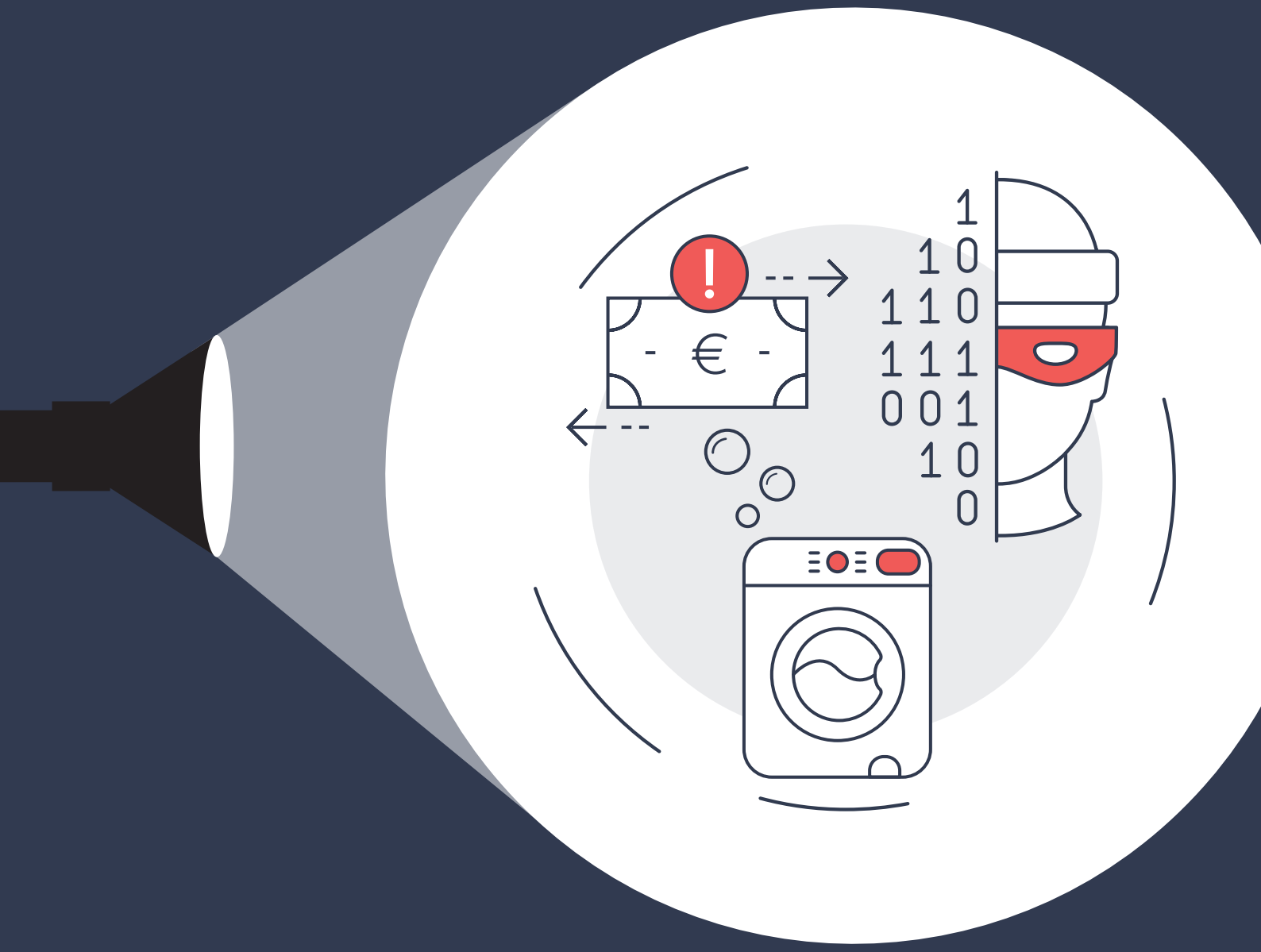
Banks: gatekeepers in the fight against money laundering



febelfin

Banks assume responsibility for detecting fraudulent practices

Money circulates. It keeps the economy going. Banks play a crucial role in this regard as they facilitate financial transactions and payments.
But there is also a downside to money: sometimes it is used to fund criminal activities such as terrorism. Or money from criminal circles is laundered by repeatedly transferring it to other accounts. After a while, criminal money appears to be completely clean or legal.

The fight against money laundering and the financing of terrorism remains challenging, and banks play a key role today in detecting financial fraud.

You can read about the efforts that banks put in as gatekeeper in the fight against money laundering and the financing of terrorism in this brochure.

COMPLYING WITH AND MONITORING LEGISLATION

Banks are subject to anti-money laundering legislation and play a leading role in detecting financial crime. Belgian legislation is based on **European** directives (EU AMLD) and **international standards** (FATF/GAFI), which have been framed **even more strictly in recent years** (cf. AML III, IV, V, VI, and so on). More specifically, this means:

- That the scope of application has been extended and more institutions must comply with obligations
- Even higher penalties have been set (up to 10% of the institution's annual turnover) for non-compliance with regulations
- A risk-based – as opposed to a 'tick the box' – approach has been chosen but for individual risk assessments (i.e. no standardisation possible)
- More inspections by supervisory authorities
- Risk of damage to an institution's image every time a scandal emerges

The **role as gatekeeper in the fight against money laundering does not stop with checking the client's ID card in advance.** It requires a **continuous duty of vigilance** throughout the business relationship with **numerous obligations**:

- Know your customer 'KYC'
- Know your transaction 'KYT'
- Checking the origin of assets
- Risk-based approach
- Complying with financial embargoes
- Restricting the use of cash
- Obligation to report suspected money laundering to the Financial Information Processing Unit (CFI)
- Obligation to report to Schatkist (embargoes)
- and so on

Know your customer

The fight against money laundering significantly affects the **relationship between the bank and the client**. A client who wants to open an account with a bank must first identify themselves. Because of the goodwill of the client who agrees to disclose their identity and other data, the bank can correctly assess the client relationship and take any appropriate measures to combat financial crime. To explain how everything works, Febelfin has produced the brochure **'Waarom vraagt mijn bank mijn identiteitsgegevens?'** (Why does the bank want my identity data?) that banks can use to inform their clients why they are requesting these data and what these data are used for.

Among other things, the brochure deals with the information and documentation that the bank must collect before it can offer financial services. More specifically, this means:

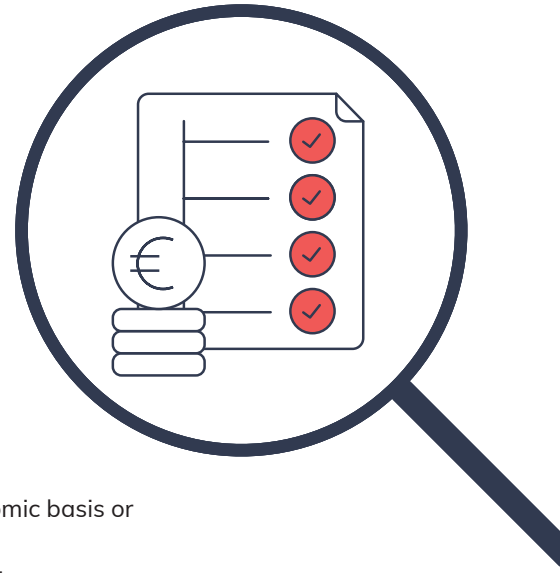
- There is a need to identify and verify by means of supporting documents
- For **natural persons,** this involves:
  - Verifying data (first name, surname, place of birth, date of birth, and so on) by reading the electronic identity card (natural persons with Belgian nationality) or passport (natural persons with another nationality)
  - Investigating whether a person has a 'specific risk-increasing status' (e.g. Politically Exposed Persons)
- Specific information is required for **legal entities**, such as:
  - Updated articles of association
  - Clarity about the identity of the directors, the Ultimate Beneficial Owners (UBOs)
  - Provisions on the power to bind a legal entity
  - Clearly identifying the actions of mandataries (i.e. holders of powers of attorney, agents)

This process must be repeated periodically (i.e. continuous vigilance). This means that banks must repeatedly follow up on various issues:

- New address?
- New articles of association?
- New UBOs? => The company must identify its UBOs in the UBO register and inform the bank.
  More information: **What you need to know about the UBO register | Febelfin**
- Bank repeats the exercise to assess whether it affects the risk profile and the measures it must adopt
- and so on

The above list is not exhaustive and is subject to strict legislation and recommendations by the National Bank of Belgium (NBB).

Know your transaction



Banks must always consider whether a transaction is compatible with the client's characteristics and with the purpose and nature of the relationship. They have to detect 'atypical' transactions, for example, based on its objective characteristics or based on the client's characteristics, including:

- abnormally complex transactions
- transactions for an unusually high amount
- intrinsically unusual transactions with no apparent economic basis or legitimacy
- transactions that seem inconsistent with the client's profile

Risk-based approach

Banks must focus their AML efforts and resources on limiting the risk of being misused for money laundering or the financing of terrorism. This risk-based approach must allow financial institutions to take less far-reaching measures in situations in which the risks are low and to use the resources freed up by this to apply more stringent measures to situations in which the risks are higher.

If a bank finds there are certain AML risk-increasing factors, it must:

- Obtain further information to verify information
- Pay increased attention and monitor transactions
- Update data faster
- And obviously report the suspicion of money laundering to CFI and end the relationship, if necessary

Banks must always be able to apply a fully risk-based approach **under the Belgian Anti-Money Laundering Act**. This means that they must be able to **analyse and mitigate** the **risk of money laundering** associated with **each individual client**. To give an idea of the work involved: in 2019, this involved following-up around **18,787,773 clients**[1], of which 94.3% were natural persons and 5.7% were legal entities.

Reporting suspicious transactions

The above procedures allow banks to optimally fulfil their **legal role** in the fight against money laundering and to **report suspicious transactions or facts** to the Financial Intelligence Processing Unit (CFI). These transactions and facts can thus be more thoroughly investigated and, if necessary, brought to the attention of the public prosecutor's office. **CFI's** figures show that **banks** are **one of the main players** in the fight against money laundering.

In 2020, credit institutions reported 17,678 **suspicious transactions to the CFI** and initiated **55%** (an increase of 12% compared to 2019)[2] of the money laundering cases that the CFI forwarded to the judicial authorities. The amount involved was €1.9 billion[2].

Compliance with all obligations, including the obligation to report suspicious transactions to the CFI, and legislation not only requires extensive investment in monitoring and investigative procedures, strengthening internal organisations (staff training, additional recruitment and so on), but also extensive cooperation between banks and with other organisations and the authorities.

[1] Febelfin survey conducted in 2020 with data relating to the situation on 31/12/2019 at 18 banks, including the four major banks.

[2] Source: CFI Annual Report 2020: jv2020.pdf (ctif-cfi.be)

INVESTING IN MONITORING AND INVESTIGATIVE PROCEDURES

Protecting society against money laundering and the financing of terrorism is an absolute priority for Belgian banks.
In recent years, banks have **invested** more in their **monitoring and detection procedures**:[1]

- Belgian banks **invested more than €93 million in their AML compliance departments** in **2019**.
- Banks are also investing heavily in **tools to automate onboarding, screenings and transaction monitoring**. For example, 95% of periodic name screenings are already automatic.

STRENGTHENING THE INTERNAL ORGANISATION

Banks have also **strengthened their internal organisation** to intensify the fight against money laundering practices and assume their responsibility as **gatekeepers** more than ever:

- It is estimated that more than **1,600 bank employees** in Belgium are involved in the fight against money laundering **on a daily basis**. But this goes much further in practice, with each bank employee having to pay continuous attention to this issue. **The above shows that not only compliance departments but also all departments in the bank, and primarily employees who come into contact with the client, follow up the fight against money laundering.**
- **61% of banks plan additional investments in 2021** to recruit **more staff** for the purpose of the fight against money laundering and the financing of terrorism.
- **Almost every financial institution (94.4%)** organises **specific in-service AML training for its employees**. This can range from e-learning to traditional classroom training or self-study. In 2019, **44,000 bank employees** (or 89% of all bank employees in Belgium) had already **attended at least one specific AML training course**.

[1] Febelfin survey conducted in 2020 with data relating to the situation on 31/12/2019 at 18 banks, including the four major banks.

Banks: the crucial link in a bigger picture

Banks are clearly a fundamental link in preventing and detecting money laundering. But they are only part of a bigger picture. The fight against money laundering would benefit from more options for exchanging information, not only between financial institutions themselves, but also with other public bodies.

COOPERATION BETWEEN BANKS

Banks exchange expertise and know-how about Know Your Customer (KYC) utilities. This not only leads to further administrative simplification for both the client and the bank, but also strengthens the quality of the 'KYC' data and encourages banks to use new technologies (such as blockchain) to automate and digitise processes.

Febelfin thus follows up various projects to optimise its KYC (know-your-customer) services, particularly identifying companies and private individuals. For this purpose, Febelfin supports the Isabel Group in developing the Kube system, which allows companies to identify themselves through a system using blockchain technology to verify user identities. Clients of financial institutions can be identified easier, faster and more accurately through this system. The Febelfin survey[1] showed that most financial institutions are very positive about using data-sharing utilities (such as Kube or Itsme).

But **banks are not always allowed to share information about suspicious transactions or clients with other banks**. A **legal framework is needed to facilitate the safe and legal sharing of data and information**.

[1] Febelfin survey conducted in 2020 with data relating to the situation on 31/12/2019 at 18 banks, including the four major banks.

CONSULTATION BETWEEN BANKS AND GOVERNMENT AGENCIES

In 2020, following the 'FinCEN Files', Febelfin recommended closer consultation between the financial sector and public authorities (government, NBB, anti-money laundering unit, judicial authorities, FSMA, and so on) to **efficiently exchange information** and **jointly intensify the fight against money laundering**.

Although individual **banks provide information to the government and the anti-money laundering unit** today, it often stops there. They can exchange information among themselves only to a very limited extent and receive little feedback. Febelfin therefore argues for **more cooperation between the financial sector and public authorities** (government, anti-money laundering unit, judicial authorities, and so on) to exchange information securely, increase efficiency, and join forces in the fight against fraud and money laundering.

> "Let banks and governments exchange information about suspicious transactions with each other through a secure environment so they can be more responsive and avoid money laundering."
>
> – Karel Baert

Such forms of cooperation between all stakeholders involved have already started in other **European countries**, such as the Netherlands and the United Kingdom. Banks are fervent supporters of establishing such a platform in Belgium as well.

The government has now heard this plea and such a Private-Public Partnership is being set up based on examples from neighbouring countries. A cooperation protocol has been drawn up to establish and shape this consultation platform. The partners in this project are CFI, NBB, the Finance Office, MinFin (Treasury), Assuralia, FSMA and the banking sector represented by Febelfin. The objectives of the platform are:

- Exchanging information and expertise on established AML developments, trends, emerging risks, mechanisms and types
- Discussing AML/CFTP topics relevant to the various participants

- Proposing guidelines and providing feedback on applying the statutory AML/CFTP obligations, particularly on detecting and reporting suspicious transactions.
- Preparing opinions or proposing initiatives to promote AML/CFTP to the policymakers.
- Examining data-sharing options, case-specific or otherwise, within the framework of AML/CFTP, considering the statutory provisions on professional secrecy and processing of personal data, and, if necessary, proposing legal and technological solutions for exchanging these data digitally

This partnership will undoubtedly contribute towards a **legal framework for sharing data and information securely and legally**.

AML stakeholders in Belgium:

EUROPEAN SECTION

The sector also closely follows the work of the **European Union** in this regard. Europe is namely reforming the rules to combat money laundering practices and wants to develop a **single rulebook** to **harmonise the rules across the Union, for example by working with directly applicable regulations**. Harmonisation will ensure a more **uniform application of the rules and make anti-money laundering legislation more efficient**. European legislative proposals are also expected to evolve towards a European anti-money laundering supervisory authority.

Febelfin has worked on several recommendations for an effective European anti-money laundering policy with the European Banking Federation (EBF):

- One European Regulation instead of Directives (more binding)
- Limiting the discretionary powers of the Member States
- A global level playing field in the fight against money laundering
- Stronger role for the **European Banking Authority (EBA)** in regulation
- Harmonising supervision (cross-border coordination); this also applies to the work of the Financial Intelligence Units
- More information-sharing, within privacy boundaries, between banks and public-private bodies
- Transparent and careful UBO registration

We can expect the first proposals from the European Commission in the coming weeks, and these will be closely monitored.

Trends in money laundering and the financing of terrorism[2]

The practice of money laundering is in constant flux. If one modus operandi is thwarted, perpetrators find another creative way of disguising the criminal origin of assets and resources. It remains a real cat-and-mouse game.

While the COVID-19 crisis slowed down the economy, it unfortunately did not have the same effect on fraudsters and their activities. On the contrary, several new fraud trends were identified during this period, capitalising cleverly on current events and bringing additional challenges to the banking sector in the fight against money laundering and the financing of terrorism.

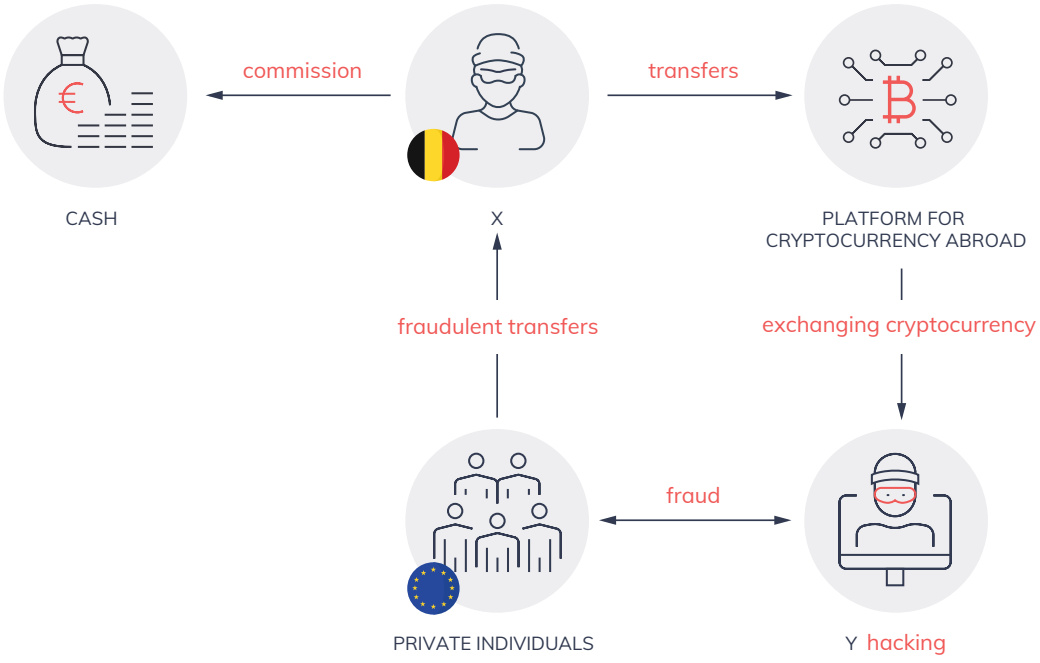
[2] Source: CFI Annual Report 2020: jv2020.pdf (ctif-cfi.be)

For example, the number of **phishing emails** in which cybercriminals ask you, ostensibly on behalf of a financial institution or other authorities, to update your card's security details – under the pretext of the exceptional times we are living in – has increased dramatically and the 'fish pond' of potential victims has expanded.

Febelfin statistics show that around **67,000 fraudulent transactions occurred through phishing** in 2020, totalling a net amount of roughly **€34 million**.
Alarmingly, **more and more money mules** are being used to quickly and easily channel money obtained by criminal means from one account to another.

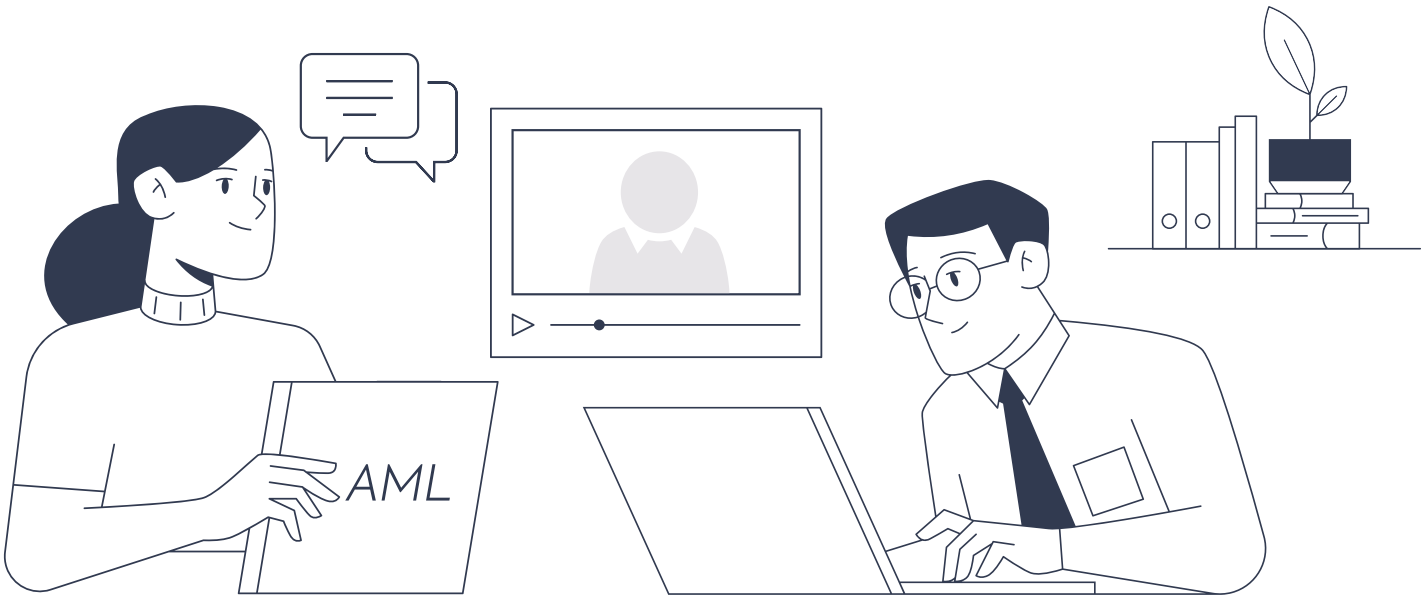
It is not yet possible for banks to exchange personal data about fraud because of privacy and other legislation. Banks remain very cautious in this area because they are bound by extremely strict regulations through supervisory authorities and legislation. Febelfin is investigating the possibility of establishing a system for exchanging the identity data of money mules between financial institutions on a statutory basis.

Investment fraud (online advertising of false forms of investment) and **cryptocurrency fraud** are also on the increase. Most fraud reports involving investments are about **boiler rooms, recovery rooms and binary options**. **Money mules** also play a major role in cryptocurrency fraud. They receive money obtained by criminal means in their bank account with which they must purchase cryptocurrency. The illustration below shows how it all works.



Example of how money mules and money laundering with cryptocurrencies work: source CFI

A SELECTION OF THE TRAINING COURSES OFFERED BY FEBELFIN ACADEMY



Febelfin Academy offers a wide range of basic, advanced and expert training courses in different learning formats (e-learning – classroom – blended) and co-created with various partners. From this year, they now also focus on how to apply the theory/legislation in the day-to-day relationship with the client.

Knowledge requirements on starting in the profession

Every bank, insurance or credit officer who comes into contact with a client must be able to prove their knowledge. This is based on statutory initiatives and also includes AML. This means, for example, that a garage employee must have proven knowledge to offer a car loan.

- Banking intermediation (Willems Act)
- Insurance distribution IDD
- Credit intermediation

CONTINUING PROFESSIONAL DEVELOPMENT

Basic training courses

These training courses are aimed at every employee who comes into contact with AML in their daily work.

Basic training with the objective of painting a general picture of AML: importance and impact:

- **The fight against money laundering (AML) and combating the financing of terrorism (CFT): general module + Investment funds + Payment Services and Electronic Money**
- **Money Laundering Regulation (AML V) obligations – a global overview**

Applying AML in practice and our relationship with the client: focus on trading skills

- **Anti Money Laundering (AML) and Know your Customer (KYC) in the relationship and contacts with clients**

Advanced training courses

The focus is on deepening AML knowledge and applying it in the organisation and its processes. These training courses are aimed mainly at employees who work substantially with AML subject matter.

Advanced training with the objective of recognising the players in the financing of terrorism, and this from practice, presented by a federal crime detective commissioner:

- **Preventing the financing of terrorism**
- **Learning to recognise types of money laundering**

Advanced training that provides more in-depth knowledge of history and the general statutory framework:

- **Anti-money laundering: AML V**

Importance of AML in insurance:

- **Further training in life insurance – Life insurance offerings: the pre-contractual obligations of the AML Act, the Belgian Economic Law Code (WER) and the Insurance Distribution Directive (IDD)**

Expert training courses

The focus is placed on AML's impact on various aspects of an organisation's policies. These training courses are aimed at employees who help develop the organisation's policies. The emphasis is also placed on the future and strategic impact.

AML and cryptocurrencies:

- **Investing in bitcoins or other cryptocurrencies: prudential framework**

Sanctions and embargoes under AML:

- **AML: Sanctions and embargoes**

AML and the role of the Management Board:

- **Executive program – The Board of Directors in the Financial Sector**

What does AML mean for our privacy and how do we deal with this in our organisation?

- **Developments for AML and challenges with Privacy: the perfect storm?**

Certification programme in conjunction with Deloitte Regulatory Services to prepare for the Certified Compliance Officer examination

- **Pathway – Certified Compliance Officer**

How to develop risk assessment for the organisation

- **Practical organisation and approach to risk assessment in compliance**

Belgian Financial Sector Federation

www.febelfin.be