL OWNERS (UBO REGISTER)

The 2022 Eurojust Report on Money Laundering[10], which is based on an analysis of cases registered with Eurojust between 1 January 2016 and 31 December 2021, notes that identifying beneficial owners is one of the main legal and practical challenges facing the authorities concerned in light of the use of shell or letterbox companies to facilitate money laundering and terrorist financing operations.

The introduction in Belgium of the UBO register, which records all beneficial owners of all legal entities, including non-profit organisations, is therefore an important step. Indeed, a high level of transparency of information on beneficial owners is essential to combat the creation of structures that are deliberately opaque. In addition, however, financial institutions should also develop tools to ensure that beneficial owners are identified as part of their customer due diligence measures.

2.4.8 RUSSIA'S MILITARY AGGRESSION AGAINST UKRAINE

Following Russia's invasion of part of Ukrainian territory in February 2022, the EU severely tightened the sanctions put in place against Russia since 2014 and also imposed measures against Belarus. The European Commission mentioned these measures in its supranational ML/FT risk assessment of 27 October 2022. Strict application of the rules on beneficial owners is essential for sanctions to be effectively implemented.

However, the targeted financial sanctions (TFS) imposed by the EU in this context are not related to the fight against money laundering, terrorist financing or the financing of the proliferation of weapons of mass destruction[11]. Furthermore, there is no clear evidence that the invasion of Ukraine has increased ML/FT risks in Europe. On the contrary, the TFS imposed on Russia and Belarus - for geopolitical reasons unrelated to AML/CFT - may have curbed the flow of criminal funds to Europe.

2.4.9 USE OF CASH

Criminals continue to prefer cash since it cannot be traced and therefore permits anonymous transactions.

Consequently, financial products involving the use of cash are more likely to be linked to one of the three stages of money laundering (placement, layering and integration). The same applies to assets such as gold and diamonds, which can be readily traded and transported and easily and safely stored.

Products relating to the use of cash are therefore considered to be riskier, especially given the steady and confirmed reduction in the use of cash in the economy, as demonstrated below.

Firstly, cash withdrawals from ATMs are continuing to fall in 2018, there were around 260 million withdrawals totalling €35 billion or, in terms of the Belgian population, 23 withdrawals averaging €134 per Belgian citizen per year. In 2021, there were around 148 million withdrawals for a total of €22 billion, and the decline is ongoing.

This trend is reinforced by the decrease in the number of accessible bank branches and ATMs each year since 2015. The number of ATMs in Belgium has fallen from 15,306 in 2010 to 10,649 in 2019, 8,460 in 2020, 5,062 in 2021 and around 5,000 in 2022. According to current estimates, by the end of 2025 there will be 2,369 cash withdrawal sites remaining in Belgium, covering 4,061 ATMs. This

10 https://www.eurojust.europa.eu/publication/eurojust-report-money-laundering.

11 They therefore fall outside the scope of Articles 4(6) and 8 §1(3) of the AML/CFT Act.

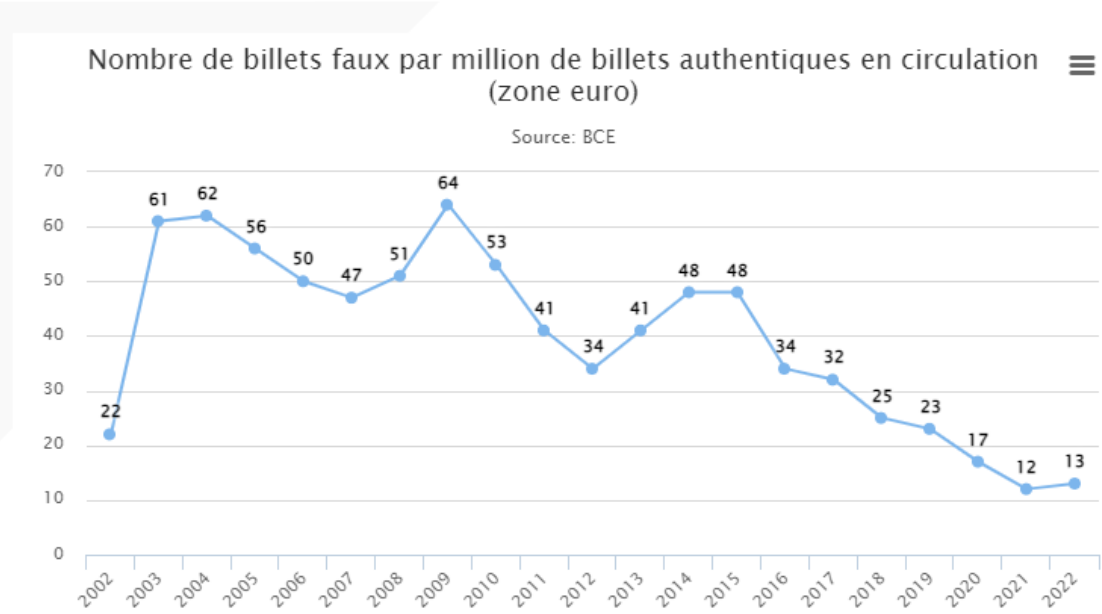
represents a decrease of 1,296 sites and 1,872 ATMs compared to the end of 2021. The reduction in the number of ATMs will affect the volume of cash in circulation but will have little impact on the use that criminals can make of it.

Branch closures due to lockdowns during the COVID-19 pandemic have fundamentally altered the behaviour of some consumers. This has prompted some financial institutions to accelerate their digital transformation plans and aim to reduce the number of branches and ATMs in Belgium. The most noticeable change in consumer banking behaviour has been the significant increase in online banking and mobile applications, but also the rise in the number of electronic payments in shops at the expense of cash. These behavioural changes will also have a longer-term impact on the channels through which financial institutions distribute their products.

To reduce the risk associated with the use of cash, the AML/CFT Act has since 2017 limited cash payments and gifts to €3,000 per commercial transaction and banned the use of cash entirely for real estate transactions.

Finally, with regard to counterfeiting, the number of forged banknotes withdrawn from circulation in Belgium has been declining steadily since 2016, notably as a result of improvements in banknote security measures and the NBB's efforts to raise awareness on the subject. According to NBB statistics, 12,016 counterfeit notes worth €589,605 were withdrawn from circulation in 2022, 24% fewer than the previous year. The same trend has been observed in the euro area.

Number of counterfeit notes per million genuine notes in circulation (euro area)



2.4.10 DISTRIBUTION METHODS/DIGITALISATION

The distribution channels used for financial products and activities have a clear influence on the risk of money laundering, in that they may have deficiencies contributing to insufficient identification of customers and their characteristics and inadequate monitoring of their transactions.

In particular, if a financial institution uses self-employed agents to distribute its products, there is a risk that, in the absence of any chain of command, some of them may be tempted to pay more attention to fulfilling the expectations of their customers, on whom their fees depend – even if those expectations are unlawful - rather than complying with the internal instructions and procedures of the

financial institution which they represent. This risk is even greater if the agent is not exclusive and can therefore divide its customers' substantial transactions into smaller, less conspicuous transactions which are carried out by the various financial institutions it represents, thus making it more difficult to detect the suspicious nature of such transactions. Institutions must therefore implement reliable and effective supervision mechanisms and allocate the necessary resources.

Furthermore, as revealed in the Joint Opinion of the European Supervisory Authorities[12], the growing digitalisation of financial activities may also make it more difficult to identify customers and know their characteristics, either through circumvention of the automatic checks (or even electronic identity theft), or more traditionally through the intertwining of multiple transactions with the aim of disguising the recipient of the laundered funds.

Digitalisation thus represents an increased ML/FT risk in cases where customer due diligence procedures insufficiently take account of the specific technical characteristics of the digital distribution channel used or are not applied correctly across all distribution methods favoured by these new players.

2.4.11 IDENTIFICATION OF CUSTOMERS AND THEIR CHARACTERISTICS

As identified in the European Commission's supranational ML/FT risk assessment of 27 October 2022, anonymity remains a vital characteristic sought by criminals for laundering funds derived from an illicit activity.

In practice, certain financial activities offering products which are entirely or partly anonymous in their composition therefore present an increased risk of money laundering.

Customer identification remains the cornerstone of the current system for combating money laundering in that it is the only way of establishing adequate knowledge of the customer's characteristics, which ultimately makes it possible to detect transactions which are potentially suspicious based on the customer's profile and which, following analysis, may need to be passed on to the Belgian Financial Intelligence Unit (CTIF-CFI).

Digitalising the process for entering into a business relationship with a customer, and consequently for identifying the customer, can give rise to risks when the technology used is not fully mastered or has deficiencies.

Document falsification, which is a real issue in Belgium[13], or the use of money mules[14] or front men for various financial activities therefore represent definite risks of circumventing the customer identification-based due diligence measures set up by institutions.

Customer identification and knowledge may also be hampered where criminals resort to complex legal structures involving multiple shell companies or letterbox companies.

---

12 Joint Opinion of the European Supervisory Authorities of 4 October 2019 on the risks of money laundering and terrorist financing affecting the European Union's financial sector (JC2019 59), updated by the EBA Opinion of 3 March 2021 on the risks of money laundering and terrorist financing affecting the Union's financial sector.

13 In 2019, the Belgian police seized almost 3,000 forged identity documents. With regard to terrorism, reference is also made to the case of the forged documents that enabled the terror cell behind the Paris and Brussels terrorist attacks to finance their attacks.

14 Money mules, also known as "cash couriers", are people who are recruited - knowingly or unknowingly - to help criminal organizations launder illicit funds. They do this by making their own accounts available to receive and transfer fraudulent funds, thus giving them an appearance of legitimacy.

To reduce the risk relating to the identification of customers and their characteristics, on 31 October 2018 the register of beneficial owners (UBO register) was launched in Belgium. However, this register does not prevent the establishment in high-risk foreign countries of opaque structures which money launderers can use to attempt to become customers of financial institutions based in Belgium while endeavouring to conceal their true identity.

2.4.12 CONCENTRATION OF POLITICALLY EXPOSED PERSONS (PEPS)

Belgium's host nation policy and, in particular, the presence of the headquarters of NATO and the European Union, affect the concentration of politically exposed persons (PEPs) on Belgian territory. Bribery of PEPs is a predicate offence to money laundering and remains a key element of the modus operandi of organised crime groups, as indicated in the EU Strategy to tackle Organised Crime 2021-2025.

The sector's exposure to this risk was highlighted by the news at the end of 2022 concerning possible bribery of members of the European Parliament, who were potential customers of institutions operating in Belgium.

In its 2021 Annual Report, CTIF-CFI indicated that the analysis of money laundering cases revealed cases involving important figures in politics, diplomacy, etc. Several of these cases concerned PEPs in Belgium or abroad or close relatives of PEPs.

Alongside the network of international organisations and national embassies, Belgium also attracts multinational companies, lobby groups, NGOs and the international press, which also contributes to the increased number of PEPs who could potentially be customers and/or beneficial owners of an institution pursuing its activity in Belgium.

This potentially high concentration of PEPs represents an increased risk for institutions with certain vulnerabilities, for example institutions pursuing activities in Belgium without having knowledge or sufficient resources to establish the origin of the assets and to ensure that they are not derived from corruption and/or intended for bribery.

2.4.13 CRIME AND RISK OF MONEY LAUNDERING LINKED TO THE ACTIVITIES OF THE PORT OF ANTWERP

Various criminal investigations in recent months have highlighted the importance of the port of Antwerp as a gateway for drug trafficking to a large part of Europe. It appears from the findings of the police and judicial authorities and from CTIF-CFI's 2021 Annual Report that money laundering of the proceeds of this trafficking occurs at two levels.

The largest amounts, directed to the organisers of the trafficking networks, require the use of more sophisticated means, such as the creation and use of shell companies through whose accounts the funds are transferred, and the use of forged commercial documents. These criminals also use certain money laundering techniques to avoid the financial system, such as offsetting or the cross-border transport of cash. However, the Belgian financial sector is also at increased risk of being used by organised crime for money laundering purposes.

Those involved at a lower level in the network use less sophisticated means to transfer funds, often in cash. Credit institutions (engaged in retail banking or trade finance), but also payment and electronic money institutions, particularly those offering payment services with accounts denominated in multiple currencies, may be particularly exposed to these risks.

2.4.14 NEW PRODUCT DEVELOPMENTS

The new products and distribution methods, in particular those based on new technologies which leave little room for individual contact between the institution and the customer, are attractive to criminals, who assume that neither financial institutions or supervisors have sufficient knowledge and expertise about the new product or method at its entry into service.

2.4.15 (ONLINE) BANK CARD FRAUD, PHISHING, SPOOFING

Due to the COVID-19 pandemic, 2020 saw an increase in all forms of online fraud, including phishing. In a phishing scam, victims are tricked into passing on their personal bank codes to fraudsters - usually by clicking on a link to a fraudulent website - enabling the latter to carry out transactions in the victim's name. In 2020, €34 million was stolen in this way in Belgium. In 2021, this figure fell to €25 million[15].

Meanwhile, investment or "boiler room" fraud is on the rise in Belgium. This is a type of scam in which fraudsters persuade victims to buy fake or worthless shares or other financial products. The victim is usually contacted unsolicited with the promise of very high returns. The criminals use bank accounts opened in Belgium or that have a Belgian IBAN. These are often virtual IBANs (see below). The NBB has been informed of several cases in which bank accounts were used by criminals to obtain funds paid by their victims, which were then transferred abroad.

A number of financial institutions in both the retail banking and money remittance sectors have been confronted with an increase in cases involving money mules. Analysis of these cases shows that the customer's activity changes abruptly (pay in and pay out suddenly to or from abroad). The Belgian judicial authorities dismantled a major network engaged in this activity in September 2021, but it is clear that many other criminals remain active from Belgium or abroad.

2.4.16 INFORMATION FROM THE CTIF-CFI ANNUAL REPORT

The CTIF-CFI 2021 Annual Report provides an overview of the reports submitted by financial institutions subject to the NBB's supervision.

Number of reports

	2019	**2020**	**2021**	**2022**
Credit institutions	11.237	17.678	21.624	28.379
Life insurance companies	308	661	749	1.172
Stockbroking firms	49	33	39	54
Payment institutions	5.814	6.263	16.016	16.425
Electronic money institutions	90	654	774	520

Number of obliged entities submitting reports

	2019	**2020**	**2021**	**2022**
Credit institutions	60	58	57	55
Life insurance companies	16	17	22	18
Stockbroking firms	6	6	6	7
Payment and electronic money institutions	37	32	32	36

15 https://febelfin.be/en/press-room/fraude-veiligheid/phishingfraude-in-2021-de-cijfers

Number of cases referred to the Public Prosecutor

	2019	2020	2021	2022
Credit institutions	783	942	990	1.029
Life insurance companies	-	2	2	6
Stockbroking firms	2	3	-	1
Payment institutions	102	96	97	80
Electronic money institutions	1	4	7	5

It is not easy to draw conclusions from an analysis of the number of reports per sector of activity.

Indeed, the total number of reports made by institutions belonging to a specific sector is inevitably impacted by the volume of their activities and of the transactions carried out by their customers. A high number of suspicious transaction reports may be indicative of the number of suspicious transactions identified and therefore the ML/FT risk incurred but can also reflect the attention paid to detecting suspicious transactions. The opposite reasoning can be applied when the number of suspicious transaction reports is low.

There has been a steady increase in the number of suspicious transaction reports in all sectors (with the exception of stockbroking firms). This is certainly due to greater awareness on the part of institutions. The actions carried out by the NBB, particularly with regard to credit institutions and payment or electronic money institutions also contributed to this increase, in particular where they led to lookbacks on past transactions that did not receive the required attention.

Furthermore, the very sharp increase (of over 300%) in suspicious transaction reports made by payment institutions seems to be partly due to some major British operators establishing themselves in Belgium following Brexit, but also to the fact that some payment institutions made reports on the sole base that transaction thresholds were exceeded. Although this can be explained by the fact that it is more difficult for these institutions to obtain information on the characteristics of their customers and, consequently, to identify transactions that are “atypical” with regard to these characteristics, such an automatic and objective reporting process is inadequate.

The table below provides a breakdown of the types of suspicious transactions in the cases transmitted by CTIF-CFI in 2021. A single transmitted case may include suspicious transactions of different types.

Type of transactions	% 2021
Domestic transfers	48,19
International transfers	22,77
Cash withdrawals from an account	11,97
Cash deposits into an account	11,51
Money remittance - Sent	2,39
Money remittance - Received	0,41
Casino transactions	0,36
E-money	0,31
Life insurance	0,25
Payments in cash	0,25
Purchase of real estate	0,15
Transport of cash	0,10
Consumer credit	0,10
Mortgage credit	0,10
Fiscal regularisations	0,05
Other	1,09
Total	**100**

2.5 ASPECTS RELATING TO TERRORIST FINANCING

The immediate and most visible consequences of terrorism are of course the atrocities committed, causing death or inflicting serious injury or trauma on citizens who are often randomly targeted by indiscriminate actions. In addition to this suffering, the IMF sees terrorism as a threat to the financial stability of a jurisdiction, the financial sector and the broader economy, with lasting effects on infrastructure and the financial system. Consequently, terrorist financing represents a risk to the monetary and financial stability of countries and should be treated as a macro-critical issue for the economy. For financial institutions in particular, involvement in terrorist financing increases risk and generates reputational risk.

It is not easy for authorities responsible for the supervision of financial institutions to analyse the risks associated with terrorist financing. As part of their activities, the intelligence services have relevant information on aspects relating to terrorist financing. The Coordination Unit for Threat Analysis (OCAM/OCAD) also conducts analyses in this context, which, however, are not intended to be shared and do not involve the NBB.

The confidentiality of investigations and the presumption of innocence, which are fundamental guarantees in a state governed by the rule of law, logically do not allow systematic and rapid communication of related information to financial institutions or even supervisors.

The designation of persons suspected of acts related to terrorism or terrorist financing on targeted financial sanctions lists provides financial institutions with an extremely useful tool but cannot be totally effective on its own.

Nonetheless, on the basis of exchanges in the Assembly of Partners (Assemblée des partenaires/Partnerraad), the 2017 national assessment of the risks of terrorism and terrorist financing, CTIF-CFI's annual reports, documents issued by Europol and information gathered from various scientific sources, it is possible to draw various lessons concerning terrorist financing activities in Belgium.

Five forms of terrorism deserve particular attention in terms of terrorist financing in Belgium[16]:

- Islamic fundamentalism
- Right-wing extremism
- Left-wing extremism and anarchism
- Terrorism linked to the political situation in a foreign country (ethno-nationalist and separatist terrorism)
- Other forms of terrorism

2.5.1 ISLAMIC FUNDAMENTALISM

The attacks of 11 September 2001 in the United States highlighted the sprawling structure of the Al-Qaeda terrorist group, which attracted the attention of the intelligence services.

Between 2015 and 2018, Belgian authorities were particularly concerned by the financing of Islamic fundamentalist terrorism, in the context of both attacks carried out on Belgian territory and attacks abroad organised from Belgium. In addition, a substantial number of Belgian citizens or residents joined the ranks of Islamic State (IS) fighters or sympathisers. The decentralised structure and operation of this group has made it possible for funds to be sent to a large number of people or organisations for the benefit of the group, but also its fighters and sympathisers, who could use them to finance terrorist activities (purchase of weapons, plane tickets, means of subsistence, etc.).

16 Europol_TE-SAT_2023.pdf (europa.eu)

In its 2021 Annual Report, CTIF-CFI indicated that the downward trend observed in recent years in the number of cases reported to it because of serious indications of terrorist financing also continued in 2021. Furthermore, the amounts involved in the reports are limited.

In its European Union Terrorism Situation and Trend Report 2022, Europol reports that one attack linked to Islamic terrorism was foiled in Belgium in 2019 and another in 2020. Respectively 11 people in 2019, 2 people in 2020 and 18 people in 2021 were arrested in Belgium for reasons linked to Islamic terrorism.

The vast majority (340) of the convictions and acquittals handed down by courts in EU Member States in 2021 for all terrorist offences concerned jihadist terrorism. Most judgments and rulings were delivered in Belgium (100) and France (83). It should also be considered that some terrorist financing activities carried out in Belgium are intended to finance a terrorist action in another country. On this subject, CTIF-CFI states in its Annual Report 2021 that the content of a significant proportion of suspicious transaction reports (22%), mainly received from payment institutions authorised in Belgium to carry out activities in the EEA under the freedom to provide services, is outsourced to CTIF-CFI's European counterparts.

The situation of returnees and their families, as well as the imminent release of people convicted of terrorism, are major points of concern for the future.

Despite the relatively low number of cases, as mentioned above, certain elements emerge from the analysis of the cases. These primarily concern the method of transferring funds and the techniques used to conceal financial flows.

The CTIF-CFI points out - as for money laundering - that the "new" online payment systems offered by neobanks[17], payment service providers (PSPs) or virtual asset service providers (VASPs) are more frequently used to finance terrorism than traditional banking services. Criminals are attracted to the international nature of these systems and the speed with which accounts are opened and transactions carried out. This is especially the case with terrorist financing, as the amounts involved are smaller than for money laundering. However, the impact of terrorist financing can be very significant, even with small amounts, as the investigations following the attacks in Paris and Brussels have shown. The risk-based approach of neobanks and PSPs is generally based on the size of the amounts and is therefore severely tested when it comes to terrorist financing, even more than for money laundering, given the small amounts per transaction.

2.5.2 RIGHT-WING EXTREMISM

Since 2020, there has been an increase in cases relating to right-wing extremism, a trend that continued in 2021. This type of extremism is gaining in importance and visibility in both Belgium and Europe. It concerns individuals and groups whose ideology is based on racism, nationalism, and totalitarianism. However, with the alt-right movements in the United States and the identity discourse and ultra-conservative currents in Russia and Eastern Europe, right-wing extremism in Belgium and Western Europe has become more complex to describe, analyse and combat than 20 years ago. This difficulty is compounded by the fact that, unlike with Islamic fundamentalist terrorism, there is no central right-wing extremist organisation that acts as the disseminator of the ideology and receives the bulk of financial support.

Europol reports that one attack linked to extreme right-wing terrorism was foiled in Belgium in 2020 and another in 2021. Respectively 1 person in 2020 and 3 people in 2021 were arrested in Belgium for reasons linked to extreme right-wing terrorism.

---

17 Neobanks use technology to offer retail banking services, mainly through a smartphone application and an internet platform. They offer a range of services including checking, deposit and business accounts, credit cards, financial advice and loans.

In addition to the strict application of the asset freeze regime, a list has been drawn up of acronyms, logos and numerical codes that, when used in names or communications, can serve as criteria for identifying this ideology.

Analyses currently do not show a close link between the financing of extreme right-wing terrorism and money laundering. It seems that the funds used to finance this terrorism generally come from the legitimate personal resources of supporters of the cause (salaries, savings, etc.) or from fundraising activities (concerts, etc.). Social networks are used to attract funds. Right-wing extremists also show an interest in crypto-currencies. In principle, the activities of right-wing extremists do not require travel or departure from their home country (as was the case with the financing of IS in Syria), since any terrorist activities financed are carried out on national territory. The only potential warning signs are an individual's links and financial transactions with certain notorious associations or sympathisers.

However, CTIF-CFI's work has shown that, in several cases, certain extreme right-wing organisations were found to have financial links with foreign counterparts. It was also noted that organisations which have modern working methods and a thorough understanding of social media have seen their funding increase sharply in recent years.

Financial analyses also reveal that individuals with a right-wing extremist ideology regularly make purchases from foreign online shops that exclusively target people with this ideology.

2.5.3 LEFT-WING EXTREMISM AND ANARCHISM

Left-wing extremism and anarchism are manifested in Europe in the destruction (arson attacks) of or damage to property representing an ideology or activities contrary to their ideology (5G installations, bank branches, ATMs), or in the disclosure of sensitive data concerning natural or legal persons.

Europol's European Union Terrorism Situation and Trend Report 2022 shows that 6 people linked to extreme left-wing terrorism and anarchism were arrested in Belgium in 2021.

Analyses currently do not show a close link between the financing of extreme left-wing terrorism and money laundering. It seems that the funds used to finance this terrorism generally come from the legitimate personal resources of supporters of the cause (salaries, savings, etc.) or from fundraising activities (concerts, etc.).

2.5.4 ETHNO-NATIONALIST AND SEPARATIST TERRORISM

Ethno-nationalist and separatist terrorism was a major threat in the EU in the not-too-distant past, mainly through the activities of groups such as ETA in Spain and the IRA in Northern Ireland. However, the terrorist activities of these groups have declined significantly in recent years.

Belgium may be affected by terrorism linked to the activities of the PKK in Turkey, firstly because of the presence of a Turkish diaspora and secondly because of the establishment in Belgium of the European Kurdish Democratic Societies Congress (KCDK-E), the political branch of the Kurdish separatist movement.

Two people were arrested in 2019 in connection with ethno-nationalist and separatist terrorism in Belgium.

2.5.5 OTHER FORMS OF TERRORISM

Certain official documents[18] identify a threat linked to ecoterrorism, which is defined as the use or threatened use of violence of a criminal nature against persons or property by a subnational group for environmental-political reasons. This concept has been defined and observed in the United States since the 1990s, and some movements are classified on the FBI's domestic terrorist movements list. Ecoterrorists commit violent acts of protest or civil disobedience aimed at protecting the planet or saving animals. Such violent actions (bombings, arson attacks) have been observed in the United States, but not in Belgium or Europe. However, the growing radicalisation of certain rhetoric and actions suggest that a potential threat could emerge.

2.5.6 CURRENT TREND IN TERRORIST FINANCING ACTIVITIES

The downward trend observed in recent years in the number of cases transmitted to CTIF-CFI because of serious indications of terrorist financing continued in 2021. Furthermore, the amounts involved in the reports are limited. However, the drop in the number of cases does not mean this threat no longer exists. In 2022, there were 215 reports of threats linked to terrorism or extremism in Belgium. This figure is comparable to that for 2021. It was also found that between 1 January and 30 April 2023, three planned attacks were foiled in Belgium.

CTIF-CFI's analysis of the cases revealed a number of striking similarities.

For instance, the terrorist networks that were active in Belgium mainly between 2015 and 2016 used cash because of its anonymity and the lack of expertise required.

It has also been observed - as with money laundering - that **the "new" online payment methods** offered by payment service providers (PSPs) are increasingly being used to finance terrorism.

Some risks associated with terrorist financing seem to be moving away from "traditional" activities such as money transfers or the use of cash towards newer products and services. For example, the "e-wallet" or "**ibanisation**" activities that are currently being developed may be attractive in terms of terrorist financing. These activities, which involve payment accounts denominated in multiple currencies, enable customers to open a set of accounts identified by IBANs with different national codes simultaneously with a financial institution, making it difficult to trace transactions and to identify the financial institution that holds the funds and carries out the transactions ordered by the customer.

The international nature and the speed with which these accounts are opened, and transactions are carried out, present new challenges for financial intelligence units. This is particularly the case with terrorist financing, as the amounts involved are smaller than for money laundering and are therefore more difficult to detect. However, the impact of terrorist financing can be very significant, even with small amounts. The risk-based approach of some financial institutions relies too much on the analysis of transaction amounts and volumes, which is insufficient, particularly with regard to terrorist financing.

The transition to online payment systems is also partly the result of a certain degree of de-risking on the part of traditional banks. As a result, the accounts of high-risk customers (family members of people whose assets are frozen, or people whose names are mentioned in an investigation) are sometimes closed. This not only makes the work of financial intelligence units and intelligence services more difficult, but also encourages these people to turn to institutions offering inter alia online services, which are often based abroad. The financial trail in their own country then stops and becomes difficult to follow.

---

18 Europol – European Union Terrorism Situation and Trend Report 2022

Digital assets can be used to anonymously acquire goods or transfer funds internationally. In this case, customers convert their funds into digital assets, then use the blockchain to carry out a peer-to-peer transaction, after which they convert the funds back into legal tender.
These funds can then be withdrawn in cash from a local commercial business or from an automated kiosk. Crypto assets can be used inter alia to purchase goods, weapons and products on the darknet.

However, the use of digital assets requires specific skills and technical expertise, which hinders access by criminal and terrorist groups, even though these assets are becoming increasingly accessible. The high volatility of digital assets and the relative lack of liquidity of some of them also limit the possibility of them being used for money laundering or terrorist financing purposes.

As a reminder, the NBB has no jurisdiction on the supervision over virtual asset trading platforms.

Traditional banking services (retail accounts) also remain a possible vector for terrorist financing, through the use and transfer of the personal resources of terrorists or sympathisers of the cause.

2.6 PERIOD CONSIDERED

In view of the availability of data on the institutions subject to NBB supervision, this assessment is based on the situation as at 31 December 2022, and will be updated on the basis of a two-year cycle.

2.7 SCORING

In a first stage, the inherent risks of each activity considered are assessed and quantified by a score (of 1 to 5)[19]. “Inherent risk” means the risk of the activity being used for money laundering purposes on account of its nature and objective characteristics, disregarding any measures financial institutions may take to reduce and manage this risk. An activity’s inherent risk level is also influenced by its relative importance in the Belgian financial sector.

Next, each activity is given a score (of 1 to 5) for the vulnerabilities identified in institutions pursuing these activities. Vulnerability should be understood as the risk that financial institutions engaging in the activity concerned may not have an adequate organisation and internal control system or sufficient resources to reduce and manage the inherent risks of that activity. This score is based inter alia on the knowledge gained by the NBB via - in particular but not exclusively - its off-site supervision and various inspections, as well as the associated findings and recommendations.

The two scores for the activities assessed are then entered in a matrix forming the basis of the overall assessment for the sector as a whole, which determines the “residual risk” relating to each activity based on the combination of the inherent risk level and the vulnerability level. For example, an activity considered to present a high inherent risk but low vulnerability may be given a lower residual risk score (“overall score”) than an activity with a lower inherent risk but higher vulnerability.

3 PAYMENT AND ELECTRONIC MONEY INSTITUTIONS

This section covers six specific types of activity: (i) traditional payment activities, (ii) money remittance activities, (iii) acquiring activities, (iv) payment initiation services, (v) account information services, and (vi) electronic money activities. New services related to payment accounts denominated in multiple currencies are also discussed.

---

[19] 1 = low; 2 = moderate; 3 = significant; 4 = high; 5 = critical

As stated in point 2.4, the payment and electronic money sector continues to undergo profound changes following the arrival of a series of new players on the Belgian market.

The number of payment and electronic money institutions operating in Belgium has risen sharply in recent years. This trend has been amplified by Brexit and the need for a number of UK institutions to establish themselves in continental Europe in order to obtain authorisation, which allows them to carry out their activities throughout the EEA. Between 2016 and 2021, the NBB granted authorisation to over a dozen institutions in this context, including major players such as MoneyGram International, WorldRemit Belgium, Ebury, PPS EU and Wise Europe.

The large increase in the number of players from other Member States of the EEA, combined with the significant growth in the number of players offering products under the freedom to provide services[20], i.e. without being established in Belgium via a branch or a network of agents and/or distributors, is radically altering the sector's dynamics and influencing both risk appetite models and the knowledge that payment institutions may have about financial activities that are spread over a multitude of players and products.

Except for a number of institutions specialising in one particular activity, e.g. account information services or payment initiation services, most institutions pursue multiple payment activities simultaneously or in conjunction with other partners.

It appears from reports to the NBB that the majority of institutions that specified the nature of their activities as at 31 December 2022 provided, in practice, payment services that are not or only slightly diversified.

3.1 PAYMENT SERVICES

3.1.1 DESCRIPTION OF THE ACTIVITY

What is meant by a payment service activity?

Payment services cover various types of specific activities provided in whole or in part by payment and electronic money institutions (including branches of EEA and non-EEA institutions) established in Belgium and by payment and electronic money institutions authorised in other Member States of the European Economic Area and active in Belgium via one or more agents and/or distributors.

These activities include:

1. All operations required for managing a payment account (including services enabling cash to be placed on a payment account);
2. Services enabling cash withdrawals from a payment account;
3. Execution of payment transactions:
   - Execution of direct debits, including one-off direct debits;
   - Execution of payment transactions through a payment card or similar device;
   - Execution of credit transfers, including standing orders;
4. Execution of payments for which the funds are covered by a credit line granted to the payment service user:
   - Execution of direct debits, including one-off direct debits;
   - Execution of payment transactions through a payment card or similar device;
   - Execution of credit transfers, including standing orders;
5. Issuing and/or acquiring of payment instruments;

[20] Most of these institutions originate from the United Kingdom and the Netherlands in the case of payment institutions, and the United Kingdom, Lithuania and Cyprus in the case of electronic money institutions.

6. Money remittance;
7. Payment initiation services;
8. Account information services.

Since the last three activities have their own specific characteristics in terms of ML/FT risks, they are analysed separately.

Although payment activities in the strict sense have traditionally been performed by the banking sector, their performance by payment institutions offers added value compared to traditional banking activities, not only due to these institutions' digitalisation, shorter transaction times and integration and distribution networks, but also their competitive advantage in terms of exchange rate margin and correspondent banking fees or in the related non-financial services linked to the products of these activities.

Activities of payment institutions in Belgium

As per 31 December 2022, there were 71 authorised institutions falling under the AML/CFT supervision of the NBB.

This figure breaks down into 34 authorised payment institutions governed by Belgian law, 8 payment institutions governed by the law of another EEA Member State that maintain a branch in Belgium, and 24 institutions operating in Belgium through an establishment consisting solely of one or more agents. The latter only fall under the NBB's AML/CFT supervision and not under its prudential supervision.

Finally, there are 5 institutions authorised as electronic money institutions but which also provide payment services, and 1 institution governed by the law of another EEA Member State.

Apart from money remittance services (see point 3.2) and electronic money services (see point 3.6), payment activities in Belgium focus on the provision of accounts and means of payment for individuals and businesses as well as payment terminals and online payment solutions for business users.

These institutions offer their services primarily online or via a network of agents/distributors, and do not necessarily have a physical presence in Belgium.

The number of payment institutions operating in Belgium has risen sharply in recent years. This trend has been amplified by Brexit and the need for a number of UK institutions to establish themselves in continental Europe in order to apply for a European passport to carry out their activities throughout the EEA. These institutions were sometimes found to be implementing a minimalist structure in Belgium without allocating sufficient control and human resources, and to be relying heavily, via agreements to outsource AML/CFT functions, on the organisation in place within the group, which is often based outside the EEA. On-site inspections and other controls carried out by the NBB at some of these institutions have revealed that their AML/CFT systems do not fully meet Belgian statutory and regulatory requirements.

3.1.2 RISKS INHERENT IN THE ACTIVITY

As a large number of different products are classified as payment activities, it is first necessary to make a distinction between the associated risks according to the institution's involvement in the payment transaction; a provider of payment initiation services or account information services is not in fact subject to the same risks as an institution offering services involving cash deposits/withdrawals or money remittance.

The high inherent risk associated with payment institutions is primarily explained by the following **general risk factors**[21]:

- the high volume and speed of transactions, which are mainly monitored post-execution on the basis of the customer's transactional activity;
- the intensive use of cash;
- the prevalence of occasional transactions over established business relationships, and the resulting lack of knowledge of the customer's profile;
- geographical corridors for transferring funds to high-risk jurisdictions;
- the use of new technologies to facilitate remote customer onboarding;
- the distribution channel used (a network of agents and distributors).

As regards **product risks**, payment activities enable faster, higher-volume transfers than other financial products, which makes them particularly attractive for the mass transfer of funds derived from illicit activities.

Moreover, most payment activities continue to use cash. For instance, only 35% of payment institutions offering payment services in Belgium that responded to the periodic questionnaire on AML risks indicated that they do not offer any products involving cash (deposit and/or withdrawal).

The sector is also particularly prone to **transversal risks** that are associated with knowledge of the customers, their characteristics and the purpose of the business relationship, digitalisation, and to risks associated with the distribution network when it includes physical agents who are not in themselves subject to the AML/CFT Act.

Payment institutions are offering new services related to payment accounts denominated in multiple currencies ("ibanisation"). More specifically, these services involve the issue and use of digital international bank account numbers, also called virtual IBANs, which are intended solely to redirect incoming payments to an ordinary IBAN linked to a physical bank account. This makes it more difficult to identify and locate the underlying account. These services can also make it more difficult for financial intelligence units to identify transactions, which makes them attractive to criminals. Some institutions governed by Belgian law offer these accounts and payment services to companies generating large sums of money. The presence of institutions governed by Belgian law that are very active in these activities, increases the risk for the Belgian market.

A new phenomenon known as "**white-label banking**" has also been identified in the sector. This involves payment institutions making their licence available to independent agents who develop their own product under the licence of the regulated institution. It is difficult for the regulated institutions to properly integrate all these products and the corresponding risks into their AML/CFT framework and to adequately monitor and control these risks (Enterprise-Wide Risk Assessment (EWRA), agent monitoring, transaction monitoring, etc.). The presence of institutions governed by Belgian law that are very active in these activities, increases the risk for the Belgian market.

Apart from the traditional risks of money laundering which also apply to e.g. deposit activities, the European Commission's supranational ML/FT risk assessment of 27 October 2022 specifically identifies the high-risk case in which payment services are used, misused or controlled directly by criminal organisations for money laundering purposes without adequate due diligence measures being implemented within a reasonable period of time to permit prompt intervention.

The inherent risk of payment activities varies greatly according to the product characteristics and distribution arrangements. Without prejudice to the individual assessment of the inherent risk

[21] These risks factors have been highlighted since 2017 in the European Commission's supranational ML/FT risk assessment of 27 October 2022 and in successive EBA opinions on ML/FT risk.

associated with each institution, the average level of this risk is consequently assessed as high (score of 4 out of 5).

3.1.3 VULNERABILITIES OF INSTITUTIONS PURSUING THE ACTIVITY

Although institutions pursuing payment activities have differing profiles and activities (from very small businesses to large firms in a global financial group), the vulnerabilities of these institutions identified by the NBB via its off-site supervision or its on-site inspections, are often but not exclusively related to:

- unwillingness to establish a structure in Belgium that is independent of group entities located outside the European Union;
- lack of experience and relevant, ongoing AML/CFT training of management and/or staff;
- high turnover of AML/CFT staff and difficulties in recruiting staff with knowledge of the subject in Belgium;
- inadequate preventive framework (unsatisfactory automated procedures and monitoring tools);
- lack of in-depth knowledge of the Belgian statutory and regulatory AML/CFT framework and of the sanctions and embargoes regime;
- non-application of the statutory provisions owing to the absence of checks relating to PEPs;
- poor organisation of the three lines of defence with regard to AML: some outsourced functions are not sufficiently supervised or properly carried out, the procedural framework is not fully adapted to Belgian regulations and its implementation is not sufficiently efficient;
- knowledge of customers is based mainly on a posteriori analysis of their transactional activity, and alerts are triggered primarily when thresholds are exceeded, without taking sufficient account of the customer's transactional behaviour;
- weak analysis of the origin of customer funds;
- weak resources allocated to supervision of the distribution network, whether digital or through physical points of sale.

Some of these observations were confirmed during on-site inspections carried out by the NBB.

As mentioned above in point 2.4.13, the sector may be exposed to crime linked to the activities of the port of Antwerp.

In addition, the diamond industry, which is particularly important in Belgium, is highly vulnerable to ML/FT risks. Following de-risking decisions taken by certain credit institutions, companies active in the diamond industry have turned to payment institutions offering payment accounts that are sometimes denominated in multiple currencies, which can make transactions more difficult to trace.

Consequently, without prejudice to the individual assessment of the vulnerability of each institution, the average vulnerability level of payment institutions subject to NBB supervision are assessed as high (score of 4 out of 5) based on their nature, the characteristics of their products and their distribution networks.

3.1.4 OVERALL SCORE OF THE ACTIVITY

In view of the significant inherent risks in payment activities and the substantial vulnerabilities of the institutions offering these products, the residual risk of money laundering associated with payment activities is generally assessed as high (score of 4 out of 5).

3.1.5 TERRORIST FINANCING

Inherent risk

Payment institutions can be attractive for terrorist financing due to the speed with which primarily international transactions are carried out, including to high-risk countries.

CTIF-CFI's 2021 Annual Report shows in particular that the "new" payment services, especially those offered online by payment institutions, could be used to finance a terrorist group or action. This is particularly the case for services enabling accounts to be opened in multiple currencies.

The international nature and the speed with which accounts are opened and transactions are carried out, can make them attractive to criminals. This is especially the case with terrorist financing, as the amounts involved are smaller than for money laundering.

The inherent risk of terrorist financing associated with this activity is assessed as high (score of 4 out of 5).

Vulnerability

The risk-based approach applied by these institutions is generally based on the volume and amount of their transactions. However, it was found between 2015 and 2018 that terrorist attacks were financed by various small-value transactions.

Regulations require institutions to draw up a customer profile that takes into account all the customer's characteristics and not just transactional activity. This is not always the case in practice.

This activity's vulnerability to terrorist financing is assessed as high (score of 4 out of 5).

Residual risk

The residual risk of terrorist financing associated with this activity is assessed as high (score of 4 out of 5).

3.2 MONEY REMITTANCE

3.2.1 DESCRIPTION OF THE ACTIVITY

Money remittance is "a payment service where funds are received from a payer, without any payment accounts being created in the name of the payer or the payee, for the sole purpose of transferring a corresponding amount to a payee or to another payment service provider acting on behalf of the payee, and/or where such funds are received on behalf of and made available to the payee"[22].

Money remittance distinguishes itself from other payment activities in that transfers are made without any account necessarily being opened in the name of the payee and/or the payer.

Money remittance activities are mostly aimed at private individuals, although some products are specifically offered to businesses and professionals since they sometimes offer certain advantages over more traditional correspondent banking.

---

22 Article 4(22) of Directive 2015/2366.

Through vast networks of local agents and points of sale, in Belgium or abroad, money remittance activities can reach people throughout the world in countries or regions where few if any financial institutions have a presence. This activity has a definite social interest in the sense that the vast majority of transfers made by diaspora members are for family support.

In view of their ease of access, the speed of transfer and sometimes attractive fees , money remittance institutions target customers who would not naturally turn to a classic bank for this type of services.

There are several major institutions governed by Belgian law operating on the global market which offer money remittance services that are conducted mainly in cash (MoneyGram International) or exclusively digitally (WorldRemit).

Among the payment institutions subject to NBB supervision, 15 institutions declared that they engaged in money remittance activities as at 31 December 2022. [23]

On 31 December 2022, money remittances carried out from Belgium by customers of payment institutions represented more than €1 billion on an annual basis, almost half of which was in cash. Almost half the volume of remittances was destined for a high-risk country.

The main outgoing money remittances in Belgium are destined for Morocco and the Democratic Republic of Congo, while incoming payments primarily originate from Congo and Cameroon. This can be attributed to the presence of a large diaspora in Belgium. The other main high-risk countries originating or receiving remittances are Afghanistan, Ivory Coast, Tunisia and Turkey.

The great majority of institutions in Belgium accept cash as the means of effecting money remittances, and most operate both online and via a large network of non-exclusive agents, mainly retail businesses.

3.2.2 RISKS INHERENT IN THE ACTIVITY

The majority of money remittance activities still use cash. However, the largest traditional players operating in Belgium are developing and encouraging (by reducing fees) the use of digital remittance applications.

Some institutions only use digital distribution channels. While the inherent risk is reduced by the absence of cash, it is increased by the absence of contact at the start of the business relationship and weaknesses in remote onboarding methods, which make it possible for the same customer to create multiple profiles.

Money transfers, by their nature, provide less assurance of efficient knowledge of customers' activities, not only because they make it difficult to establish that the occasional nature of transactions characteristic of the business model has been exceeded, but mainly due to the fundamental characteristic that no account is opened. There is a strong need for procedures to ascertain the customer’s identity and characteristics, especially if the transfer takes place to or from a high-risk country.

In regard to product risk, money remittance services remain intrinsically linked to the use of cash, as they are – by nature – aimed at profiles with little or no access to banking services. The product risk associated with money remittance is therefore significant.

---

[23] It should be noted that credit institutions can also remit funds, but for those institutions this activity is in practice usually linked to the creation of an account and therefore does not meet the definition of money remittance as understood in this analysis.

In regard to geographical risk, it seems that money remittance services are aimed mainly at persons with links to countries considered to present a high risk of money laundering. Money remittance activities are thus often linked to a high geographical risk, all the more so in the case of remittances to a country with different informal money remittance systems, which makes them even more attractive to money launderers.

Where money remittance activities are aimed at customers from sectors of the illegal economy or sectors known for their money laundering risks, the customer-related risk is even higher.

Payment institutions are exposed to the risk of fraud, in particular through criminals' use of money mules to help layer the proceeds of the fraud. The use of mules has been identified in Belgium in connection with various types of fraud (romance scams, phishing, etc.).

It should also be noted that the risk incurred by the various institutions operating in this sector varies due to differences in the products and services offered.

In view of the above, the inherent risk associated with the money remittance activities of payment institutions is assessed as high (score of 4.5 out of 5).

3.2.3 VULNERABILITIES OF INSTITUTIONS PURSUING THIS ACTIVITY

It should be noted once again that institutions pursuing money remittance have differing profiles and activities (from very small businesses to large firms in a global financial group).

Controls have shown that some institutions have a minimalist structure in Belgium and rely heavily on the organisation in place within the group, which is often based outside the EEA.

On-site inspections and other controls by the NBB at some of these institutions have sometimes revealed that their AML/CFT systems do not fully meet statutory and regulatory requirements.

In regard to the distribution risk, money remittance services primarily rely on local distribution networks consisting mainly of retail businesses which do not offer the necessary guarantees for ensuring proper application of the statutory AML requirements. These agents often offer services from several institutions. All the institutions subject to NBB supervision which engage in money remittance are SMEs (with less than 250 FTEs), but some of them use a network of more than 2,500 agents/distributors, most of whom are not exclusive and can therefore offer multiple competing products. The vast majority of these agents are not subject to supervision or any form of professional ethics or rules. Information available to the NBB also shows that organised criminals are attempting to enter the sector through agents working with them, either voluntarily or under duress (blackmail, etc.). Organised criminals could use these agents' position and access to information and systems to carry out money laundering transactions.

Monitoring and recent inspections of payment institutions involved in money remittances revealed the following vulnerabilities:

- unwillingness to establish a structure in Belgium that is independent of group entities located outside the European Union;
- lack of experience and relevant, ongoing AML/CFT training of management and/or staff;
- high turnover of AML/CFT staff and difficulties in recruiting staff with knowledge of the subject in Belgium;
- poor organisation of the three lines of defence in terms of AML: some outsourced functions are not sufficiently supervised or properly carried out;
- inadequate preventive framework (unsatisfactory automated procedures and monitoring tools);

- incomplete overall risk analysis taking no account of the risks presented by new products or specific geographical risks;
- lack of in-depth knowledge of the Belgian statutory and regulatory AML/CFT framework and of the sanctions and embargoes regime;
- weaknesses in remote onboarding methods;
- knowledge of customers is based mainly on an ex-post analysis of their transactional activity;
- alerts are triggered primarily when thresholds are exceeded, without taking sufficient account of the customer's transactional behaviour;
- lack of analysis of the origin of customer funds;
- inadequate resources allocated to supervision of the distribution network, whether digital or through physical points of sale;
- inadequate supervision of the agent network, either owing to a lack of human and/or material resources allocated to training and supervision, or because the institution's monitoring measures are inappropriate;
- the fact that many agents are not exclusive also weakens the ability of payment institutions to monitor all remittance activities pursued by those agents, and enables agents to split large remittances into smaller transactions effected via the various money transmitters that they represent;
- insufficiently thorough monitoring of transactions effected by agents in their own name.

Some of these observations were confirmed during on-site inspections carried out by the NBB.

Continuous monitoring and individual inspections in particular led to improvements in methods of reporting to CTIF-CFI and in AML control systems. However, there has been a very sharp increase (of over 300%) in suspicious transaction reports made by payment institutions, which seems to be partly due to the fact that some payment institutions made reports on the sole basis that transaction value thresholds were exceeded. Such a procedure is inadequate.

As a result, the vulnerability to money laundering risks of institutions engaging in money remittance is assessed as high (score of 4 out of 5).

3.2.4 OVERALL SCORE OF THE ACTIVITY

Based on the high inherent risk (score of 4.5 out of 5) and the high level of vulnerabilities (4 out of 5) identified for money remittance activities, the residual risk of this activity is assessed as high (4.5 out of 5).

3.2.5 TERRORIST FINANCING

Inherent risk

More specifically with regard to terrorist financing in Belgium, it was found that certain terrorist attacks carried out in or largely organised and prepared from Belgium between 2015 and 2018 were financed by various money remittance transactions of generally small amounts that were carried out by various parties, some of which had family relations with each other, which made it more difficult to identify the transactions.
According to Europol, jihadist actors use money transfer services directly or via money mules. Mules are key figures in these networks: they act as intermediaries and collectors of cash on behalf of the end receiver. Intermediaries have also been noted to withdraw money from remittance services in locations outside the EU and close to conflict zones, where the money is then routed and handed over to the receivers.

Money remittance products and services are attractive for terrorist financing, in particular because of the speed with which international transactions are carried out and the possibility of splitting transfers, whether with the same money remitter or different ones.

The inherent risk of terrorist financing associated with this activity is assessed as high (score of 4 out of 5).

Vulnerability

Following the first terrorist attacks in 2015, the main players in the sector developed monitoring scenarios to identify and limit money remittances to Turkey's border area with Syria. However, it was revealed afterwards that some agents did not act with sufficient due diligence and accepted money remittances with the justification that they were intended to purchase medicines or were meant for a family member with whom the family link could not be proved.

To date, controls carried out by the NBB on payment institutions have not revealed any failure to comply with sanctions, asset freezes or embargoes.

This activity's vulnerability to terrorist financing is assessed as high (score of 4 out of 5).

Residual risk

The residual risk of terrorist financing associated with this activity is assessed as high (score of 4 out of 5).

3.3 ACQUIRING ACTIVITIES

3.3.1 DESCRIPTION OF THE ACTIVITY

Acquiring activities refer to the various activities associated with carrying out transactions and which enable points of sale or on e-commerce websites to accept transactions. The role of the acquirer is to facilitate or carry out the clearing and settlement of transactions.

The activity in Belgium

There are currently 4 Belgian payment institutions offering payment initiation services that specialise in acquiring. However, the Belgian market is characterised by major players operating on the international market that offer services linked to activities carried out by points of sale or on e-commerce websites. In addition, some credit institutions also carry out acquiring activities.

3.3.2 RISKS INHERENT IN THE ACTIVITY

Acquiring activities present certain money laundering risks.

In terms of product risk, it should be noted that these activities make it possible to carry out financial transactions that are cross-border and involve substantial amounts.
Acquiring services provided by third-party merchants has been identified as an emerging trend generating new money laundering risks for payment institutions. The merchant acquirer, which is the entity providing payment services to merchants, outsources certain parts of the acquiring process to a third-party acquirer (TPA). The TPA puts the merchant acquirer at risk of indirectly dealing with illicit funds should the framework put in place prove to be insufficient.

The lack of adequate or up-to-date knowledge of the actual activities of the customer operating a point of sale equipped with a payment terminal or an e-commerce website constitutes a risk. It is possible that this activity does not correspond to the activity declared when the business relationship was entered into, or that this activity is subsequently modified.

Certain customer activity sectors are identified as presenting a high risk, such as those “reserved for adults”, gaming, gambling, tobacco, or certain pharmaceutical products.

Acquiring activities also make it possible to send funds to or receive funds from counterparties established in high-risk third countries.

Some international studies indicate the emergence of an activity involving the rental of “private” ATMs for cash withdrawals. Such an activity, which is not currently authorised in Belgium, presents risks in that it would allow the ATM lessee to replenish the machine with funds derived from illicit activities.

However, the possibility of materialisation of these risks is considered to be moderate. In view of the above, the inherent risk associated with acquiring services is assessed as moderate (score of 2 out of 5).

3.3.3 VULNERABILITIES

Institutions operating in this segment must ensure that the activity of the customer (i.e. the merchant or e-commerce website) at all times corresponds to the activity declared at the start of the business relationship, and that the volume of transactions is consistent with the customer’s profile and expected activity.

They must also be able to check the identity of the customer’s beneficial owners on a regular basis, as they are at risk of not detecting quickly enough potential changes with regard to the UBOs who control these activities.

While it is the acquirer who is involved in the payment transactions, the financial institution with which the payment accounts are opened is also required to exercise due diligence with regard to the customers, in order to improve its knowledge of them, and with regard to the customers’ transactions, which mitigates the risk.

As a result, the vulnerability to money laundering risks of institutions engaging in acquiring activities is assessed as moderate (score of 2 out of 5).

3.3.4 OVERALL SCORE OF THE ACTIVITY

Based on the moderate inherent risk (score of 2 out of 5) and the identification of moderate vulnerabilities (2 out of 5) for acquiring activities, the residual risk of this activity is assessed as moderate (2 out of 5).

3.3.5 TERRORIST FINANCING

Inherent risk

Acquiring activities do not appear to present any particular risk of terrorist financing. The use of acquiring services for the purpose of financing terrorist activity would require knowledge, a set of procedures and the implementation of a structure. This renders these services unsuitable for terrorist financing in Belgium. Belgium.

The inherent risk of terrorist financing associated with this activity is assessed as low (score of 1.5 out of 5).

Vulnerability

This activity's vulnerability to terrorist financing is assessed as low (score of 1.5 out of 5).

Residual risk

The residual risk of terrorist financing associated with this activity is assessed as low (score of 1.5 out of 5).

3.4 PAYMENT INITIATION SERVICES

3.4.1 DESCRIPTION OF THE ACTIVITY

Payment initiation is when a service provider gives instructions on behalf of another person to the financial institution with which that other person has a payment account, to execute payments from that account (of which the service provider is not a holder).

This service may be offered in the context of a business relationship between the payment initiation service provider (PISP) and a merchant (usually engaging in e-commerce), in order to make it easier for the merchant's customers to pay for their purchases, and thus to give the merchant a guarantee that those payments will actually be executed. In this case, there is no business relationship between the PISP and the merchant's customers, and the merchant is the sole potential recipient of payments initiated by the PISP.

However, PISPs may also offer their services to a person holding the account(s) from which the payments will be initiated, with the aim of facilitating the payments to be made by that person from the account(s) in question. In this case, payments are made to an extremely large range of recipients with whom the PISP does not have any business relationship. The service makes it possible to initiate payments for reasons which are not necessarily linked to the business activities of the payees and which are unknown to the PISP.

Payment initiation can be offered by all types of payment service providers (credit institutions, payment institutions, electronic money institutions), in which case it supplements the range of services which they offer to their customers. However, it may also be offered by payment institutions specialising solely in this activity.

The activity in Belgium

At present there are 9 Belgian payment institutions offering payment initiation services, of which only 4 specialise in offering this service in combination with account information services (see chapter 3.5 below) but without simultaneously offering payment accounts or credit services or issuing payment instruments. For the purposes of this chapter, only these 4 institutions are considered to be PISPs.

3.4.2 RISKS INHERENT IN THE ACTIVITY

Payment institutions that only provide payment initiation services present a low risk, as this service is limited to the execution of a payment transaction at the request of a customer. These service providers do not hold customer funds at any time.

However, PISP activity is not entirely devoid of money laundering risks.

There are risks related to the product itself, as it enables the transfer of large amounts of funds from different payment accounts to the same person without there necessarily being any economic justification.

Where PISP services are offered to the holders of the payment accounts concerned, payments can be initiated to a very wide range of recipients without it being possible to establish the reason.

Sending or receiving funds associated with counterparties established in high-risk third countries constitutes a geographical risk.

However, it should be pointed out that:

- the PISP is never in possession of funds belonging to the holder of the payment accounts concerned;
- the intervention of the PISP in no way impedes the performance of the due diligence obligations (in particular the transaction monitoring) of the financial institution with which the payment account concerned is opened.

In view of the above, the inherent risk associated with payment initiation services is assessed as low (score of 1.5 out of 5).

3.4.3 VULNERABILITY OF INSTITUTIONS PURSUING THIS ACTIVITY

PISPs are to some extent vulnerable to money laundering, in particular because:

- unlike the financial institution with which the account concerned is opened, the PISP does not have full information on all the transactions effected via that account, but only those initiated by the PISP itself;
- PISP activities are often pursued by small firms that are focused mainly on developing new technological solutions, and which do not necessarily have detailed knowledge of the Belgian statutory and regulatory AML framework.

Conversely, where the payment initiation service is offered in the context of a business relationship with the merchant, the PISP is able to ensure that the payments initiated by it are consistent with the merchant's profile and commercial activities.

As a result, the vulnerability to money laundering risks of institutions pursuing payment initiation activities is assessed as moderate (score of 2.5 out of 5).

3.4.4 OVERALL SCORE OF THE ACTIVITY

Notwithstanding the low inherent risk (score of 1.5 of out of 5) associated with payment initiation activities, due to the moderate level of vulnerability (2.5 out of 5), the residual risk is assessed as moderate (2 out of 5).

3.4.5 TERRORIST FINANCING

It follows from the above that this activity does not give rise to any particular risk of terrorist financing, as the institutions concerned do not hold any customer funds. However, through their activities, they could have a more complete view of an individual's transactions from multiple accounts.

The residual risk of terrorist financing associated with this activity is assessed as low (score of 1.5 out of 5).

3.5 ACCOUNT INFORMATION SERVICES

3.5.1 DESCRIPTION OF THE ACTIVITY

Account information services are services that enable the customer to access, through a single interface, information relating to their balances and transactions across multiple institutions.

Account Information Service Providers (AISPs) may offer this service as their primary activity or as an ancillary activity.

The activity in Belgium

In addition to the 4 Belgian payment institutions offering account information services in combination only with payment initiation services, only 3 companies are authorised in Belgium to offer account information services exclusively.

3.5.2 INHERENT RISKS OF THE ACTIVITY

Account information services do not involve any intervention in the execution of customer transactions, and in particular do not place the AISP in possession of customer funds. Furthermore, account information services do not impair the ability of financial institutions to fulfil their due diligence obligations with regard to transactions carried out via the accounts concerned. This activity therefore does not present any evident money laundering risk.

3.5.3 VULNERABILITY OF INSTITUTIONS PURSUING THIS ACTIVITY

Since no inherent risk can be identified, the assessment of the vulnerability of these service providers is irrelevant.

3.5.4 OVERALL SCORE OF THE ACTIVITY

In view of the absence of risks and vulnerabilities, the overall score of account information services is zero.

3.5.5 TERRORIST FINANCING

It follows from the above that this activity does not give rise to any particular risk of terrorist financing.

3.6 ELECTRONIC MONEY

3.6.1 DESCRIPTION OF THE ACTIVITY

Electronic money is an electronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions as defined in Article 2(22) of the AML/CFT Act and which is accepted by a natural or legal person other than the electronic money issuer[24].

A number of differences can be identified in terms of the products offered as part of this activity, ranging from cards and electronic wallets used to make payments in a limited acceptance network such as one or more retail chains, to prepaid credit cards.

However, all electronic money activities require the user (or a third party) to load electronic money through cash deposits, subject to varying usage thresholds, onto a digital medium (hardware or software), and involve applications for carrying out any payments, generally including cash withdrawals.

The activity in Belgium

The number of payment and electronic money institutions subject to the NBB's AML/CFT supervision is decreasing. On 31 December 2022, there were twelve electronic money institutions subject to the NBB's supervision: five authorised electronic money institutions governed by Belgian law, one electronic money institution governed by the law of another EEA Member State with a branch registered in Belgium, and six electronic money institutions governed by the law of another EEA Member State operating in Belgium under the freedom to provide services through an agent and/or distributor.

The institutions subject to NBB supervision in the context of this activity issued around €350 million in electronic money in Belgium, and only one institution offered the option of having products credited/recharged by a third party.
As well as issuing electronic money, these institutions also offer payment services and are thus subject to the same risks as covered in point 3.1, including the risks associated with cash withdrawals and payments. In addition, electronic money products are increasingly digitalised and targeted at both private individuals and businesses.

The activity on the Belgian market is characterised by the fact that certain electronic money institutions have developed a business model in which they work with agents/distributors that carry out a different activity requiring payment and electronic money solutions. As these agents/distributors do not have the required authorisation to issue electronic money and offer payment services themselves, they ask the authorised electronic money institution to integrate payment and electronic money solutions into their business.

Insofar as the customers of the electronic money institution enter into a business relationship to be able to benefit from the services offered by the agent/distributor, the risks associated with these customers necessarily vary depending on the other activity carried on by the agent/distributor concerned.
The structure of this business model therefore requires the electronic money institution to pay particular attention to the risks associated with all the activities developed by each agent/distributor in the context of which the electronic money is distributed and the payment services are offered.

---

[24] Article 2(77) of the Act of 11 March 2018 on the legal status and supervision of payment institutions and electronic money institutions and access to the activity of payment services provider, to the activity of issuing electronic money and to payment systems.

3.6.2 RISKS INHERENT IN THE ACTIVITY

Electronic money activities are particularly exposed to the risk of customer characteristics not being adequately identified, whether as a result of anonymised products or the use of front men. This risk has been exacerbated by digitalisation, as the use of virtual money mules now makes it easier to carry out large-scale money laundering operations via electronic means; by using a large number of (real or fake) e-commerce websites, criminals can launder electronic money loaded with cash derived from illegal transactions.

Electronic money products remain subject to the transversal risk relating to cash, either because it is possible to load up the electronic money with cash, or because the product allows cash to be withdrawn from a vast network of terminals throughout the world. Criminals wanting to launder cash will continue to opt for products that make use of cash, that can be bought/reloaded with cash or that allow cash to be withdrawn in Belgium or elsewhere in the world. Moreover, compared to cash, electronic money has the additional characteristic of being dematerialised and therefore easier to transport and/or transfer to third parties.

However, it should be noted that, as soon as the statutory limits on anonymous use set at €150 are exceeded, the relative ease of tracing electronic money from its issuance to its distribution and use is a potential risk reduction factor that is absent in other payment activities involving the use of cash, which by definition cannot be traced.

Apart from the possibility of cash withdrawals and aside from the relatively small problem of anonymous products, the main risk of this activity is therefore that electronic money may be used simply as a medium for a larger-scale money laundering process.

The inherent risk of electronic money activities is therefore assessed as low by nature when it does not involve cash, but potentially higher given that these activities are often performed alongside other payment services that are more risky because of their nature and distribution method (score of 2.5 out of 5).

3.6.3 VULNERABILITIES OF INSTITUTIONS PURSUING THIS ACTIVITY

As stated in the European Commission's supranational ML/FT risk assessment of 27 October 2022, police forces have detected numerous cases of money laundering via prepaid cards, and the use of agents/distributors is sometimes preferred to front men, who are considered more expensive. Once again, this use of mules is made possible by digitalisation and the use of electronic devices.

As electronic money activities are generally offered via a network of physical agents, some of whom are not in themselves subject to the AML/CFT Act, supervision of the agent network becomes crucial. This supervision must be implemented as soon as agents are onboarded and then focus on the monitoring of their activities. Agent training must also be a point of attention.

However, other players in Belgium have developed systems to monitor electronic money from acquisition to use. These systems are assessed via continuous supervision and one-off thematic inspections designed to ensure, among other things, that the risk management measures are adequate to meet the challenges of money laundering. This dual supervision has not revealed any major anomalies in the operation of payment institutions as regards payment activities.

Continuous monitoring and recent inspections of payment institutions involved in issuing electronic money revealed the following vulnerabilities:

- unwillingness to establish a structure in Belgium that is independent of group entities located outside the EEA;
- lack of experience and relevant, ongoing AML/CFT training of management and/or staff;
- high turnover of AML/CFT staff and difficulties in recruiting staff with knowledge of the subject in Belgium;
- poor organisation of the three lines of defence in terms of AML/CFT: some outsourced functions are not sufficiently supervised or properly carried out;
- inadequate preventive framework (unsatisfactory automated procedures and monitoring tools);
- incomplete overall risk analysis taking no account of the risks presented by new products or specific geographical risks;
- the supervised entity's lack of expertise regarding certain products developed by its agents;
- knowledge of customers is based mainly on a posteriori analysis of their transactional activity;
- lack of in-depth knowledge of the Belgian statutory and regulatory AML/CFT framework and of the sanctions and embargoes regime;
- alerts are triggered primarily when thresholds are exceeded, without taking sufficient account of the customer's transactional behaviour;
- lack of analysis of the origin of customer funds;
- inadequate supervision of the agent network, either owing to a lack of personnel and/or material resources allocated to training and supervision, or because the institution's monitoring measures are inappropriate;

The vulnerabilities identified above do not apply to all institutions issuing electronic money, but to some that have a specific business model based on agents/distributors. As a result, overall, the vulnerabilities associated with this activity are assessed as significant (score of 3 out of 5).

3.6.4 OVERALL SCORE OF THE ACTIVITY

As stated in the EBA Guidelines of 1 March 2021 on ML/FT risk factors, "*the level of ML/TF risk associated with electronic money [...] (e-money) depends primarily on the features of individual e-money products and the degree to which e-money issuers use other persons to distribute and redeem e-money on their behalf*".

In view of the relevant considerations concerning the Belgian market, the residual risk of electronic money activities ranges from moderate to significant, depending primarily on the specific characteristics and terms of the products offered and on the characteristics and distribution methods of the institutions. The residual risk of this activity is assessed as moderate (score of 2.5 out of 5).

3.6.5 TERRORIST FINANCING

Inherent risk

Electronic money institutions can be attractive for terrorist financing due to the speed with which primarily international transactions are carried out, including to high-risk countries, and the difficulty for institutions to establish a customer profile based on anything other than transactional activity. The international nature and the speed with which accounts are opened and transactions are carried out, can make them attractive to criminals. This is especially the case with terrorist financing, as the amounts involved are smaller than for money laundering.

The inherent risk of terrorist financing risk with this activity is assessed as significant (score of 3 out of 5).

Vulnerabilities

The risk-based approach applied by these institutions is generally based on the volume and amount of their transactions. However, it was found between 2015 and 2018 that some terrorist attacks were financed by various small-value transactions.

This activity's vulnerability to terrorist financing is assessed as significant (score of 3 out of 5).

Residual risk

The residual risk of terrorist financing associated with this activity is assessed as significant (score of 3 out of 5).

4 CREDIT INSTITUTIONS

There are 30 credit institutions governed by Belgian law, 45 credit institutions governed by the law of another Member State of the European Economic Area with a branch registered in Belgium, and 5 branches of credit institutions governed by the law of a non-Member State of the EEA.

The Belgian market is characterised by the presence of several "universal" banks offering an extremely wide range of products and services to both private customers and businesses. Other credit institutions only offer more restricted and specialised services to a targeted customer base.

This assessment covers 9 types of activities that can be carried out by authorised credit institutions.

4.1 PRIVATE BANKING

4.1.1 DESCRIPTION OF THE ACTIVITY

Private banking activities are services provided by financial institutions in which they:

- on the one hand, hold assets and manage the wealth or economic resources of a customer in amounts exceeding a specific - generally high - threshold. In this respect, a distinction should be made between discretionary management, in which the bank is given a mandate to decide on portfolio management operations based on an investment objective and policy, and advisory management, in which the customer retains the power to decide on portfolio management operations;
- on the other hand, offer specific services, products and advice suited to the customer's specific profile.

Asset management includes but is not limited to the following products and services:

- banking services (holding accounts, lending, including Lombard facilities);
- investment services (investment advice, portfolio management);
- life insurance products;
- asset engineering, business transfer advice, etc.

The activity in Belgium

In Belgium, private banking is offered by specialised divisions of major universal banks (BNPPF, ING, KBC, Belfius, etc.), credit institutions governed by Belgian law specialising in this field (Banque Degroof Petercam, Delen Private Bank, etc.) and Belgian branches of institutions governed by the law of another EEA Member State (ABN Amro, Deutsche Bank, Puilaetco, Edmond de Rothschild,

etc.). It should be noted that this activity may also be pursued by stockbroking firms (Capitalatwork, Leleux, etc.), and that the points made in this chapter therefore also apply to them.

Private banking is a major activity in Belgium, with assets under management estimated at €454 billion in 2022.

4.1.2 RISKS INHERENT IN THE ACTIVITY

Private banking is a particularly risk-sensitive activity owing to the risk associated with managing substantial assets, the origin of which is sometimes difficult to establish, as well as to the discretion required by some very wealthy people and to the repatriation of funds in connection with fiscal transparency, which directives have made compulsory in the European Union in recent years.

In addition, the amounts involved are generally large, which makes it easy to conceal illicitly obtained funds among funds of legal origin, so that suspicions are less likely to be aroused.

This activity is also characterised by the provision of - sometimes aggressive - tax optimisation advice. This may involve setting up special “Cum/Cum” and “Cum/Ex” structures[25], which could entail reputational risks for the financial institutions involved.

Private banking is also associated with the following inherent product risks:

- the frequency and scale of cross-border movements;
- complex asset structures in countries with favourable tax regimes;
- the lack of transparency regarding the origin of funds and the difficulty, in some cases, of identifying the beneficial owners.

Once the origin of the funds has been established, the inherent risk declines dramatically, as the management operations are initiated by the financial institution itself pursuant to its mandate. The main due diligence efforts must therefore be deployed when the funds are received, and primarily focus on proving the funds’ origin and ensuring their consistency with the customer’s characteristics, including the extent and origin of the customer’s assets.

Other inherent risks relating to customers and products:

- customers with income and/or assets originating from high-risk economic sectors (arms, construction, gambling, mining, the diamond industry);
- customers against whom credible allegations of violations have been made;
- customers demanding an unusual degree of confidentiality or discretion, particularly in regard to the origin of the funds (see above);
- customers whose level of transactions does not correspond to their profile (particularly the size of their assets);
- very wealthy and influential customers;
- non-resident and PEP customers;
- requests for large amounts in cash or precious metals;
- financial arrangements involving countries or territories with a higher ML/FT risk;
- use of complex commercial structures e.g. trusts (although this appears to be fairly uncommon in Belgium);

---

25 “Cum/Cum” and “Cum/Ex” are schemes aimed at evading or wrongfully reclaiming the withholding tax on a financial instrument. In the case of Cum/Cum (dividend arbitrage), foreign investors in a domestic company who are not eligible for a dividend tax refund sell their shares to a domestic bank, which is eligible. After unlawfully collecting the refund from the tax authorities, the bank returns the dividends received to the investor in exchange for a commission. Cum/Ex involves shares being traded on a high-frequency basis around the time of dividend distribution between multiple global banking institutions, all of which declare themselves to be the owners of the shares in their country and the beneficiaries of the associated dividends. This enables each of them to claim dividend tax refunds, while the actual tax was paid only once.

- commercial activities pursued in multiple countries;
- cross-border arrangements, potentially involving uncooperative countries or territories;
- products favouring anonymity.

Given the above, the inherent risk of this activity is assessed as significant (score of 3.5 out of 5).

4.1.3 VULNERABILITIES OF INSTITUTIONS PURSUING THIS ACTIVITY

The following vulnerabilities were identified:

- the pursuit of commercial objectives and an inadequate AML/CFT monitoring culture, which may be due to the special links between relationship managers and their customers;
- the in-depth technical and regulatory AML/CFT and tax knowledge required to combat money laundering, whether or not connected with tax fraud;
- the allocation of insufficient resources to this task, as AML/CFT monitoring is often seen as costing money rather than making money, and as conflicting with commercial imperatives;
- problems relating to the exchange of information within groups where the same person is a customer of multiple entities in the same group (this sometimes seems to cause problems for certain third countries).
- difficulty in identifying the beneficial owners;
- difficulty in ascertaining the origin of funds, particularly in case of transactions in the context of the repatriation of funds organised by Belgian law (the DLU/EBA tax regularisation procedure);
- inadequate transaction monitoring.

Measures can be put in place to limit these risks, including:

- strengthening due diligence measures if the customer or the customer's beneficial owner is a PEP or is located in a high-risk country;
- implementing an AML/CFT policy at group level;
- strengthening due diligence measures for repatriations;
- the requirements arising from the European Markets in Financial Instruments Directive (MiFID), and in particular the rules relating to customer identification.

Given the above, the vulnerability associated with this activity is assessed as high (score of 4 out of 5).

4.1.4 OVERALL SCORE OF THE ACTIVITY

The activity's overall residual risk of money laundering is assessed as high (score of 4 out of 5).

4.1.5 TERRORIST FINANCING

Inherent risk

There does not appear to be a specific link between private banking and terrorist financing. Entry into private banking business relationships is subject to fairly strict conditions, particularly in terms of the amount of investment required, which makes it unattractive to those involved in terrorist financing. In addition, this activity does not allow for rapid transfers of the sums invested to other parties involved.

The inherent risk of terrorist financing associated with this activity is assessed as low (score of 1.5 out of 5).

Vulnerabilities

There are no specific vulnerabilities relating to terrorist financing other than those identified above.

This activity's vulnerability to terrorist financing is assessed as moderate (score of 2 out of 5).

Residual risk

The residual risk of terrorist financing associated with this activity is assessed as low (score of 1.5 out of 5).

4.2 RETAIL BANKING

4.2.1 DESCRIPTION OF THE ACTIVITY

Retail banks offer a wide range of services, such as current accounts and savings accounts, payment services (transfers, direct debits, bank cards, etc.) and loans (consumer loans, mortgage loans, etc.) for both private customers and small or medium-sized businesses.

The activity in Belgium

Retail banks have a strong presence in Belgium, be it in the form of banks governed by Belgian law or branches (mainly EEA) of banks governed by foreign law. They range from large universal banks to small and medium-sized institutions.

Competition is therefore very fierce, characterised by:

- margins under pressure in an environment where interest rates remained low for many years;
- an increase in digitalisation and a drastic reduction in the number of branches.

4.2.2 RISKS INHERENT IN THE ACTIVITY

Retail banking attracts a vast number of customers and covers a very large number of transactions (particularly payments) carried out for those customers, in highly variable amounts, which can make it difficult to identify potential money laundering transactions. This activity is also characterised by a wide range of customer profiles, including customers with particular risks associated with their profession. On the other hand, these transactions are executed in the context of - often long-standing - business relationships which means that, in principle, the bank has relatively detailed knowledge of its customers, including the origin of their funds, making it easier to detect atypical transactions. Also, the money laundering risk factors associated with retail transactions have long been relatively well known, which could likewise reduce the inherent risk associated with this activity.

In this context, retail banks are subject, in particular, to the risk associated with cash use (cash deposits/withdrawals) and, to a lesser extent, the risk associated with products favouring anonymity (although that risk is currently fairly low in Belgium, except in a few cases such as the repayment of loans by third parties that were not previously identified). The risk relating to digitalisation and its practical implications (e.g. remote identification) is also growing rapidly.
Other inherent risk factors associated with this activity include:

- the customer's professional activity;
- the accessibility and large range of bank accounts offered;
- the nature of the products and services offered, including cash withdrawals;
- the methods of funding accounts (problem of traceability of cash deposits);
- exposure to cross-border risk;

- use of new technologies for products which are not always properly mastered;
- opening a bank account using forged documents;
- fraud, through criminals' use of money mules to help layer the proceeds of the fraud.

The inherent risk of this activity is assessed as moderate (score of 2.5 out of 5).

4.2.3 VULNERABILITIES OF INSTITUTIONS PURSUING THIS ACTIVITY

The main vulnerabilities affecting retail banks are as follows:

- the allocation of insufficient resources, particularly in terms of IT and staff, to monitor what can be an extremely large flow of information (KYC) and transactions;
- the difficulty of obtaining an accurate view of the profile of customers who use various products and services;
- the difficulty of identifying beneficial owners of corporate customers and incorporating this information into the transaction monitoring system;
- the use of computerised systems that are insufficiently robust or, where appropriate, insufficiently interconnected to ensure that information flows correctly between the first two lines of defence and that the measures adopted (product restrictions, etc.) cannot be circumvented;
- the large volume of transactions to be monitored;
- the use of automated monitoring systems based on models and fundamentals which are not fully mastered (black box) or that are not sufficiently up to date to take account of changes in risks or new trends;
- IT procedures and systems that are insufficiently effective to ensure that customer information is properly stored and available;
- the potentially high number of atypical transactions;
- the implementation of mechanisms limiting the number of alerts to be processed by the AMLCO;
- the staffing of the compliance function with junior employees or persons lacking AML/CFT-related experience.

The vulnerability of retail banks is assessed as moderate (score of 2.5 out of 5).

4.2.4 OVERALL SCORE OF THE ACTIVITY

The activity's overall residual money laundering risk is assessed as moderate (score of 2.5 out of 5).

4.2.5 TERRORIST FINANCING

Inherent risk

The accessibility of bank and payment accounts to the vast majority of citizens exposes retail banks to the risk of terrorist financing. Funds may pass through an account before being used to finance a terrorist group or action, for example to finance terrorist actions on national territory or to finance the departure of fighters to conflict zones or neighbouring regions.

It is not easy for financial institutions to implement appropriate and sufficiently detailed scenarios in their monitoring systems to identify atypical transactions that could be linked to terrorist financing among the mass of daily transactions. Furthermore, to avoid attracting attention and being identified

by monitoring scenarios, the sums transferred generally remain below €1,000. As indicated by Europol, “smurfing”[26] remains a common practice.

It is imperative that the obligations associated with the sanctions regime be applied without fail. Controls carried out have revealed temporary deficiencies in the systems used to screen customers and counterparties against sanctions lists.

Current trends also show that a number of terrorist actions are financed through the income of the persons involved in these actions, in particular using their bank accounts. Traditional banking services (retail accounts) are therefore still a possible vector for terrorist financing, by enabling the use and transfer of the personal resources of terrorists or sympathisers of the cause.

Consumer credit that is not allocated to a specific expense may be at risk of being used for terrorist financing if it involves small amounts and if the sums can be withdrawn in cash.

The inherent risk of terrorist financing associated with this activity is assessed as high (score of 4 out of 5).

Vulnerabilities

In addition to the vulnerabilities mentioned above, it appears that the monitoring and identification of suspicious transactions is complicated by the fact that the transactions to be detected among an extremely large overall volume only involve small amounts. Remote onboarding, which is becoming increasingly widespread, can enable identity theft in certain cases.

This activity’s vulnerability to terrorist financing is assessed as high (score of 4 out of 5).

Residual risk

The residual risk of terrorist financing associated with this activity is assessed as high (score of 4 out of 5).

4.3 CORPORATE BANKING

4.3.1 DESCRIPTION OF THE ACTIVITY

Corporate banking refers to banking services offered to companies, such as:

- finance services (loans, liquidity credit/overdrafts, investment loans excluding leasing, factoring and mortgages, discounting, refinancing of invoices, assignments of trade receivables);
- payment services;
- custody services;
- savings services (savings accounts, deposit accounts) and investment services.

The activity in Belgium

Corporate banking services are provided mainly by two types of institutions in Belgium: large universal banks and around twenty subsidiaries or branches of foreign institutions, some of which are established in higher-risk countries, created to support the activities abroad (in Belgium or Europe) of their domestic businesses.

---

26 Transaction splitting.

Outsourcing may be used for associated functions such as IT or accounting. In the case of small establishments such as subsidiaries and branches where in-house capacity is insufficient, outsourcing may also extend to the internal audit and compliance functions. However, essential elements of activities for which an authorisation is required may not be outsourced under any circumstances.

4.3.2 RISKS INHERENT IN THE ACTIVITY

Corporate banking services are subject to the following inherent risks:

- in regard to business loans:
  - the involvement of a legal entity as debtor, which may make it possible to conceal the illicit origin of the funds used to repay the loan, and opens up the possibility for the transactions to be “steered” by the customer’s beneficial owners;
  - document fraud, which gives an inaccurate view of the company’s accounting situation and may thus facilitate criminal activity (bankruptcy fraud, misuse of company assets);
  - lending to businesses which are in a highly compromised position or subject to collective insolvency proceedings, or to "dormant" companies reactivated for criminal purposes;
  - refinancing of fake receivables: the institution purchases a receivable which does not correspond to any actual delivery of goods or services and pays the creditor, who receives funds from a financial institution.
    The latter institution is then paid by the debtor on the basis of the fake receivable, using funds of dubious origin which are thus laundered;
  - under- or over-invoicing, which enables the buyer and the seller to recover more than the value of the goods or services supplied; the extra value is passed on by the buyer to the seller in case of under-invoicing or by the seller to the buyer in case of over-invoicing (trade-based money laundering). Particularly sensitive sectors are construction and public works and import/export, whether or not relating to public contracts in emerging countries, as these sectors are at risk of predicate offences relating to corruption or unlawful acquisition of an interest;
  - the possibility of using funds of dubious origin to repay the loan, especially if the customer operates in sectors with a high money laundering risk where cash is heavily used;
  - excessive debt accumulation may be a means of fraudulently arranging bankruptcy. Where a firm acts as guarantor for a loan granted to another firm or to a natural person (entrepreneur), this may constitute misuse of company assets.
- In regard to leasing:
  - criminals can use leasing to acquire tangible movable assets of significant value (e.g. luxury cars) without having to purchase them and thus being required to justify the origin of the funds used for the purchase.

Given the above, the inherent risk of this activity is assessed as significant (score of 3 out of 5).

4.3.3 VULNERABILITIES OF INSTITUTIONS PURSUING THIS ACTIVITY

The Belgian market is characterised by the presence of large branches of institutions established inside or outside the EEA. It has been found, in certain cases, that these branches rely heavily on tools developed by the group - whose parent company is sometimes established in a country with a high ML/FT risk - and which do not necessarily take into account the specific characteristics of the activity carried out in Belgium. In addition, these tools must be sufficiently effective.

In some of these institutions, there has also been a high turnover of AML/CFT-related staff.

Furthermore, it was found that some institutions have difficulties in identifying the beneficial owners and incorporating this information in a useful way into the mechanisms for detecting and analysing atypical transactions.

The use of new technology and of remote (non face-to-face) commercial relationships are a vulnerability.

Actions taken by institutions:

- financial institutions operating in this sector are generally well aware of the risks associated with money laundering;
- fewer and fewer banks are targeting companies operating in sensitive sectors such as the diamond industry. In recent years, companies in the diamond industry have had to find a dedicated service provider, owing to a degree of de-risking;
- in general, financial institutions no longer offer services to businesses organised in the form of a trust.

The vulnerability to money laundering risks of institutions providing corporate banking services is assessed as moderate (score of 2 out of 5).

4.3.4 OVERALL SCORE OF THE ACTIVITY

The residual risk of money laundering associated with corporate banking is assessed as moderate (score of 2.5 out of 5).

4.3.5 TERRORIST FINANCING

Inherent risk

Given the sophisticated arrangements required, this activity's inherent risk of terrorist financing is fairly low. In addition, the activity generally involves large sums of money, which is not how terrorist organisations are currently financed. To date, there is no evidence that terrorist organisations have used this method of financing.

The inherent risk of terrorist financing associated with this activity is assessed as moderate (score of 2 out of 5).

Vulnerability

There are no specific vulnerabilities relating to terrorist financing other than those identified above.

This activity's vulnerability to terrorist financing is assessed as moderate (score of 2 out of 5).

Residual risk

The residual risk of terrorist financing associated with this activity is assessed as moderate (score of 2 out of 5).

4.4 TRADE FINANCE

4.4.1 DESCRIPTION OF THE ACTIVITY

Trade finance is a form of corporate banking that consists of a third party (a credit institution) acting as an intermediary in a trade transaction to organise payments and thus facilitate the movement of goods and the supply of services both domestically and internationally. The aim is to guarantee that the goods involved in the transaction will be both delivered and paid for.

Examples of trade finance activities include:

- open account transactions;
- letters of credit;
- documentary collection.

The activity in Belgium

The major universal banks governed by Belgian law are generally active in this sector. In addition, around twenty subsidiaries or branches of non-EEA institutions, some of which are established in countries with a higher risk profile, have been set up in Belgium to support the trade finance activities of these institutions in Belgium or the EEA

4.4.2 RISKS INHERENT IN THE ACTIVITY

The following inherent risks have been identified in connection with this activity:

- certain transactions may involve countries with a high risk of money laundering or terrorist financing, or countries where a large number of predicate offences are committed (counterfeiting, drug trafficking);
- trade finance operations can be used to repatriate funds acquired abroad in a seemingly legitimate manner, or to export assets of dubious origin. Under- or over-invoicing may be used to transfer funds of dubious origin from one country to another, to artificially increase the amount of refundable VAT or to reduce the amount due in customs duties. International trade finance operations may also be used to fund breaches of embargoes on goods or on the countries for which those goods are destined;
- multiple invoicing (the issuance of multiple invoices for the same transaction) may be used to provide an economic justification for transferring funds of dubious origin.

Given the above, the inherent risk of this activity is assessed as significant (score of 3 out of 5).

4.4.3 VULNERABILITIES OF INSTITUTIONS PURSUING THIS ACTIVITY

Credit institutions do not always have full access to information about the trade transaction and the parties to it. It is sometimes difficult for them to know precisely the actual activity carried out by (one of) the parties and to judge whether the transaction is consistent with the activities of the companies concerned. Another difficulty is that credit institutions must have sufficient expertise to judge the adequacy of the documents provided.

The vulnerability of institutions providing trade finance is assessed as significant (score of 3 out of 5).

4.4.4 OVERALL SCORE OF THE ACTIVITY

Trade finance is assessed to present a significant risk of money laundering (score of 3 out of 5).

4.4.5 TERRORIST FINANCING

Inherent risk

The risk of terrorist financing associated with this activity is fairly low given the sophistication of the structures and arrangements to be put in place and the knowledge required. In addition, the activity generally involves large sums of money, which is not how terrorist organisations are currently financed. To date, there is no evidence that terrorist organisations have used this method of financing.

The inherent risk of terrorist financing associated with this activity is assessed as moderate (score of 2 out of 5).

Vulnerability

There are no specific vulnerabilities relating to terrorist financing other than those identified above.

This activity's vulnerability to terrorist financing is assessed as moderate (score of 2 out of 5).

Residual risk

The residual risk of terrorist financing associated with this activity is assessed as moderate (score of 2 out of 5).

4.5 MANUAL CURRENCY EXCHANGE SERVICES

4.5.1 DESCRIPTION OF THE ACTIVITY

Manual foreign exchange services consist of accepting the immediate exchange of banknotes or coins denominated in different currencies, as well as the exchange of cash delivered to a customer, in exchange for payment by other means denominated in a different currency.

The activity in Belgium

Although this activity has fallen sharply following the introduction of the euro in 2002, it is still carried out by a large number of retail banks, stockbroking firms and payment institutions. Foreign exchange activity is most common in major Belgian cities, tourist towns and around the ports of Antwerp and Zeebrugge. Some financial institutions have signed contracts with shipping companies enabling foreign crews to be paid in euros.

4.5.2 RISKS INHERENT IN THE ACTIVITY

The risk of money laundering is particularly high with people wishing to exchange currencies whose origin is difficult to establish.

The main risks inherent in this activity are related to:

- the frequent use of cash ;
- the nature of the customer base, which is often made up of travelling communities such as immigrants, asylum seekers, border workers and tourists;
- the occasional nature of many transactions, which makes it difficult to build up accurate knowledge of the customer; customers may seek to convert funds into another currency to facilitate their conversion or transfer;
- the splitting up of foreign exchange transactions between different financial institutions to avoid attracting attention, sometimes by using different names or by using money mules to avoid the identification thresholds applied by the institutions. Where appropriate, transactions may be split between different institutions;
- customers with links to high-risk countries.

Given the above, the inherent risk of this activity is assessed as significant (score of 4 out of 5).

4.5.3 VULNERABILITIES OF INSTITUTIONS PURSUING THIS ACTIVITY

Financial institutions offering this service are exposed to the following vulnerabilities:

- lack of experience and relevant, ongoing AML/CFT training of management and/or staff;
- lack of knowledge of certain staff who are in direct contact with customers may limit the effectiveness of the identification and verification of the identity of the customer, and complicate the collection of information on the origin of the customer's funds;
- high turnover of AML/CFT staff and difficulties in recruiting staff with knowledge of the subject in Belgium;
- the origin of funds can be difficult to establish.

The materiality of these vulnerabilities may vary depending on the type and the (more or less developed) structure of the institution. Overall, the vulnerabilities associated with this activity are assessed as significant (score of 3 out of 5).

4.5.4 OVERALL SCORE OF THE ACTIVITY

Overall, manual foreign exchange services are assessed to present a significant risk of money laundering (score of 3.5 out of 5).

4.5.5 TERRORIST FINANCING

Inherent risk

Foreign exchange can be attractive for terrorist financing because it is based on the use of cash, facilitates the conversion and transfer of currencies and does not require any particular knowledge. One of the risks associated with this activity is the splitting up of foreign exchange transactions between different financial institutions to avoid attracting attention, sometimes by using different names or by using money mules to avoid exceeding the identification thresholds applied by the institutions.

The inherent risk of terrorist financing associated with this activity is assessed as high (score of 4 out of 5).

Vulnerability

There are no specific vulnerabilities relating to terrorist financing other than those identified above.

This activity's vulnerability to terrorist financing is assessed as significant (score of 3 out of 5).

Residual risk

The residual risk of terrorist financing associated with this activity is assessed as significant (score of 3.5 out of 5).

4.6 GUARANTEE AND PLEDGE SERVICES

4.6.1 DESCRIPTION OF THE ACTIVITY

Guarantees and pledges are two types of additional agreements that can be added to a principal obligation that a natural or legal person owes to a credit institution. Guarantees involve a third party (the guarantor) undertaking to fulfil an obligation to the creditor if the debtor fails to do so. Pledging is the assignment of one or more tangible or intangible assets, present or future, such as works of art, company shares, financial securities or life insurance or capitalisation contracts, as security for an obligation. An account can be pledged if it is a securities account.

4.6.2 RISKS INHERENT IN THE ACTIVITY

Pledging can be used in certain tax fraud schemes. An example is when a borrower pledges a life insurance policy to secure a real estate loan, fails to repay the loan and instead uses the pledged policy to repay it (Lombard loan scheme).

Guarantees offer the possibility of paying the guaranteed debt with funds from a third party, making it more difficult to trace the origin of the funds.

Given the above, the inherent risk of this activity is assessed as low (score of 1.5 out of 5).

4.6.3 VULNERABILITIES OF INSTITUTIONS PURSUING THIS ACTIVITY

Since the guarantor is not a customer of the financial institution, the institution has less knowledge of the guarantor and the guarantor's characteristics.

In addition, the origin of the funds can be difficult to establish.

The activity's vulnerability is assessed as low (score of 1.5 out of 5).

4.6.4 OVERALL SCORE OF THE ACTIVITY

The overall risk of money laundering associated with guarantee and pledge services is assessed as low (score of 1.5 out of 5).

4.6.5 TERRORIST FINANCING

It follows from the above that this activity does not give rise to any particular risks of terrorist financing, as the techniques used do not allow funds to be made available sufficiently quickly for a potential terrorist action. The risk of terrorist financing associated with this activity is assessed as low (score of 1.5 out of 5).

4.7 FACTORING

4.7.1 DESCRIPTION OF THE ACTIVITY

Factoring is a method of financing and collecting receivables offered mainly by credit institutions that allows suppliers to be paid in advance for their invoices, in order to benefit from cash flow before the contractual payment date. Factoring covers three types of service, which can all be provided separately or in combination:

- collection of receivables, including management of the open account (recording invoices, sending reminders to debtors in the event of late payment, etc.);
- cash flow financing, by advancing the amount of receivables as soon as they are transferred by the customer;
- credit insurance with a guarantee of payment of the receivable.

The activity in Belgium

The majority of banks active in the corporate sector offer services related to setting up and managing factoring operations.

4.7.2 RISKS INHERENT IN THE ACTIVITY

Factoring may be used to finance fake receivables. In this case, the institution purchases a receivable which does not correspond to any actual delivery of goods or services and pays the creditor, who receives funds from a financial institution. The latter institution is then paid by the debtor on the basis of the fake receivable, using funds of dubious origin which are thus laundered.

There is also a potential risk of over-invoicing, whereby the buyer and seller recover more than they actually paid for the goods or services provided, as the seller can pass on the over-invoiced amount to the buyer.

Given the above, the inherent risk of money laundering associated with this activity is assessed as moderate (score of 2 out of 5).

4.7.3 VULNERABILITIES OF INSTITUTIONS PURSUING THIS ACTIVITY

It can be difficult for credit institutions to verify whether a transaction is consistent with the activities of the companies concerned.

This activity's vulnerability is assessed as moderate (score of 2 out of 5).

4.7.4 OVERALL SCORE OF THE ACTIVITY

Factoring is assessed to present a moderate risk of money laundering (score of 2 out of 5).

4.7.5 TERRORIST FINANCING

It follows from the above that this activity does not give rise to any particular risks of terrorist financing, as the techniques used do not allow funds to be made available sufficiently quickly for a possible terrorist action. The risk of terrorist financing associated with this activity is assessed as low (score of 1.5 out of 5).

4.8 CORRESPONDENT BANKING

4.8.1 DESCRIPTION OF THE ACTIVITY

Correspondent banking is the provision of banking services by a bank acting as a correspondent bank for another bank which is its customer (the respondent bank), including the provision of a current account and associated services such as cash management, international remittances, foreign exchange services and relationships between and among credit institutions and financial institutions. The correspondent institution thus conducts transactions on behalf of third parties.

The activity in Belgium

In Belgium, correspondent banking is concentrated in a few major credit institutions.

4.8.2 RISKS INHERENT IN THE ACTIVITY

Correspondent banking is associated with the following inherent risks:

- if banking services are provided to shell banks[27] or banks which are not subject to adequate supervision, unregulated or inadequately regulated institutions can gain indirect access to the banking system. Such institutions established in off-shore areas thus present a particularly high ML/FT risk.
- since the correspondent bank provides the respondent bank with services consisting in the execution of transactions initiated by the latter's customers, the inherent risk of money laundering associated with correspondent banking is very greatly influenced by the quality and effectiveness of the AML mechanisms applied by the respondent bank and by the sectors in which its customers operate.
- the inherent risks of this activity are also greatly influenced by geographical risks if the respondent banks are based in countries or territories which have serious weaknesses in their AML legislation and/or the supervision of its effective implementation;
- the risks are even greater if the respondent bank uses the correspondent banking relationship not only to serve its own customers, but also to offer the same or similar correspondent services to various other banks based in the same country or even other countries ("netting"): in that case, the risks of money laundering incurred by the correspondent bank are greatly influenced by the quality of the AML mechanisms applied by those other respondent banks, and by any associated geographical risk;
- the services offered may include the opening of a payable-through account enabling customers of the respondent institution to carry out transactions directly on the account of the respondent institution.

[27] See Article 4(37) of the AML/CFT Act.

The inherent risks of money laundering associated with these activities are assessed as high (score of 4 out of 5).

4.8.3 VULNERABILITIES OF INSTITUTIONS PURSUING THIS ACTIVITY

It is difficult for financial institutions providing these services to obtain relevant and reliable information on the activities of the respondent institutions and the quality of their AML mechanisms. In addition, they have difficulty allocating sufficient staff with suitable knowledge and experience to conduct individual assessments of the risks associated with each respondent institution and to analyse its transactions. Correspondent banks also need to have specifically designed tools to conduct adequate monitoring of the respondent banks' transactions, taking account of each bank's profile.

Another vulnerability is that the respondent bank's account may be used by other respondent banks that have a direct relationship with the respondent institution but not with the correspondent bank (i.e. nesting or downstream clearing), so that the correspondent institution indirectly provides services to other banks that are not among its respondent institutions.

Conversely, it is noted that this type of financial services is only provided by major or specialised financial institutions that have substantial resources and are able to recruit specialist personnel.

The use of intermediaries in fund transfer execution chains can make it more difficult to detect payers or payees on international sanctions lists.

Correspondent banking with institutions established in third (non-EEA) countries presents greater intrinsic vulnerabilities, as the respondent institution in this case is subject to (regulatory and/or supervisory) AML/CFT requirements that differ from European requirements.

The vulnerability to money laundering risk of institutions engaged in this activity is assessed as moderate for cross-border correspondent banking within the EEA (score of 2.5 out of 5) and significant for cross-border correspondent banking outside the EEA (score of 3 out of 5).

4.8.4 OVERALL SCORE OF THE ACTIVITY

The residual risk of money laundering is assessed as significant (score of 3.5 out of 5).

4.8.5 TERRORIST FINANCING

Inherent risk

More specifically with regard to terrorist financing, cross-border correspondent banking may enable persons or entities whose funds are frozen to gain indirect access to the banking system through banks established in third countries (e.g. if the correspondent bank provides banking services to banks which have establishments in territories presenting FT risks).

Banks are therefore at risk of inadvertently transferring terrorist-related funds when they provide correspondent banking services to other foreign financial institutions. This can lead to the bank unwittingly processing transactions from foreign banks on behalf of complicit organisations or individuals. Examples of this are larger funds transfers made on behalf of Hezbollah or its financial supporters, or funds channelled through Iran to support terrorist proxies, regional militant groups or other nefarious activities.

It is important that the rules and measures relating to compliance with sanctions, asset freezes and embargoes be applied without fail, and that beneficial owners be identified.

The inherent risk of terrorist financing associated with this activity is assessed as high (score of 4 out of 5).

Vulnerability

In addition to the vulnerabilities mentioned above, it can be noted that the amounts of terrorist financing transactions in Belgium are generally small and may not be identified by the systems used to monitor correspondent banking transactions, which involve much larger amounts.

This activity's vulnerability to terrorist financing is assessed as significant (score of 3 out of 5).

Residual risk

The residual risk of terrorist financing associated with this activity is assessed as significant (score of 3.5 out of 5).

4.9 CLEARING AND SETTLEMENT/CUSTODY/CENTRAL SECURITIES DEPOSITORY ACTIVITIES

4.9.1 DESCRIPTION OF THE ACTIVITY

The purpose of clearing and settlement is to execute and settle sales and purchases of securities, wherever they occur, by transferring the securities from one account to another in exchange for payment of the price, thereby releasing the parties to the transaction from their respective obligations. These services are also used by large companies and institutions that are not subject to supervision.

Central securities depositories (CSDs) have a dual role:

- they act as a "notary", in the sense that they register securities at the time they are issued. To this end, they serve as a link between the companies that issue financial securities and deposit them with the CSD, and the financial intermediaries that hold these securities on behalf of investors (or for their own account); and
- they act as the manager of the securities settlement system, enabling securities to be exchanged between participants. They thus enable financial intermediaries to deliver financial securities against payment following their trading or sale.

The activity in Belgium

Custody and central securities depository activities are particularly significant in Belgium, being performed by two central and essential financial players.

In addition to settlement, these financial institutions offer other ancillary services linked to securities activities, such as:

- securities lending and borrowing: intraday loans that are always collateralised so that transactions can be settled on time;
- asset servicing and custody;
- investment fund-related services:
- collateral management;
- fund settlement services;
- money transfer services: very limited "bank account" services, enabling participants to deposit the proceeds of securities sales into their own accounts at (other) commercial banks.

4.9.2 RISKS INHERENT IN THE ACTIVITY

The inherent risks associated with clearing and settlement, custody and central securities depository activities are similar to the risks in correspondent banking if the customer is also a bank or financial institution subject to AML obligations (see above).

Although participants in a central securities depository also monitor their customers through their own AML/CFT systems, proprietary and third-party transactions are nevertheless a risk factor because of their potential complexity. In this respect, although all flows are traceable, the fact that they may be offset against other transactions can make it difficult to identify any suspicious behaviour. As a result, given the vast volume of instructions between participants, their possible offsetting and the variety of possible instructions, the central securities depository does not have a detailed view of the underlying strategies of the transactions passing through its system.

Institutions may be confronted with special mechanisms set up to evade tax. This is the case, for example, with “Cum/Ex” or “Cum/Cum” dividend arbitrage schemes, which involve evading or wrongfully reclaiming the withholding tax on a financial instrument. Several transactions are carried out around the dividend date to mislead the tax authorities of the countries involved[28].

The amounts of these transactions are particularly high, which increases the risk.

The inherent risks of these activities are assessed as moderate (score of 2.5 out of 5).

4.9.3 VULNERABILITIES OF INSTITUTIONS PURSUING THIS ACTIVITY

The entities carrying out this activity in Belgium are specialised and show clear expertise.

Another risk-mitigating factor is that participants in central securities depositories and institutions providing support to central securities depositories are themselves supervised entities that are subject to AML/CFT supervision and do not have natural persons as customers.

In addition, participants are subject to due diligence, which consists in verifying their compliance with admission criteria (including monitoring by an AML/CFT system) on the basis of mainly geographical risk criteria. The process of onboarding participants involves procedures for verifying their compliance with requirements regarding registration, authorisation, shareholders and directors, but also, depending on their articles of association, their compliance with AML regulations.

The vulnerability of institutions pursuing this activity is assessed as moderate (score of 2 out of 5).

4.9.4 OVERALL SCORE OF THE ACTIVITY

The residual risk of money laundering is assessed as moderate (score of 2 out of 5).

4.9.5 TERRORIST FINANCING

Inherent risk

This activity has relatively little direct exposure to the risk of terrorist financing. It is highly embedded into the financial ecosystem and only offers electronic exchange procedures requiring the use of standardised communication systems that are difficult to access (Swift). It is inaccessible to private

28 See the section on private banking.

individuals and difficult to access for legal entities with no significant long-term securities settlement activity. The high level of investment required to access settlement systems renders direct use of central securities depositories unsuitable for terrorist financing. However, it is still important that the rules and measures relating to compliance with sanctions, asset freezes and embargoes be applied without fail, and that beneficial owners be identified.

To date, there is no evidence that terrorist organisations have used this method of financing.

The inherent risk of terrorist financing associated with this activity is assessed as moderate (score of 2 out of 5).

Vulnerability

There are no specific vulnerabilities relating to terrorist financing other than those identified above.

This activity's vulnerability to terrorist financing is assessed as moderate (score of 2 out of 5).

Residual risk

The residual risk of terrorist financing associated with this activity is assessed as moderate (score of 2 out of 5).

5 INVESTMENT ADVICE (STOCKBROKING FIRMS)

5.1 DESCRIPTION OF THE ACTIVITY

For the purposes of this assessment, the two main activities of stockbroking firms are private banking (for this aspect, see the information included in point 4.1 regarding credit institutions engaging in this activity) and receiving/transmitting instructions. In this context, stockbroking firms are authorised to open securities accounts and cash accounts for their customers; the use of those accounts is subject to specific rules. It should be noted that the authorisation granted to stockbroking firms is a "modular" authorisation which also allows them to pursue other activities such as proprietary trading or underwriting. However, those activities are not covered in this assessment.

The activity in Belgium

This sector is trending towards consolidation and a reduction in the number of supervised institutions governed by Belgian law. This can mainly be explained by the critical mass of activity required for profitability, digitalisation, the ageing customer base and the difficulty of dealing with regulatory inflation.
At the end of 2022, the sector comprised 12 firms governed by Belgian law, 7 being family-owned and 5 belonging to a group.
It should also be noted that among the 5 companies belonging to a group, two stockbroking firms focus exclusively on asset management.
At the end of 2020, the amount of assets under management with these 12 Belgian stockbroking firms totalled €8.88 billion.
In addition, there are 10 branches of stockbroking firms governed by the law of another EEA Member State.

5.2 RISKS INHERENT IN THE ACTIVITY

The inherent risks associated with the activities of receiving and executing instructions are as follows:

- unusually large transactions;
- investments with no obvious economic purpose, e.g.:
  - the customer requests the repurchase or redemption of a long-term investment after a short time and without any clear justification, thereby incurring a financial loss;
  - the customer transfers more funds than necessary for the investment and requests repayment of the excess amount;
  - the customer is reluctant to supply information in the context of legitimate due diligence measures;
- the nature of the customer (unregulated investment vehicle, PEP, etc.);
- the customer's activities (e.g. if the funds originate from sectors of activity associated with a high risk of financial crime);
- geographical risk (the investor or depositor is based in a high-risk country or territory, or the funds originate from such a country or territory);
- insufficient knowledge of the origin of the funds.

The level of vulnerability can vary according to the nature of the product (listed/unlisted, simple/complex, products traded on the less regulated over-the-counter market, etc.).

Based on the above, the level of inherent risk is assessed to range between moderate for receiving/transmitting instructions (score of 2 out of 5) and significant for private banking (score of 3.5 out of 5).

5.3 VULNERABILITIES OF INSTITUTIONS PURSUING THIS ACTIVITY

The following vulnerabilities can be highlighted with regard to this activity:

- the absence of adequate monitoring. For instance, stockbroking firms are only allowed to open cash accounts for private individuals if the accounts are to be used to receive either funds awaiting investment or funds resulting from the sale of financial instruments. Such accounts are therefore not intended for carrying out ordinary payments. Consequently, they are at risk of being used to carry out suspicious or abnormal transactions, without any adequate monitoring capable of identifying them as such;
- FinTech/RegTech development is creating new risks relating to e.g. non face-to-face identification, outsourcing of due diligence checks and reliance on third-party service providers;
- experience has shown that some stockbroking firms underestimate the money laundering risk associated with their activity, and therefore do not have the human and/or technical resources required to address this risk, nor the necessary expertise, and that they do not devote the necessary resources to training their personnel.

The vulnerability can be assessed as moderate for the activity of receiving/transmitting instructions (score of 2 out of 5), and as high for the private banking aspect (4 out of 5).

5.4 OVERALL SCORE OF THE ACTIVITY

The residual risk of money laundering is assessed as moderate for the activity of receiving/transmitting instructions (score of 2 out of 5), and as high for private banking (4 out of 5).

5.5 TERRORIST FINANCING

Inherent risk

There does not appear to be a link between the activities of stockbroking firms and terrorist financing. Entry into a business relationship is subject to fairly strict conditions, but unlike private banking, the amounts of investment requested are lower. The activity does not lend itself to anonymous transactions or to the direct and rapid transfer of sums invested to other persons involved.

The inherent risk of terrorist financing associated with this activity is assessed as low (score of 1.5 out of 5).

Vulnerabilities

There are no specific vulnerabilities relating to terrorist financing other than those identified above.

This activity's vulnerability to terrorist financing is assessed as significant (score of 3 out of 5).

Residual risk

The residual risk of terrorist financing associated with this activity is assessed as moderate (score of 2 out of 5).

6 LIFE INSURANCE

6.1 DESCRIPTION OF THE ACTIVITY

Life insurance products are products designed to protect the beneficiary against the risk of occurrence of a future event relating to the length of human life.

Life insurance activity consists in selling life insurance products for individuals (e.g. savings insurance and investment insurance) and for groups (pension insurance).

The various life insurance products are divided into classes (from 21 to 29) according to their characteristics and the associated risk.

21. Life insurance not linked to investment funds, excluding marriage insurance and birth insurance.
22. Marriage insurance and birth insurance not linked to investment funds.
23. Life insurance, marriage insurance and birth insurance linked to investment funds.
24. Permanent health insurance (long-term non-cancellable health insurance available in Ireland and the United Kingdom).
25. Tontines.
26. Capitalisation operations.
27. Management of group pension funds.
28. The operations referred to in Book IV, Title IV, Chapter I of the French Insurance Code.

29. Operations related to the length of human life, as defined or provided for by social insurance legislation, when practised or managed in compliance with a Member State's legislation by insurance companies at their own risk.

In addition to differentiating the type of risk, the division of life insurance products into classes also makes it possible to distinguish aspects relating to possible tax benefits, premium taxes and withholding taxes.

The activity in Belgium

As of 2022, the Belgian life insurance sector comprises 34 approved or authorised companies (compared to 40 in 2020). This number can be broken down into 25 approved or authorised insurance companies governed by Belgian law (compared to 29 in 2020) and 9 branches of EEA companies (11 in 2020).
Over 50% of institutions active in life insurance form part of a bancassurance group.

The fifteen largest insurance groups together represented 97% of total premium income in 2022.

While individual guaranteed rate life insurance (class 21) and group insurance remain the most popular products, classes 26 and 23 have seen an increase in premium income in recent years.

6.2 RISKS INHERENT IN THE ACTIVITY

FinTech/RegTech development is liable to create additional risks relating to remote identification or the use of outsourcing for AML.

The following risk factors can be highlighted for this activity:

- The beneficiary of the policy is not necessarily the policyholder. Consequently, the insurance company may have less information about the former.
- payment flexibility (payments originating from unidentified third parties, high or unlimited premiums, etc.);
- product tradability;
- product anonymity;
- the nature of the customer (PEP, active in a sector that uses substantial amounts of cash or is exposed to the risk of corruption, etc.);
- the customer's behaviour (the customer transfers the contract to a third party with no apparent link, or incurs high costs by requesting early cancellation of a product, or pays in cash, etc.).

Insurance companies operating in Belgium no longer allow premiums to be paid in cash, which somewhat limits the risk of money laundering.

Long-term life insurance

Most traditional life insurance products (i.e. excluding investment products) are designed for the long term, and many of them are not flexible enough to be attractive to money launderers. Moreover, the costs of early redemption and contract cancellation make the money laundering process expensive if it is executed in the short term. In addition, early redemptions and contract cancellations are easily identifiable by insurance companies. However, the risk that funds used to purchase life insurance may be derived from a criminal activity cannot be ruled out, especially in the case of contracts with large single premiums.

The risks associated with the activity ultimately depend on the type of life insurance.

For instance, pension insurance, which is widely used in Belgium, is regarded as presenting a significantly lower risk of money laundering if the premiums are low and the model is based on a fixed and limited contribution. Group insurance is also considered less risky if the volume of premium payments is likewise limited and premiums are deducted from remuneration and reserved exclusively for the employer and the employee. The way in which the capital is built up and the terms of payment or redemption of group insurance (on retirement or as an advance against the purchase of real estate) mean that this type of insurance is not attractive in terms of money laundering and terrorist financing.

Insurance products as investment instruments

Conversely, life insurance policies consisting of capitalisation contracts (class 26) present a higher inherent risk, as they enable the short-term investment of money derived from a criminal activity, e.g. tax evasion (repatriation of funds/undeclared donations).
Class 23 insurance, which is linked to investment funds, may also present a higher risk. This is an investment product which differs from the traditional class 21 life insurance and which has a favourable tax profile compared to more conventional bank investments. It also offers the possibility of tax-free withdrawals on the policy. In recent years, class 23 insurance has seen very strong growth, often to the detriment of class 21 where guaranteed yields have fallen sharply owing to the general decline in interest rates. Class 23 products permit indirect investment in the financial markets.

Other inherent risks are as follows:

- the origin of the funds, e.g. if they were repatriated from abroad;
- being flexible, class 23 savings products may be used to set up complex structures concealing the identity of the beneficiary;
- possibility of withdrawing funds invested in class 23 with no tax impact .

Consequently, the inherent risk of life insurance activity in Belgium is assessed as moderate in the case of traditional life insurance (score of 2 out of 5) and significant for life insurance as an investment instrument (3 out of 5).

6.3 VULNERABILITIES OF INSTITUTIONS PURSUING THIS ACTIVITY

In general, it is apparent that insurance companies – in principle less likely than other financial institutions to face the risk of money laundering – have neglected this issue to some extent, both as regards the human and material resources devoted to it, and as regards their in-house expertise (particularly by not providing suitable training).

There are two key moments in an insurance contract when it comes to preventing money laundering: the conclusion of the contract and the payment of the benefit. It is at these two moments that essential information about the customer and the beneficiary or beneficiaries is collected. It is more difficult for an insurance company than a credit institution to build up genuine knowledge of the customer. A new sector code developed by the trade association Assuralia in 2019 and updated in 2021 seems to have helped increase understanding within the sector and achieve a better level of compliance with AML/CFT regulations. In particular, the majority of insurance companies operating in Belgium have changed their approach from one based on the individual contracts taken out to one based on the customer, which provides a holistic view of the customer's portfolio.

Life insurance products necessitate monitoring actions that require the company's full attention at the entry into the relationship and at the time of pay-out, as well as in case of surrender or pledging. Between these moments, monitoring is generally less strict (provided there are no changes (identity of the person paying into the contract, higher premium, etc.).

The use of third parties for marketing insurance products and for identifying customers and business relationships as well as for storing the relevant AML data could constitute a vulnerability for insurers if the procedures are not appropriate and adequate checks are not carried out.

However, it should be noted that insurance intermediaries (tied or non-tied agents, brokers) are subject to AML/CFT supervision by the FSMA in Belgium.

Traditional life insurance

Traditional life insurance products are less widely distributed than other financial services, which could make them less attractive to criminals.

On the subject of money laundering risks in financial intermediation, reference is made to the work of the FSMA, and in particular its findings following a number of inspections of insurance intermediaries[29].

Institutions offering life insurance activities are also relatively less exposed to possible clandestine/unregistered transactions; since they have to collect a great deal of information on the customer, the knowledge they can obtain is qualitatively better.

In the light of the above, the vulnerabilities of insurance companies are assessed as low to moderate (score of 1.5 out of 5) in the case of traditional life insurance.

Life insurance as an investment product

Life insurance policies as investment products are subject to the general vulnerabilities set out above. The lack of adequate resources and expertise in terms of AML may be particularly harmful for a fairly flexible product such as class 23 insurance.

Although the risk is still relatively low, the vulnerability in that respect is nevertheless assessed as moderate to significant (score of 2.5 out of 5).

6.4 OVERALL SCORE OF THE ACTIVITY

The residual risk of money laundering is assessed as low for traditional life insurance (score of 1.5 out of 5) and as moderate for life insurance as an investment product (score of 2.5 out of 5).

6.5 TERRORIST FINANCING

It follows from the above that this activity does not give rise to any particular risks of terrorist financing, as the techniques used do not allow funds to be made available sufficiently quickly for a possible terrorist action. The risk of terrorist financing associated with this activity is assessed as low (score of 1.5 out of 5).

29 https://www.fsma.be/sites/default/files/legacy/content/FR/Blanchiment/2020-05-26_rapporttpc.pdf

7 SCORE SUMMARY:

Overview of risks related to money laundering

	Inherent risk	/5	Vulnerabilities	/5	Residual risk	/5
Payment activities	High	4	High	4	High	4
Money remittance	High	4.5	High	4	High	4.5
Acquiring activities	Moderate	2	Moderate	2	Moderate	2
Payment initiation services	Low	1.5	Moderate	2.5	Moderate	2
Account information services	Zero	0	Zero	0	Zero	0
Electronic money activities	Moderate	2.5	Significant	3	Moderate	2.5
Private banking	Significant	3.5	High	4	High	4
Retail banking	Moderate	2.5	Moderate	2.5	Moderate	2.5
Corporate banking	Significant	3	Moderate	2	Moderate	2.5
Trade finance	Significant	3	Significant	3	Significant	3
Manual exchange services	High	4	Significant	3	Significant	3.5
Guarantee and pledge services	Low	1.5	Low	1.5	Low	1.5
Factoring	Moderate	2	Moderate	2	Moderate	2
Correspondent banking	High	4	Significant	3	Significant	3.5
Clearing/Custody/Central securities depository activities	Moderate	2.5	Moderate	2	Moderate	2
Investment advice (private banking)	Significant	3.5	High	4	High	4
Investment advice (no funds held)	Moderate	2	Moderate	2	Moderate	2
Life insurance	Moderate	2	Low	1.5	Low	1.5
Life insurance (investment products)	Significant	3	Moderate	2.5	Moderate	2.5

Overview of risks related to terrorist financing

	Inherent risk	/5	Vulnerabilities	/5	Residual risk	/5
Payment activities	High	4	High	4	High	4
Money remittance	High	4	High	4	High	4
Acquiring activities	Low	1.5	Low	1.5	Low	1.5
Payment initiation services	Low	1.5	Low	1.5	Low	1.5
Account information services	Zero	0	Zero	0	Zero	0
Electronic money activities	Significant	3	Significant	3	Significant	3
Private banking	Low	1.5	Moderate	2	Low	1.5
Retail banking	High	4	High	4	High	4
Corporate banking	Moderate	2	Moderate	2	Moderate	2
Trade finance	Moderate	2	Moderate	2	Moderate	2
Manual exchange services	High	4	Significant	3	Significant	3.5
Guarantee and pledge services	Low	1.5	Low	1.5	Low	1.5
Factoring	Low	1.5	Low	1.5	Low	1.5
Correspondent banking	High	4	Significant	3	Significant	3.5
Clearing/Custody/Central securities depository activities	Moderate	2	Moderate	2	Moderate	2

Investment advice (private banking)	Low	1.5	Significant	3	Moderate	2
Investment advice (no funds held)	Low	1.5	Significant	3	Moderate	2
Life insurance	Low	1.5	Low	1.5	Low	1.5
Life insurance (investment products)	Low	1.5	Low	1.5	Low	1.5