ctif cfi

Belgian Financial Intelligence Processing Unit

26th Annual Report
2019

TABLE OF CONTENTS

I. PREFACE BY THE DIRECTOR

The publication of CTIF-CFI's 26th annual report is an opportunity to firstly thank all of CTIF-CFI's members of staff for the work done in 2019 and to secondly present the latest developments with regard to the prevention of money laundering and terrorist financing.

The major changes in the national and international financial landscape continued with the emergence of new financial players, leading to new high-risk sectors, in particular platforms for exchanging virtual currencies and custodian wallet providers established in Belgium.

Although the provisions of the fifth Directive should ensure a legal framework for platforms for exchanging virtual currencies, it is regrettable that the fifth Directive only relates to the exchange of virtual currencies and legal tender and that the exchange between various types of virtual assets has been forgotten, contrary to what is required by the FATF recommendations.

Part V is dedicated to the main changes to the AML/CFT framework by the transposition of the fifth Directive and hopefully provides some useful information to the reader.

In 2019 there was a significant decrease in the number of disclosures (from 33.445 disclosures in 2018 to 25.991 disclosures in 2019). This substantial change can be explained by the drop in the number of disclosures by payment institutions, as a result of a change with one of these institutions in the way disclosures are sent to CTIF-CFI. From now on this way of disclosing is based on a subjective analysis of suspicious transactions, which is more consistent with the provisions of the Law of 18 September 2017.

The decrease in the number of disclosures did not lead to a decrease in the number of files disseminated to the judicial authorities, however. CTIF-CFI disseminated 1.065 new files and a large number of additional investigation reports to the judicial authorities with information from 2.945 disclosures, for a total amount of EUR 1.538,83 million.

As Advocate-General Mr Damien Vandermeersch already mentioned, the investigation report disseminated by CTIF-CFI to the judicial authorities is "not an end point as such but should be the starting point of the judicial investigation. The information collected by CTIF-CFI is not evidence in the strict sense of the word. The data should be considered to be intelligence that should be checked and confirmed by the judicial investigation."

The last ten years 633 judgments and rulings were issued by courts and tribunals in files disseminated by CTIF-CFI. Fines and confiscations of more than EUR 300 million were imposed.

Yet the effect of preventive measures should not only be measured on the basis of judicial decisions, judgments or confiscated amounts though. CTIF-CFI sent 975 information notes, operational or strategic notes to the Federal Public Service Economy, the unit "Anti-fraud Coordination (CAF)" of the Federal Public Service Finance, Customs, the Social Intelligence and Investigation Service [SIRS-SIOD], the Central Office for Seizure and Confiscation [OCSC-COIV], the intelligence services and the Coordinating Unit for Threat Analysis [OCAM-OCAD].

CTIF-CFI keeps playing a major role in the international cooperation between financial intelligence units, especially in the European Union, with new mechanisms for exchanging and matching information, discussed in detail in this report.

CTIF-CFI does not operate in isolation. Its prime aim is judicial, creating a privileged partnership with the judicial authorities. In 2019, CTIF-CFI also extended the partnerships and the operational and strategic synergies, for instance by coordinating the activities of the Board of Partners [*Assemblée des partenaires*] of the Board for coordinating the fight against laundering money of illicit origin [*Collège de coordination de la lutte contre le blanchiment de capitaux d'origine illicite*].

CTIF-CFI's autonomy and independence is a necessary reality for its operations. Given its judicial aim it should fit in with and take into account the choices and the criminal policy of the judicial authorities, without prejudice to its autonomy.

This 2019 annual report relates to the period prior to COVID-19. The consequences of the COVID-19 crisis on ML/TF are not discussed in this report. In April CTIF-CFI published two statements that were made available.

I hope you enjoy reading the report.

Philippe de KOSTER
Director

PREFACE BY THE PROSECUTOR-GENERAL OF BRUSSELS

CTIF-CFI's 26th annual report enables me to, as Prosecutor-General, responsible for the "portfolio" of economic, financial, fiscal matters and corruption within the Board of Prosecutors-General [*Collège des procureurs généraux*] to emphasise that the preventive aspect of combating money laundering of illegal origin and the enforcement aspect should be seen as a whole, although the responsibilities are divided between different institutions.

So I would like to mention a few bridges that link CTIF-CFI and the Public Prosecutor's Office and illustrate the importance of an intelligent cooperation between us in order to achieve convincing results in combating money laundering.

One aspect that usually remains unnoticed is the creation of the Board for coordinating the fight against laundering money of illicit origin [*Collège de coordination de la lutte contre le blanchiment de capitaux d'origine illicite*] pursuant to the Royal Decree of 23 July 2013. CTIF-CFI's Director and the Prosecutor-General in charge of specific tasks with regard to financial crime and tax crime within the Board of Prosecutors-General jointly chair this Board. This body enables high-level interaction of the preventive and law enforcement aspects. This body plays an important role within the comprehensive AML framework. In this regard we would like to mention that the updated version of the ML risk assessment in Belgium, commenced in 2019, was finalised in 2020. This document, developed on the basis of a new and professional methodology, will make it possible to dedicate the resources of the different partners for the detection of suspicious transactions in the most high-risk sectors.

As a result, the judicial response will be improved and better targeted, thus strengthening the entire Belgian framework.

Cooperation on the ground was also extended in 2019. The Prosecutor-General's Office and the Auditorate-General of Brussels set up a platform consisting of the Public Prosecutor of Brussels, the French-speaking and Dutch-speaking commercial courts [*tribunaux de l'entreprise*] of Brussels and the federal judicial police of Brussels (as well as other partners) to detect dormant companies and dissolve them. This is an example of synergies in order to clean up the "market" of legal persons to avoid that criminals can easily use legal persons as a channel for money laundering operations.

The Board of Prosecutors-General is also finalising a circular letter regarding the criminal policy on money laundering. This criminal policy is always in keeping with the coordination efforts of the different partners in accordance with their respective powers. The cooperation between the Public Prosecutor's Office and CTIF-CFI is one of the main points to continue prevention and enforcement. CTIF-CFI should be informed of the Public Prosecutor's Office's priorities in terms of prosecution so that human and material resources can be allocated to the most relevant objectives. By introducing clearer procedures the information exchange will also be facilitated.

To finalise this brief overview I can already announce –even though this does not relate directly to the activities of 2019, that the Board of Prosecutors-General will give special attention to the disseminations by CTI-CFI with regard to money laundering perpetrated during the COVID-19 health crisis in order to ensure that crime does not go unpunished.

Johan Delmulle
Prosecutor-General of Brussels

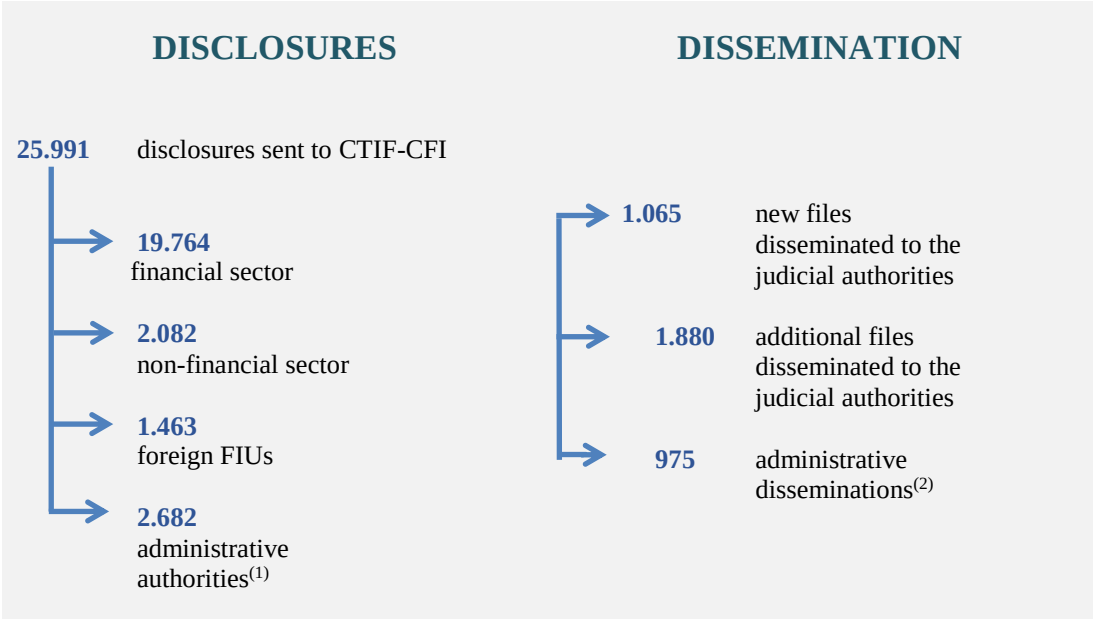
II. COMPOSITION OF CTIF-CFI[1]

Director:	Mr	Philippe de KOSTER
Vice President:	Mr	Michel J. DE SAMBLANX[2]
Deputy Director:	Mr	Boudewijn VERHELST
Members:	Mr	Johan DENOLF
		Fons BORGINON
	Ms	Chantal DE CAT
Secretary-General:	Mr	Kris MESKENS

[1] Situation on 31 December 2019.
[2] Deputy from 1 September 2017.

III. KEY FIGURES 2019

CTIF-CFI's mission is to receive disclosures of suspicious transactions from obliged entities mentioned in the Law of 18 September 2017 on the prevention of money laundering and terrorist financing and on the restriction of the use of cash[3], from foreign FIUs as part of international cooperation and from other services of the State, as referred to in the law. CTIF-CFI uses its designated powers to analyse and enhance this information. In case of serious indications of money laundering, terrorist financing, or proliferation financing, CTIF-CFI disseminates the result of its analysis to the judicial authorities.



(1) Disclosures of cross-border transportation of currency, fiscal regularisation certificates, disclosures by officials of administrative services of the State (including the State Security Department [VSSE], the General Intelligence and Security Service of the Armed Forces [SGRS-ADIV] and the Coordinating Unit for Threat Analysis [OCAM-OCAD]), by the Public Prosecutor's Office, as part of an inquiry or preliminary inquiry related to terrorism and terrorist financing and the supervisory authorities, in accordance with Article 79 of the AML/CFT Law.

(2) Information communicated to Public Prosecutor's Offices in labour matters [*auditorats du travail*], the unit "Anti-fraud Coordination (CAF)" of the Federal Public Service Finance, Customs, the Social Intelligence and Investigation Service [SIRS-SIOD], the Federal Public Service Economy, the European Anti-Fraud Office OLAF, the Central Office for Seizure and Confiscation [OCSC-COIV], the intelligence services and the Coordinating Unit for Threat Analysis [OCAM-OCAD], in accordance with Article 83 of the AML/CFT Law and the supervisory authorities of obliged entities in accordance with Article 121 of the AML/CFT Law.

CTIF-CFI is legally required to exchange and report certain information from these files to other national authorities: to the unit "Anti-fraud Coordination (CAF)" of the Federal Public Service Finance when the notification to the Public Prosecutor contains information regarding laundering the proceeds of offences that may have repercussions with respect to serious fiscal fraud, whether organised or not, to the Customs and Excise Administration when this notification contains information regarding laundering the proceeds of offences for which the Customs and Excise Administration conducts criminal proceedings; to the supervisory authorities of obliged entities and the Federal Public Service Economy when this notification contains information regarding laundering the proceeds of an offence for which these authorities have investigative powers; to the Social Intelligence and Investigation Service [SIRS-SIOD] when the notification to the Public Prosecutor contains information regarding laundering the proceeds of offences that may have repercussions with respect to social fraud; and to the Public Prosecutor in labour matters [*auditeur du travail*] when the notification to the Public Prosecutor contains information regarding

[3] Hereinafter referred to as the Law of 18 September 2017. Belgian Official Gazette of 6 October 2017 – Chamber of Representatives (www.lachambre.be) Documents: 54-2566.

laundering the proceeds of smuggling of human beings (including trafficking in illegal workers, now included in the main concept of smuggling of human beings) or trafficking in human beings.

CTIF-CFI can also inform the Central Office for Seizure and Confiscation [OCSC-COIV] when assets of significant value, of any nature, are available for potential judicial seizure.

To tackle the security threat CTIF-CFI also cooperates closely with the civil and military intelligence services and the Coordinating Unit for Threat Analysis [OCAM-OCAD]. CTIF-CFI can contextualise requests for assistance/information it sends to these three authorities. As part of mutual cooperation (Article 83 § 2, 4° of the AML/CFT Law), CTIF-CFI can also send useful information to the intelligence services and to OCAM-OCAD.

- **25.991** disclosures sent to CTIF-CFI
- **1.065** new files disseminated to the judicial authorities in 2019 and information from **2.945** disclosures was used in files disseminated to the Public Prosecutor's Offices and the Federal Public Prosecutor's Office for a total amount of **€1.538,83 million.**
- **975** information notes (or copies of investigation reports) were also sent to the Public Prosecutor's Offices in labour matters [*auditorats de travail*], the Federal Public Service Economy, the unit "Anti-fraud Coordination (CAF)" of the Federal Public Service Finance, Customs, the Social Intelligence and Investigation Service [SIRS-SIOD], the Central Office for Seizure and Confiscation [OCSC-COIV], the intelligence services and the Coordination Unit for Threat Analysis [OCAM-OCAD], in accordance with Article 83 of the AML/CFT Law and the supervisory authorities of obliged entities in accordance with Article 121 of the AML/CFT Law.

Part IV contains an overview of money laundering and terrorist financing trends in 2019. A detailed overview of the statistics of 2019 is included in part VI.

IV. MONEY LAUNDERING AND TERRORIST FINANCING TRENDS

1. Money laundering trends

1.1. Evolution of criminal threats

1.1.1. Drug trafficking

Trends identified

a. One of CTIF-CFI's priorities

The figures from the customs authorities indicate that 2019 was once again a record year in terms of drugs seizures in Belgium. In the port of Antwerp last year 61,8 tonnes of cocaine were seized, which is an increase of a quarter compared to 2018. The seizures of heroin, cannabis and synthetic drugs also peaked in 2019. The amounts involved in these seizures are astronomical. The street value of the seized cocaine alone is more than EUR 3 billion. The most optimistic estimates assume that 10% of the import is intercepted, which would bring the total annual turnover of cocaine imported via Belgium to the extraordinary amount of EUR 30 billion. Although this is just a rough estimate of criminal proceeds, these figures do provide a good insight into the enormous proportions of the money laundering aspect related to drug trafficking.

Given these figures it is only logical that combating money laundering linked to drug trafficking was one of CTIF-CFI's main priorities, as was the case in previous years.

When looking at the number of files disseminated to the judicial authorities in 2019, drug trafficking comes in third place, just like in 2018. Several files were also disseminated to the judicial authorities with organised crime as predicate offence, given that criminal organisations involved with drugs often make use of several types of crime.

The amounts that CTIF-CFI identified in these drugs-related files are not proportional to the enormous figures that can be deduced from the seizures. A possible explanation may be that part of the funds are categorised differently, such as social or fiscal fraud. In large-scale corruption cases suspicious transactions can also partially relate to funds that initially originate from drug trafficking.

The transactions in cases often relate to intermediary trade and less frequently refer to profits at the top of the criminal organisations. This becomes clear through the amounts identified in files, ranging from EUR 20.000 to EUR 200.000 a year. These sums are often deposited in cash and there is no (credible) explanation for the origin of the funds.

b. Several modi operandi

At the end of 2018, CTIF-CFI conducted a strategic analysis to record money laundering related to drug trafficking. This analysis showed that trade-based money laundering, as well as investments in luxury goods and real estate, were the most important typologies at national and international level. The conclusions of this analysis, which were shared as broadly as possible with obliged entities and partners still apply to the files disseminated in 2019.

In several files cash was injected through the accounts of front companies in cash-intensive businesses, with the final aim of purchasing real estate in Belgium or abroad. The most frequent countries of destination of funds are the United Arab Emirates (Dubai), Morocco and Turkey.

Analysis of files also indicates that at international level professional money laundering networks are active and try to integrate proceeds of drug trafficking into financial flows related to international trade.

By using mechanisms such as the offsetting technique and trade-based money laundering (TBML) funds are disguised as payments for commercial activities and laundered.

At national level and on a smaller scale, the gaming sector –casinos as well as online gaming sites – is also increasingly used to launder the proceeds of drug trafficking.

When combating the laundering of the proceeds of drug trafficking the evolution of payment systems and virtual assets should also be taken into account. A growing part of the drug market takes place online and payments are carried out using virtual assets. The speed and the ease of opening accounts and carrying out transactions with new payment services or Payment Service Providers (PSPs) may also facilitate money laundering.

Identifying the beneficial owners of large financial flows associated with drug trafficking remains a big challenge for the financial systems and for FIUs in particular. The creation of the preventive AML system in the early nineties was specifically aimed at drug trafficking as a predicate offence. Drug trafficking organisations have gained thirty years' experience in circumventing potential detection of their criminal proceeds. Yet the basic principle remains the same: these organisations still need to inject large amounts of cash into the financial system in order to invest them.

Action taken

CTIF-CFI will continue its close cooperation with national and international partners to get an insight into the money laundering mechanisms linked to drug trafficking. At national level the information of specialised police units on the composition of criminal "clans" is of great importance because this information enables CTIF-CFI to link the financial structure to the organisation's operational structure. The resulting helicopter view enables targeted subsequent action by the Public Prosecutor's Office.

At international level, cooperation with the FIUs of a number of sensitive countries remains crucial. Our neighbouring country the Netherlands largely faces the same issues with regard to drugs as Belgium does and criminal networks operate flexibly across borders. Furthermore, CTIF-CFI also continues with the swift exchange of information with the main countries of destination of drug money from Belgium in order to get an insight into the investments in these countries. Enhanced national and international cooperation is undoubtedly the best way of tackling laundering the proceeds of drug trafficking, an issue that will probably not diminish in the coming years.

1.1.2. Fraud

Trends identified

Fraud has been one of the main predicate offences in terms of the number of files disseminated to the judicial authorities. This trend continued in 2019. As in previous years large amounts are involved. Analysis of the modus operandi reveals several trends, both with regard to the types of fraud as to the methods to launder the proceeds of fraud.

a. Mass fraud: targeted approach of victims

The number of files related to mass fraud in the traditional sense, i.e. mass sending of emails to target victims among those who respond, of which CTIF-CFI was informed, was considerably lower. The fraudsters' ultimate goal remains the same: receive payments, purported to be "advance payments" in exchange for a (financial) advantage for the victims. Unlike in the past, victims are seemingly not randomly contacted on a large scale but are targeted individually through social media and selected based on their vulnerability and financial resources. This method requires more efforts to look for potential victims but has a higher success rate and may explain why victims end up sending large amounts of

money. An additional issue for financial institutions is that customers who are targeted this way are often not considered to be victims and are often not prepared to file a complaint with the police themselves.

Fraudsters often use an emotional reason as an excuse. A story is made up about an American soldier in need of money to leave a war zone and come to Belgium. Apart from an emotional reason there is often also a financial element: the payment of a large amount of money can only be carried out after advances have been paid.

Proceeds of this fraud are generally sent to African countries such as Nigeria, Cote d'Ivoire, Ghana and Tunisia, as well as to other countries such as Turkey, Bulgaria, the United Kingdom and the United States.

b. Recruiting money mules acting as accomplices

Criminal organisations also use social engineering for types of fraud targeting companies. Fictitious payment instructions from a general manager or financial manager – a CEO – have been identified, yet payment instructions are often intercepted in order to change the recipient's account number into the one of the money mule. Hacking a company's computer network or e-mail system is undoubtedly the basis of this fraud, known as Business Email Compromise (BEC).

Money mules granting access to their account to receive funds could be naive victims but the speed with which funds are transferred and the cash withdrawals indicate complicity. These transactions are different from the other transactions on the mule's account, usually a limited number of transactions take place on this account. These transactions are international transfers for large amounts with references related to invoices or deliveries from legal persons abroad. In some cases there are links between different money mules and they transfer money to each other. This shows that criminal organisations have an extensive number of accounts that they use to multiply the steps to launder the proceeds of such fraud. Money from large-scale fraud to the detriment of companies often ends up in China and Hong Kong.

c. Evolution of the modus operandi: use of new payment methods

Financial institutions look out for fraud and must contact their customers if they find that large sums are transferred to their accounts or sent to seemingly unrelated persons. Fraudsters look for alternative channels to receive their funds. They can use crypto assets, payments on accounts of payment service providers, institutions for electronic money or other alternative payment systems.

In 2019, CTIF-CFI identified several cases related to fraud in which fraudsters used payment vouchers to remove the financial ties with their victims to facilitate laundering.

The following modus operandi was used: victims were asked to go to petrol stations, bookshops or night shops where there was a terminal to print tickets for online vouchers. These were vouchers for fixed amounts of EUR 10, 25, 50 or 100 with a 16-digit code for online purchases. Fraudsters then asked their victims to give them these codes and then used them for payment, more specifically on gaming sites allowing payouts on a bank account. The bank considered this money to be the proceeds of online betting. So there was no longer a financial link between the origin of the money, i.e. fraud, and the victims of the fraud. No checks are possible when vouchers are purchased, even for large amounts. The traders with a terminal are not subject to the preventive law and the suppliers of the vouchers have not got any insight into individual payments carried out to purchase these vouchers. Although the amounts per voucher are quite small, we found that the victims sometimes purchased tens of thousands' EUR worth per day in the same shop.

Action taken

Awareness-raising and prevention

It is clear that criminal organisations want to use the recent changes to the financial landscape for money laundering purposes. These changes included the emergence of new players, the increased speed and the ease of use of the traditional financial system and new payment systems. The current challenge is to combine the advantages for the consumer, and the evolving payment transactions with monitoring mechanisms to continue the fight against money laundering, such as laundering the proceeds of fraud.

The best way to fight the laundering of the proceeds of fraud is to prevent the predicate offence, by informing potential victims of possible risks. CTIF-CFI will strengthen the cooperation with other bodies involved in combating fraud such as the FSMA and the Federal Public Service Economy. This way financial information can not only be used for the law enforcement aspect but also for the preventive part of combating fraud.

1.1.3. Social fraud and/or serious fiscal fraud

Trends identified

By adding social fraud to the list of predicate offences in 2017, CTIF-CFI was able to counter this serious criminal phenomenon and, in particular, to deal with those who set up and organise social fraud networks. In 2019, a record number of files related to social fraud was disseminated to the Public Prosecutor's Offices. Serious fiscal fraud was also identified as a predicate offence. Social fraud also involves unofficial payments, these assets are therefore not known to the tax authorities. Serious tax fraud and social fraud – and also organised crime – are linked more than ever.

a. Brazilian networks: rise of the phenomenon

For a number of years now CTIF-CFI has identified in its files that Brazilian or Portuguese nationals establish or take over companies, mainly in the industrial cleaning industry. These companies are used as a cover to employ undeclared workers.

This issue is not decreasing, on the contrary, analysis of the files shows that this phenomenon is on the rise at different levels: the number of files disseminated to the judicial authorities rose sharply, the amounts disseminated to the judicial authorities total up to millions of EUR and several links between files were identified.

Research by CTIF-CFI found that for some of these companies there is a legal obligation to retain a percentage of the invoice, which is to be paid to the Federal Public Service Finance. Some companies are not registered with the National Social Security Office. When they are registered, they only employ one employee, which seems to be a small number given the volume of the transactions on these companies' accounts. The companies are usually not listed as Belgian customers of foreign companies in the Limosa register in the Dolsis database.

Apart from cash withdrawals, funds are also transferred to accounts in Belgium or Portugal held by natural persons. These transfers refer to the payment of wages, although no Dimona-declaration was submitted. Other transfers are intended for Portuguese companies. Searches in the Limosa register show that these transfers were unwarranted.

Most of the counterparties were unfavourably known to CTIF-CFI as they feature in files disseminated to the judicial authorities with regard to social fraud and/or serious fiscal fraud. Several counterparties are also unfavourably known with foreign counterpart FIUs for being part of a network of Portuguese

companies. The accounts of these companies regularly receive international transfers from several Belgian construction companies managed by Brazilians.

b. Fraud involving secondments: increased involvement of Turkish-Bulgarian networks

Cross-border social fraud comes in many forms. Often the rules on secondment are breached. Analysis of the files disseminated to the judicial authorities by CTIF-CFI shows that a growing number of Belgian legal persons use Turkish-Bulgarian networks in the sectors of agriculture, meat processing, transport, construction and cleaning. For services provided the Belgian legal persons transfer large amounts of money to their subcontractors, which are also Belgian legal persons managed by Turkish or Bulgarian nationals. Through these buffer companies, which often use the same post office box address, money is withdrawn in cash and millions of EUR are channelled to Bulgarian front companies that also use post office box addresses.

Bulgarian front companies were initially taken over or established by individuals of Turkish or Bulgarian origin with an address in Belgium. Once established or taken over these foreign companies second Bulgarian workers to Belgium. A few months after being established or taken over, new companies are taken over or other Bulgarian companies are used. Employees, often the same Bulgarian employees (including the managers of the Bulgarian companies involved) are seconded to the same Belgian legal persons.

The Bulgarian accounts are only used to receive large transfers from Belgian buffer companies, making it clear that the company seconding employees does not carry out any significant economic activity in the country of origin of the employee. This is one of the main conditions for secondment, so this is a scheme set up to commit secondment fraud. Furthermore, the funds on the Bulgarian account are almost exclusively withdrawn in cash in Bulgaria and are smuggled back to Belgium by the manager or via cash couriers or withdrawn using a bank card in Belgium or Turkey.

The sole fact that a legal person has a subsidiary in Eastern Europe and transfers money to this subsidiary will not automatically lead to a dissemination to the judicial authorities because of serious indications of laundering the proceeds of social fraud. Such an arrangement is legitimate when the company established in Eastern Europe has a genuine activity in the country in which it is established. To determine whether there is cross-border social fraud, CTIF-CFI can send a request with the necessary context to the relevant counterpart FIU to check the economic reality of the activities and/or whether there is any unfavourable information.

An essential element of the analysis is the account history of the subsidiary, which can provide CTIF-CFI with valuable information on its actual activity. If purchases in Belgium take place consistently and very few international transactions are carried out, it can be deduced that the subsidiary is actually a shell company that does not have any real activity and that its operational activities are conducted in Belgium.

c. Return of funds: a large grey area

The largest part of tax-related disclosures involve the return of funds. Several scenarios are possible here, according to the origin of the capital and related income from moveable assets.

Here is an overview:

Capital	*Income from moveable assets*	*Regularisation?*
Declared	Declared	No, but the capital and income from moveable assets are substantiated
Declared	Undeclared	Yes, regularisation of the income from moveable assets and capital substantiated
Undeclared	Declared	Yes, regularisation of fiscally time-barred capital and income from moveable assets are substantiated
Undeclared	Undeclared	Yes, regularisation of fiscally time-barred capital and income from moveable assets

CTIF-CFI has found that there a few files for which both the capital and the income from moveable assets are not declared. This is also logical given that more information is exchanged internationally and more Belgians opt for a fiscal regularisation. The majority of the tax-related disclosures are in this grey area.

By combining data from the police, judicial authorities, the Federal Public Service Finance (including the Department for Advance Tax Rulings with the Point of Contact Regularisations), the Flemish tax authorities and/or foreign counterparts, CTIF-CFI has several sources that could lead to suspicions of money laundering, proceeds of serious fiscal fraud or not.

d. Diamonds: reservations on the announced value

In 2019 a number of significant files with regard to diamonds were disseminated to the judicial authorities due to serious indications of money laundering related to serious fiscal fraud. In these files acknowledged experts often reported reservations on the announced value of diamonds.

Under- or overvaluing diamonds with respect to the market value makes it possible to forge profit and turnover figures and facilitates serious fiscal fraud as a result.

This alleged difference between the valuation of the expert and the amounts in the documents regarding the transactions is communicated to the relevant department of the Federal Public Service Economy, which then starts an investigation. In this case the dealer in diamonds must substantiate his declaration and the difference between the declared value and the value of the expert. Pursuant to Article 8, § 3 of the Royal Decree of 20 November 2019 on measures for the supervision of the diamond sector, the Federal Public Service Economy uses a risk-based approach to report these files to CTIF-CFI.

e. VAT carousel fraud: mixing with other types of crime

CTIF-CTIF still has to deal with files related to VAT carousel fraud. Although VAT (carousel) fraud has been around for over a quarter of a century, the investigation project by journalists “Grand Theft Europe” (2019) found that EUR 50 billion is lost in the European Union every year due to such types of fraud. VAT (carousel) fraud remains appealing because there is no harmonised system for charging VAT in the EU. This is facilitated by competition between countries to provide a fiscal environment that is as beneficial as possible. Although this type of fraud is generally committed using small valuable objects such as mobile phones and computer chips, the finding is that organisers of fraud schemes increasingly use various types of other products such as copper cathodes, polymer plastic beads, platinum, precious metals, but also basic foodstuffs such as sugar and meat. Furthermore, it is found that with VAT carousel fraud mixing takes place with other types of fraud.

Action taken

a. Cooperation between CTIF-CFI and SIRS-SIOD

The Social Intelligence and Investigation Service [SIRS-SIOD] is a body in charge of developing concrete strategies to combat social fraud. This includes setting up an annual action plan to combat this type of crime and taking part in the activities of the Board for combating fiscal and social fraud.

SIRS-SIOD is an important partner of CTIF-CFI, in accordance with the Law of 18 September 2017. When CTIF-CFI disseminates information to the judicial authorities regarding laundering the proceeds of offences that may have repercussions with respect to social fraud, CTIF-CFI forwards the information to SIRS-SIOD that may be of use them resulting from the dissemination of this file to the judicial authorities.

CTIF-CFI cannot only forward information to SIRS-SIOD when CTIF-CFI has identified social fraud, trafficking in human beings or smuggling of human beings as a predicate money laundering offence, but also more general information on an offence that may have repercussions with respect to social fraud. For instance, when CTIF-CFI disseminates a file to the judicial authorities because of serious indications of illegal trafficking in narcotics or illegal trafficking in goods and merchandise and knows that the individual receives social benefits, it will assume that this information may have repercussions with respect to social fraud and will inform SIRS-SIOD.

After several years of fruitful cooperation it was necessary to amend the practical arrangements for disseminations to SIRS-SIOD to take into account the workload and the respective challenges of both bodies. Representatives of SIRS-SIOD and CTIF-CFI met several times and agreed on the new methods for providing information, which were introduced in 2019.

b. CTIF-CFI's access to the e-PV database

The e-PV database is managed by the Federal Public Service Employment, Labour and Social Dialogue. It was established in accordance with the social criminal code and contains a large array of useful information for those who are involved in combating social fraud and illegal employment.

CTIF-CFI currently does not have access to the e-PV database. Having access would be a real added value for its task of combating the proceeds of social fraud and trafficking in human beings. The Federal Public Service Employment, Labour and Social Dialogue and CTIF-CFI started their cooperation at the end of 2019 aimed at adding CTIF-CFI to the list of authorities that have access to e-PV. The work will be continued in 2020.

1.1.4 Corruption – embezzlement

Combating corruption is one of the global priorities today. According to the World Economic Forum the cost of corruption is at least 2600 billion dollars or 5% of the global gross domestic product. According to the World Bank, the bribes paid each year amount to 1000 billion dollars, which represents 9% of the world trade.

Financial intelligence units have an important role to play in this regard, in particular for early detection. The action taken by CTIF-CFI demonstrates the importance attached to this issue[4]. One of the challenges is the identification of Politically Exposed Persons (PEP). To simplify the identification of PEPs in the European Union, Member States are required, in accordance with fifth Directive, to establish a list with certain functions which, in accordance with domestic legal provisions, are considered to be important public functions[5].

[4] Cf. infra.

[5] This is a list of functions considered to be important public functions, not a list of persons.

Trends identified

In 2019, CTIF-CFI disseminated 10 files to the judicial authorities due to serious indications of laundering the proceeds of embezzlement by public officials and/or corruption. The files disseminated to the judicial authorities by CTIF-CFI related to public and to private corruption.

In most of the cases a politically exposed person (PEP) from abroad, a family member of this PEP, or a close associate was involved. The other cases mainly involved Belgian companies in the private sector[6].

As in previous years CTIF-CFI found that the majority of disseminations to the judicial authorities based on national disclosures came from credit institutions. Nearly all files disseminated to the judicial authorities also have an international element such as the personal details of those involved, financial flows or the entity disclosing the suspicious transactions to CTIF-CFI (i.e. another FIU, spontaneous disclosure of information or requests for information). International cooperation is of crucial importance in these files.

Transactions were identified linked to the payment of bribes, the use of the proceeds by the recipient and the laundering of proceeds by the party that had committed the bribery.

Various money laundering techniques were used, ranging from quite simple to more sophisticated ones, in different money laundering stages.

The total amount of suspicious transactions in these files was EUR 18,65 million.

a. Embezzlement of public resources and corruption by foreign PEPs

Several files disseminated to the judicial authorities show that politically exposed persons are vulnerable to embezzlement and corruption. The files featured PEPs from countries in West and Central Africa, relatives or close associates of these PEPs. The affected countries are politically unstable countries with mostly cash-intensive economies.

Money laundering in these files took place via straightforward transactions –international transfers from accounts in the individual's country of birth opened by relatives of the individual to the individual's account in Belgium – as well as more complex methods such as the use of channelling accounts in Belgium or foreign corporate structures. A number of cases involved real estate transactions in Belgium.

CTIF-CFI used various sources of information for its analysis and contacted domestic and international partners. In some instances relevant information on the individuals involved was obtained from the civil intelligence service, such as information on their capacity or their involvement in corruption or embezzlement. In other cases the operational exchange with Egmont Group FIUs led to valuable information on the profile of the individuals involved and the origin of funds on accounts abroad.

[6] The term "person performing a public function" should be interpreted in the broad sense and refers to all persons in charge of a public service mission and also includes private individuals that have been designated by the government to carry out a role in a matter of general interest such as awarding contracts or supervision of the awarding of contracts. The prohibited conduct for the persons performing the public function is taking action (legal or illegal actions, positive actions or refraining from actions) related to this function by means of benefits in kind. In case of facts related to private corruption the one involved in the corruption is the director or manager of a legal person or the designated person of a legal person or natural person and requests or accepts a benefit in kind, to undertake action for himself or a third party or refraining from action of his function unknown to or without the permission of, depending on the case, the board of directors or the general assembly of which he depends, or of his employer or agent.

Case: Embezzlement of public funds channelled through offshore bank accounts and invested in real estate in Belgium

In 2019, a foreign couple purchased a property in an expensive neighbourhood in the region of Brussels.

A large part of the property was paid by international transfers from the account of one of the buyers in the Middle East. There were also transfers from the individual's personal account in a financial centre in Africa and transfers from an escrow account (blocked account) with a financial institution under the law of another EU Member State in one of Belgium's neighbouring countries.

CTIF-CFI's research showed that the individual sold fossil fuels in a country in West Africa. His father had held a prominent public function for years there and coordinated government activities related to the buying and selling of fossil fuels.

CTIF-CFI was informed by FIUs in countries from where money was sent to Belgium that the funds sent from the individual's account abroad consisted of cash deposits and/or transfers ordered by foreign companies owned by the individual (consultancy, including fossil fuels).

Both the individual and his father had been mentioned in media reports for years, reporting on suspicions of embezzling the proceeds of the sale of fossil fuels that should have gone to the Treasury of this country in West Africa.

There are reasons to believe that the funds transferred by or for the individual to the notary's escrow account in order to purchase a property in Belgium partially or wholly originated from embezzlement by an individual holding a public function.

b. Involvement of private companies in corruption

Several files disseminated to the judicial authorities related to high-risk business transactions or business partners, such as transactions between companies and government authorities or transactions involving third parties (agents / intermediaries) or in sectors that are generally associated with a higher level of corruption, such as the construction industry or infrastructure projects.

Police information was often a key element in these files. In one of them, the Belgian account of a Belgian service company received transfers from a multimunicipal utility company. Police information showed that the company was suspected of public procurement offences and of producing and using forged documents. The file was disseminated to the judicial authorities because of serious indications of laundering of proceeds of fraud with public procurement[7].

Although the use of intermediaries and agents is common practice and legitimate in the current business climate, there are cases where commissions are used as bribes. An intermediary paying bribes to secure a contract can recover some of the money by using fake invoices, for instance.

Payments of bribes concealed as commissions often take place through different bank accounts or front companies. As a result, distance is created between the payer and the receiver of the bribes and the identity of both parties is concealed.

Such was the case in a file involving a Belgian national with a public function. Payments by Belgian companies suspected to be secret commissions for public procurement to these Belgian companies were

[7] *Office Central pour la Répression de la Corruption* [Central Office for Combating Corruption] https://www.police.be/5998/fr/a-propos/directionscentrales/office-central-pour-la-repression-de-la-corruption-ocrc-0

carried out through accounts of foreign corporations in one of Belgium's neighbouring countries and ended up on an account in a neighbouring country held by a foreign consultancy firm owned by the Belgian national.

This case also illustrates the crucial importance of information on companies' beneficial owners. It should be noted that the EU now requires Member States to have registers of companies' beneficial owners to detect possible conflicts of interest and reduce potential misuse of public resources.

The following case shows that private corruption in some files disseminated to the judicial authorities also involved other offences, such as the misappropriation of corporate assets.

> Case: Payment of retrocommissions derived from private corruption with a foreign company on a Belgian account
>
> An individual who was no longer registered in Belgium opened several accounts with a Belgian bank. It was alleged that the accounts were opened in Belgium because he could not open a foreign currency account in his country of origin and residence.
>
> The accounts received international transfers by order of an Asian multinational corporation manufacturing agricultural and industrial chemicals. The transfers referred to "commissions".
>
> Information received from a foreign counterpart FIU showed that the individual was an associate of the company selling agricultural production resources in his native country. According to the local customs authorities the ordering party of the transfers was a supplier of that company. The transactions should therefore have been conducted through the corporate account and not the individual's personal account.
>
> The individual used the money for stock exchange transactions and investments and transferred large amounts to accounts in his name outside of Belgium or outside of his fiscal country of residence. In addition, payments took place to a person assumed to be the manager of the company of which this individual is an associate.
>
> There is no economic rationale for the suspicious transactions, the direction of the financial flow does not make sense and the transactions are clearly being kept out of the accounting of the foreign company.
>
> It can therefore be assumed that the individual claims to be a "supplier" of the company of which he is an associate and that the commissions paid to him by the supplier of that company were the result of private corruption, so that the ordering party won the contracts with the company. The transfers to the company's official manager of which the individual is an associate are more than likely aimed at ensuring that this person acts as an accomplice.

Action taken

a. Cooperation between CTIF-CFI and OLAF

The European Anti-Fraud Office (OLAF) is the body of the European Union in charge of independent investigations into fraud and corruption with European assets. OLAF does not have its own sanctioning powers. The investigations end with financial, judicial, disciplinary or administrative recommendations to national authorities or European institutions involved in the identified shortcomings.

CTIF-CFI and OLAF are long-term partners in combating corruption. Article 79, § 3, first subparagraph, 3° of the Law of 18 September 2017 enables OLAF to disclose information to CTIF-CFI as part of an investigation into fraud detrimental to the financial interests of the European Union, including corruption.

Moreover, OLAF and CTIF-CFI are able to exchange information at every stage of their respective investigations on corruption with European assets, in accordance with Article 83, § 2, first subparagraph of the same Law.

The practical arrangements of the cooperation have been laid down in a memorandum of understanding. In 2019, CTIF-CFI started the revisions of this agreement, aimed at aligning the agreement with legislative developments of recent years and strengthening synergies between these two bodies.

b. Egmont Group – FIU.Net

Combating the proceeds of corruption was an important topic for the Egmont Group in 2019. One of the Egmont Group's Working Groups compiled a report on resources and practices used by FIUs and used for collecting, analysing and disseminating corruption-related files. A summary of the report was published in July 2019[8].

In accordance with Article 53.1 of the fourth anti-money laundering Directive, an FIU that receives a report which concerns another Member State shall promptly forward this to this Member State. A working group, led by CTIF-CFI's Secretary-General, has developed various criteria to help FIUs of the European Union comply with their requirements regarding cross-border dissemination by facilitating the identification of information that needs to be disseminated to a foreign FIU. The involvement of a PEP is obviously one of the relevance criteria that should lead to the swift forwarding to the European FIU of the PEP's country of origin.

c. CTIF-CFI's involvement in activities of international fora

- *United Nations Office On Drugs and Crime (UNODC)*

From 12 to 14 June 2019 the United Nations Office on Drugs and Crime (UNODC), in partnership with Norway, organised an expert meeting on large-scale corruption. One hundred and forty experts attended, including a representative of CTIF-CFI[9]. Following the meeting the experts drew up 64 recommendations for policy makers. Three of these recommendations emphasise the role of financial intelligence in combatting corruption and the need to have the appropriate tools to combat money laundering.

Belgium was designated in 2019 to assess the compliance of the Swedish framework with chapter II (preventive measures – including money laundering) and chapter V (asset recovery) of the United Nations Convention against Corruption. Several Belgian experts were in charge of this task, including CTIF-CFI's Director, Philippe de Koster, and one of CTIF-CFI's legal advisers. The assessment process of Sweden will be continued in 2020.

[8] Egmont Group of Financial Intelligence Units - FIU Tools and Practices for Investigating Laundering of the Proceeds of Corruption (Public Summary) Egmont Group of Financial Intelligence Units (July 2019) https://egmontgroup.org/sites/default/files/filedepot/external/20190710%20-%20Public%20Summary%20-%20FIU%20Tools%20and%20Practices%20for%20Investigating%20ML%20of%20the%20Proceeds%20of%20Corruption%20-%20final.pdf The publication includes a set of indicators that can help detect (laundering the proceeds of) corruption. The overview was compiled by FIUs and further supported by international partner organisations, including the Wolfsberg Group.

[9] The discussions included the topics of the establishment of an international court judging the most serious forms of cross-border corruption, the role of financial intermediaries in laundering the proceeds of large-scale corruption and the importance of identifying the ultimate beneficial owners of companies granting public procurement.

- ***OECD***

In 2019, as Member of the Belgian delegation, CTIF-CFI's Director took part in several meetings of the OECD Working Group on Bribery in International Business Transactions[10]. FIUs undoubtedly play a part in detecting foreign bribery and asset recovery. CTIF-CFI advocates the recognition of this role in the revised recommendation.

1.2. Evolution of money laundering techniques

1.2.1. Professional launderers working for criminals

Trends identified

CTIF-CFI increasingly finds that professional money launderers operate for the benefit of criminals. Self-laundering is replaced by the professionalisation of the money laundering activity, which is becoming an activity in itself. Money launderers operate as service providers to launder the proceeds of numerous and various crimes. This is not a local phenomenon, this trend is also identified internationally[11].

a. A series of shell companies is set up through professional intermediaries

The use of corporate structures for criminal purposes and for money laundering purposes is a recurring technique that CTIF-CFI has identified for a number of years. Several files indicate that legal professionals and accountancy professionals were used to set up corporate structures for illegal purposes.

The increasing professionalisation of money laundering entails the risk that criminals would use legal professionals and accountancy professionals as money laundering facilitators even more frequently. This risk became apparent in various files disseminated to the judicial authorities in 2019. CTIF-CFI found that intermediaries were increasingly used to carry out various illegal activities. The files in question showed that the characteristics of the customer, of the business relationships or the transactions should have been noticed by these professionals and could/should have led to suspicions.

Case: money laundering with the use of shell companies through accounting professionals and legal professionals

It became clear in several files that a series of companies was set up. These companies seemed to be shell companies that were used as front companies, indicating an increased money laundering risk.

The companies involved operated in high-risk industries with respect to money laundering, such as the construction industry, industrial cleaning, import and export or the hospitality industry. Their managers appear to be front men. They are mainly young people of foreign origin or of foreign nationality. Some of them are appointed shortly after their arrival in Belgium. They clearly do not have the necessary business management skills. Furthermore, many of them manage several companies.

[10] This Working Group monitors the implementation and enforcement of the OECD Anti-Bribery Convention, the 2009 Anti-Bribery Recommendation and related instruments. It is currently discussing the revisions of the 2009 recommendations. When assessing the implementation of the convention and the recommendation it is examined how anti-money laundering mechanisms can support the detection and reporting of foreign bribery, such as through FIUs, and add value to current investigations on foreign bribery. It is checked whether FIUs have enough resources to effectively detect the laundering of the proceeds of foreign bribery, FIUs have access to relevant information and are involved in interdisciplinary cooperation.

[11] FATF, Professional Money Laundering, July 2018, Egmont, Professional Money Laundering Facilitators, July 2019.

These companies are often located at "postbox addresses" where numerous companies have their head office. Domiciling companies in business centres may not be illegal[12], this practice is problematic given the industry in which most of the companies work.

Analysis of these files shows that the assistance provided by intermediaries such as accounting and legal professionals can take many forms: assistance with setting up companies, developing a financial plan, setting up companies, paying start-up costs, registration with the Crossroads Bank for Enterprises and the VAT authorities, preparing balance sheets, payslips and VAT documents, providing a head office, offices, a commercial, administrative or postal address.

All of these elements show that the professionals involved make their knowledge available to various criminal networks. These files were disseminated to the judicial authorities primarily because of organised crime, social fraud and/or serious fiscal fraud.

b. Offsetting schemes using intermediary companies led by professional money launderers

Trends identified

When the offsetting technique is used criminals who have cash proceeds of their illegal activities and criminals who need cash to finance their illegal activities find one another. The first group hands over the cash to a second group, they then –using fake invoices– transfer similar amounts to accounts provided by the first group. This methods prevents the most suspicious transactions, i.e. the one in cash, from taking placing through the official banking system.

Many files feature companies that operate in various sectors (construction industry, industrial cleaning, transport, packaging, meat industry,…) and need a lot of cash to pay their illegal workers. CTIF-CFI's analysis suggests that these companies work together with companies in various sectors with large amounts of cash, in particular after selling merchandise on the illegal market. The cash is handed over to the managers in need of cash, they subsequently carry out bank transfers as part of the offsetting scheme.

The transfers are carried out to Belgian or foreign companies (with an account in the EU or elsewhere, in particular in Asia) operating in a variety of sectors or trades (consumer goods, hospitality industry, telecom, trade in vehicles, international payments…).

These transfers usually contain vague references regarding the purchase of goods or the payment of invoices. The different sectors seem to indicate that the financial transactions on these accounts are based on fictitious services.

A recent trend shows that professional money launderers are increasingly used by different parties of the system. They set up companies that operate as money laundering platforms. These companies make cash available to criminals in need of cash and also transfer money to criminals who want to dispose of cash. These laundering companies enable the simultaneous laundering of proceeds of various types of predicate offences.

The transfers by these laundering platforms are often intended for wholesalers in consumer products or import or export companies. These funds can be used to pay for various types of merchandise for criminals that had handed over their cash. The merchandise is then sold as part of Trade-Based Money Laundering (TBML). With this technique the possibilities and the legitimacy of (international) trade are misused to conceal illegal funds by using international commercial transactions.

[12] Brussels (11th Chamber), 12 September 2018, *Rev. dr. pén. entr*., 2019/2, page 125.

Apart from flows to Asia CTIF-CFI also identified links with the United Arab Emirates, in particular in files featuring intermediary companies operating as offsetting platforms located in Dubai.

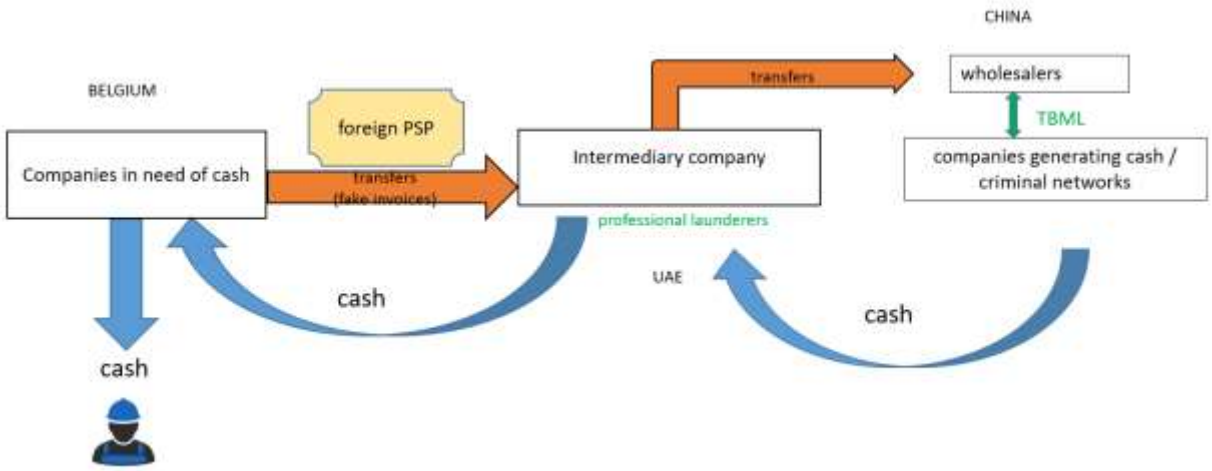
Case: use of an offsetting platform established in Dubai with financial flows to Asia and TBML practices

A company established in Dubai as a *Free Zone Establishment* (FZE) held an account with a payment service provider established in Eastern Europe. Over the period of a few months' time this account received transfers for a total amount of several million EUR. These transfers mainly referred to invoices / services from multiple Belgian companies officially operating in the construction industry and the industrial cleaning industry. The main debit transactions on this account were transfers to wholesalers in consumer goods established abroad, especially in Asia.

Analysis shows that most of the companies involved in the credit transactions featured in files disseminated to the judicial authorities in the framework of so-called Brazilian networks. Mr X, the director of the FZE also featured in a file disseminated to the judicial authorities because of organised crime and/or serious fiscal fraud and/or social fraud. Information obtained from a foreign FIU showed that Mr X was known to be a member of a criminal organisation. He transferred criminal money in order to inject it into the Belgian financial system. Moreover, Mr X was an accountant.

Given all of these elements the FZE seems to be an intermediary company operating as a money laundering platform in an international offsetting scheme. This company centralises part of the funds from the so-called Brazilian network from Belgium and then transfers these funds to wholesalers of Asian consumer products. In Asia these transfers can then be used to pay for all types of goods for companies which generated the cash handed over to the construction companies or industrial cleaning companies. Mr X was at the basis of this system and he laundered money for third parties.

By using a foreign payment service provider (PSP) the Belgian front companies were identified very quickly by the traditional Belgian financial actors because the transfers by these companies went to an Eastern European country, which is a less alarming indication than an account in Asia[13].



[13] Also refer to 1.2.3. infra on the use of payment service providers (PSPs).

Action taken

a. Cooperation between CTIF-CFI and the commercial court

The President of the French-speaking commercial court of Brussels decided to tackle dormant companies / front companies. The aim is to neutralise these shell companies as soon as possible to avoid them being used for money laundering purposes by criminal networks. Several authorities (Public Prosecutor's Office, National Social Security Office, tax authorities) take part in this project.

CTIF-CFI has valuable information that facilitates the identification of problematic companies. At the end of 2019 CTIF-CFI met the President of the French-speaking commercial court of Brussels and the financial section of the Public Prosecutor's Office to discuss the best possible cooperation in accordance with CTIF-CFI's legal framework in order to strengthen the fight against dormant companies.

b. Awareness-raising of obliged entities

Elements indicating the use of shell companies should attract the attention of obliged entities and raise suspicions. To avoid that obliged entities would be used for illegal purposes, it should be reiterated that due diligence measures should be based on an individual AML/CFT risk assessment, taking into account the characteristics of the customer and the business relationship or the transaction involved.

CTIF-CFI drafted a list of warning signs[14] to which obliged entities should pay particular attention. This is a non-exhaustive list of potentially suspicious elements. These criteria are examples that each obliged entity should assess, in order to determine whether there are suspicions of money laundering or terrorist financing. An analysis based on a range of criteria could, where appropriate, result in a disclosure.

As part of the close cooperation between CTIF-CFI and the supervisory authorities, as laid down in the Law of 18 September 2017, CTIF-CFI focussed the attention of several supervisory authorities of accounting and legal professions on the use of shell companies. The aim was for these authorities to set up awareness-raising actions.

The awareness-raising consists of reminding these groups of professionals of their due diligence obligations as part of AML/CFT prevention, such as assessing the customer's characteristics and the aim and the nature of the intended business relationship.

When one of the accounting or legal professionals is asked to set up a whole series companies in succession that have the profile of a shell company and, where applicable, to do the bookkeeping of these companies, they must identify the customers with a high money laundering risk as quickly as possible and apply enhanced due diligence to these customers.

In case they cannot meet their due diligence requirements these professionals may not engage in these business relationships and they must terminate any existing business relationships. They must also verify whether the reasons leading them to not being able to fulfil their due diligence requirements result in AML/CFT suspicions and whether these suspicions should be disclosed to CTIF-CFI.

c. The cooperation between CTIF-CFI and customs

Several files indicate that the offsetting technique is often used together with TBML practices related to wholesalers (in Europe or elsewhere around the world). The funds that are offset in Asia can be used to purchase a range of goods for criminals conducting illegal activities generating cash. These goods can ultimately be sold to criminals through import and export activities.

[14] The list of warning signs is available on CTIF-CFI's website.

Because there are customs aspects related to international commercial practices, one of the aims to strengthen the fight against TBML is to combine the financial information at CTIF-CFI's disposal with the custom authorities' information on international trade.

d. International cooperation

The use of TBML practices is a trend that is also identified internationally. The FATF and the Egmont Group decided to study this topic. A special working group was set up and CTIF-CFI is a member of this working group. Work has started and the final report should be available in the course of 2020. The results of this work will provide an international insight into this issue.

As part of the information exchange CTIF-CFI set up a new mechanism based on a strategic-operational report on the offsetting technique in order to send this report to foreign counterparts. This issue identified in Belgium has international consequences that need to be investigated. The aim of this report is twofold. Strategically, knowledge is shared by presenting files related to so-called Brazilian networks. Operationally, operational information is shared on files with a link to a foreign country, resulting in a more complete picture.

1.2.2. Use of games of chance

Trends identified

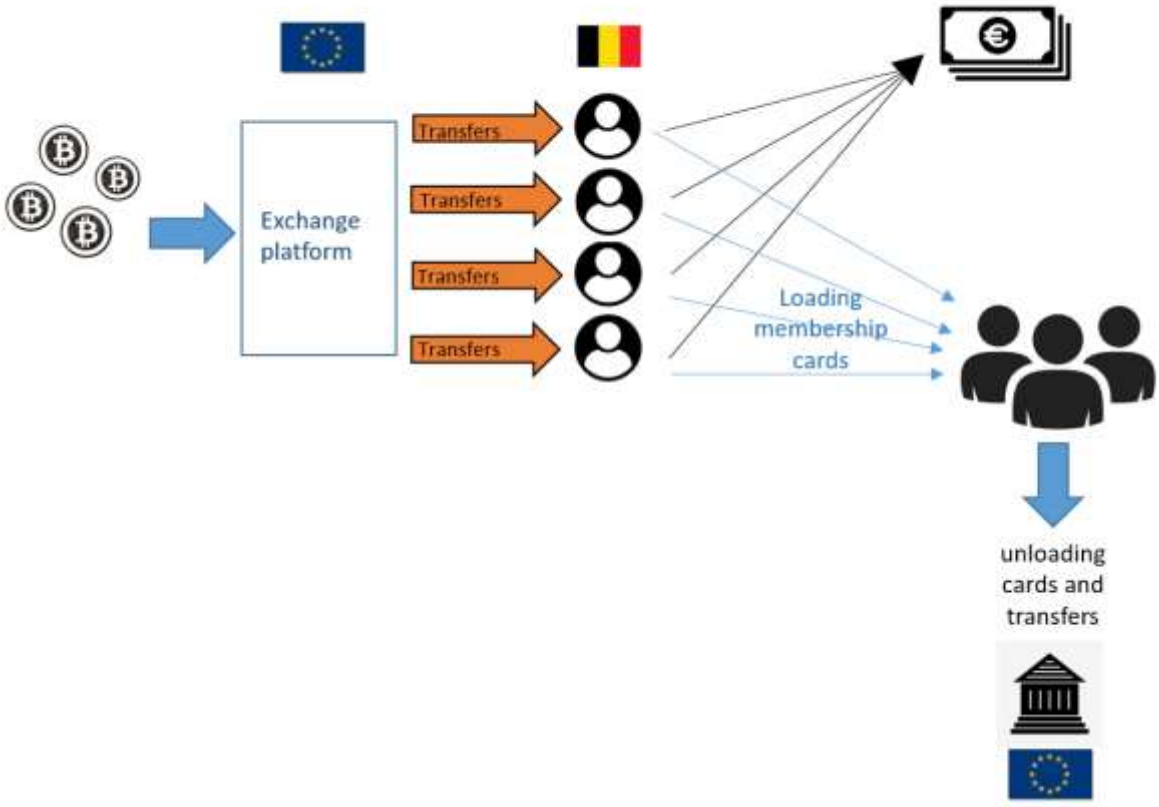
Files involving games of chance, offline as well as online, show that games of chance are generally part of larger money laundering schemes using other channels and techniques, in Belgium as well as abroad.

Some files revealed risks related to the rules for the use of players' accounts. A third party can also transfer money to a player's account. Transfers from one account to another are possible, without the account holder receiving the money necessarily being the same as the one initially used for the transfer. Moreover, there are risks related to the use of new payment methods such as virtual assets and the use of prepaid cards that can be used to transfer money to bank accounts. These prepaid cards can be used anonymously or for exchanging sums that were originally held in cash. Lastly, membership cards of gaming establishments can also entail money laundering risks.

Case: Money transferred abroad through a gaming establishment by money mules for the benefit of a criminal organisation

Individuals residing abroad opened several accounts with the same Belgian bank during the same period of time. The funds originated from a platform for exchanging virtual currencies established abroad. The funds were first moved by several transfers between the accounts of the various individuals involved. They were subsequently withdrawn in cash and/or transferred to membership accounts linked to player accounts with a gaming establishment in Belgium.

By linking these individuals to individuals abroad analysis by CTIF-CFI revealed a network of mules. These mules seemingly worked for these foreign individuals. Information from the gaming establishment showed that the membership cards mentioned the name of these foreign individuals even though they were loaded using bank cards linked to bank accounts held by mules. The money was taken off the membership cards and the funds were moved abroad to accounts of these foreign individuals. Information from a counterpart FIU showed that the individuals were part of a criminal organisation known for drug trafficking. This organisation wanted to launder the proceeds of drug trafficking via network of mules through the bank, which did not know the origin of the funds, and through a gaming establishment, which did not know the destination of the funds.



Although the use of games of chance is a tried and tested money laundering method, several files show that the gaming sector can have a particular appeal to certain criminals. In these cases it seems that criminals did not focus on laundering funds of illicit origin but wanted to gamble and even gamble away part of these funds. This preference for gambling offers a good investigative lead for CTIF-CFI. Thanks to information from the gaming establishments on the identity of their players CTIF-CFI was able to identify the economic beneficiary of the money laundering transactions.

Case: Identification of the actual economic beneficiary thanks to transactions carried out at a gaming establishment

The accounts of a recently established construction company received transfers from numerous Belgian construction companies, for a total amount of more than EUR 1 million. Some of these funds were subsequently laundered using the offsetting technique[15]. Another part of the funds on the accounts was used for considerable expenditure in gaming establishments.

Verification showed that the company's manger had not visited these gaming establishments when the money was spent. So a third party would have used the company's bank card. This seems to indicate that the manager is a front man who was designated as the company manager to conceal the identity of the actual manager of the company, the actual economic beneficiary of the transactions.

The financial transactions identified on the company's accounts were presumably based on fictitious services and were linked to laundering the proceeds of social fraud and/or serious fiscal fraud.

[15] See above.

Action taken

a. Awareness-raising of obliged professions

Since the objective part of gaming establishments' obligation to disclose[16] was repealed they must now only base themselves on their subjective assessment of the transactions they are confronted with to assess whether a disclosure to CTIF-CFI is required. We reiterate that online as well as offline games of chance are subject to the law.

It is sometimes said that the sector of online gaming, which expanded considerably in recent years[17], is not really exposed to money laundering because transactions can be traced. However, as mentioned above, bank accounts can receive funds through payment methods that can be used anonymously. Some risks relate to special characteristics of sectors linked to establishing a business relationship remotely. There are other challenges due to the cross-border nature of online gaming when these games are provided by gaming establishments subject to rules in other countries or to subject to less strict AML/CFT rules. This can lead to problems in terms of cooperation between various authorities, which are then misused by criminals.

The potential of disclosures by the gaming sector is generally underused because certain elements related to a player's behaviour and a player's use of money should get even more attention from the sector.

To raise awareness of potentially suspicious elements CTIF-CFI drafted a list of warning signs[18] to which obliged entities should pay particular attention. This is a non-exhaustive list of examples for each obliged entity to assess whether there are suspicions of money laundering or terrorist financing.

1.2.3. Use of payment service providers (PSPs)

Trends identified

CTIF-CFI found that in 2019 disclosures by payment service providers and electronic money providers increased by more than 65% compared to 2018. This increase in the number of disclosures is a result of the arrival of new entities that became subject to the AML/CFT law in 2019.

As anticipated by CTIF-CFI and mentioned in the previous annual report the prospect of Brexit has made numerous payment service providers and providers of electronic money to move their registered office from the United Kingdom to continental Europe. Because of the move of these financial institutions, new entities arrived in Belgium, leading to an increased number of cases. It should be noted, however, that although CTIF-CFI receives an increased number of cases from these obliged entities, the reporting activity of these payment service providers and providers of electronic money can be considered to be low.

Analysis of the disclosures has also shown that criminal and terrorist groups increasingly use these payment service providers and providers of electronic money to move funds. CTIF-CFI finds that Belgian and foreign payment service providers and providers of electronic money are used to make financial transactions less transparent. By using one or more payment service providers or providers of electronic money criminals can make it more difficult to trace financial flows. Using payment service providers and providers of electronic money also enable fractioning of suspicious financial transactions, which

[16] The aforementioned Royal Decree of 6 May 1999 was explicitly repealed at the end of 2018 although it was established when the Law of 6 May 1999 came into force that gaming establishments were no longer required to automatically disclose transactions that meet the criteria of the Royal Decree of 6 May 1999.
[17] The online gambling market experienced an annual growth of more than 80% between 2012 and 2015, C. ANTONELLI, *Le marché du jeu en Belgique. Quelques données chiffrées*, *Droit des jeux de hasard*, dir. D. PHILIPPE, G. SCHAMPS and A. STROWEL, Brussels, Larcier, 2018, page 11 ff., in particular page 12.
[18] The list of warning signs is available on CTIF-CFI's website.

complicates the task of financial intelligence units. Access to information held by these foreign payment service providers and providers of electronic money can be difficult, in particular when this is part of the freedom to provide services in Belgium.

As stated before, CTIF-CFI identified the construction industry as a high-risk sector with regard to money laundering as a result of repeated findings of money laundering facts linked to this sector. To launder the proceeds of illegal activities in the construction industry criminals groups use Trade-Based Money Laundering (TBML) techniques by purchasing goods from Asian wholesalers. The traditional banking system has become more vigilant, has developed warning and detection systems and can identify quickly. To avoid detection professional money launderers now use payment service providers and providers of electronic money to carry out their transactions[19].

Action taken

In 2019, the importance of the use of payment service providers and providers of electronic money in ML/TF channels was recognised. CTIF-CFI has undertaken action to mitigate the risks of these payment service providers and providers of electronic money and the exposure of the Belgian financial system to these risks. In 2020 it will become clear whether the projects launched by CTIF-CFI enable effective supervision and good understanding of the ML/TF risks in Belgium of these payment service providers and providers of electronic money.

a. *New procedure for providing information*

In many disclosures in Belgium submitted by providers established in Belgium and subject to Belgian regulations and that provide their services in the European Union based on the freedom to provide services in the European Union there are no direct links to Belgium. One example was a disclosure sent by a payment service provider established in Belgium presumably linked to fraud committed by a Spanish national to the prejudice of an individual in Germany.

To enable CTIF-CFI to disseminate information quickly and effectively to European counterparts a new procedure was introduced via FIU.Net, called the dissemination of cross-border reports (XBR). Thanks to this new procedure, which is now used by all FIUs of the European Member States, upon receipt of information CTIF-CFI can share this information with the European counterpart involved, which can then process this information and take action if necessary. In the example above, based on the new procedure, immediately upon receipt CTIF-CFI will send the information to their Spanish and German counterparts, which are in a better position to take measures to combat this issue.

b. Signing of an MOU between CTIF-CFI and the National Bank

One of the actions taken was signing a Memorandum of Understanding with the National Bank of Belgium on 17 September 2019. It enables CTIF-CFI to provide all information that can have significant consequences for the reputation of a financial institution or the financial sector as a whole, in particular with regard to the reporting activity or compliance with AML/CFT obligations. This MOU is a formal framework for closer cooperation between CTIF-CFI and the NBB applicable since the Law of 18 September 2017 came into force, aimed at making this cooperation more effective.

c. Internal awareness-raising and contacts with new disclosing entities

CTIF-CFI also launched an awareness-raising campaign for CTIF-CFI's analysts on the risks of payment service providers and providers of electronic money with regard to AML/CFT. This awareness-raising was a success, resulting in an increased number of requests sent by CTIF-CFI to payment service

[19] This trend is illustrated above in the case on the use of an offsetting platform established in Dubai with flows to Asia and TBML practices.

providers and providers of electronic money in Belgium and to its foreign counterparts for payment service providers and providers of electronic money established abroad.

New disclosing entities that were previously subject to regulation in the United Kingdom were contacted, explaining CTIF-CFI's procedures and further details were provided on the specific features of the Belgian AML/CFT system and the potential differences of the frameworks in the other countries to which these entities were subject.

Finally, CTIF-CFI also took part in the Black Wallet project[20], aimed at identifying the AML/CFT risks of the fintech sector.

1.2.4. Use of crypto assets

Trends identified

As a reminder, the fifth AML Directive requires European Member States to subject providers for exchanging virtual currencies and custodian wallet providers to the AML/CFT system, which will be the case when this Directive is transposed into Belgian law. As these entities were not subject to Belgian regulations nor to the Belgian AML/CFT framework in 2019, CTIF-CFI did not receive any disclosures from these entities.

In 2019 CTIF-CFI's experience regarding money laundering related to crypto assets was based on files opened based on suspicions of other disclosing entities related to suspicious transactions involving crypto assets. The information received mainly came from financial institutions. Following spontaneous exchange of information from foreign FIUs CTIF-CFI also received information as a result of disclosures by a foreign platform.

Establishing a legal framework will enable CTIF-CFI to receive disclosures from these entities, ask them questions and obtain more information for its investigations.

Given the specific characteristics of the sector of crypto assets and its evolution, CTIF-CFI will continue to develop its expertise in this regard and pay particular attention to the ML/TF risks of crypto assets.

CTIF-CFI also wants to strengthen its cooperation with the FSMA, designated as the supervisory authority for these entities that will be subject to regulation in the future.

[20] For more information on the project please refer to:
https://www.poliisi.fi/en/national_bureau_of_investigation/black_wallet.

2. Terrorist financing trends

Trends identified

In 2019, CTIF-CFI disseminated a total of 55 files to the judicial authorities related to terrorist financing. The total amount of these disseminations was EUR 4,5 million. The number of files is not as high as in 2015, 2016 and especially 2017, a positive trend that seems to be confirmed by partner services and seems to be linked to the decline of IS. The absolute value of an amount involved in a file is less relevant in a file related to terrorist financing. It has regrettably been demonstrated in the past that large amounts are not required to finance an attack or a terrorist group. Often a transaction –albeit small– can be used here to demonstrate the link between different people.

Apart from disseminating files to the judicial authorities because of serious indications of terrorist financing in 2019, CTIF-CFI again used the possibility laid down in Article 83, §2, 4° of the Law of 18 September 2017 in a large number of cases. This Article makes it possible, as part of the fight against the radicalisation process, to disseminate relevant information to the intelligence services (VSSE and ADIV-SGRS) and to OCAM-OCAD, also when no serious indications of terrorist financing have been identified. In 2019, CTIF-CFI used this possibility on 162 occasions. Apart from cooperation with the Public Prosecution and the police, this cooperation with the intelligence services and OCAM-OCAD is also very important to CTIF-CFI, in particular in a period when the imminent terrorist threat is not as high.

CTIF-CFI also has writing obligation for the Common Database. This is a database managed by OCAM-OCAD and the police, aimed at sharing knowledge between various departments to protect society against potentially violent people or groups linked to radicalism and terrorism. When CTIF-CFI has relevant information on people in this database (terrorists, hate preachers, potential terrorists,…), this information is entered into the database. In 2019, CTIF-CFI fulfilled its writing obligation on 102 occasions.

In the files disseminated to the judicial authorities due to serious indications of terrorist financing two trends can be identified. A first trend, which also emerged in the last two years, relates to so-called collectors. A second trend is CTIF-CFI's focus on domestic and foreign associations in which a large number of private individuals sent small donations and the money was (partly) used for terrorist financing and/or radicalism.

a. The issue of collectors

Collectors are financial intermediaries who are usually located in Syria's neighbouring countries. They can use a network to get money –received through money remittance from abroad– in cash to beneficiaries. Initially this partly informal system for money remittance was used to support Foreign Terrorist Fighters (FTFs) in conflict areas. The last two years the funds mainly seem to be intended to facilitate a possible return. It is an organised money remittance system in which collectors are regularly changed to avoid detection and money is sent from various countries around the globe.

b. Issue of Dutch foundations

A second important trend that has been identified for a number of years are the many transfers from Belgium to domestic and foreign foundations. As a result of enhanced cooperation with our Dutch counterpart many of CTIF-CFI's analyses examined Dutch foundations that could be linked to terrorism and are known for their role in the radicalisation process. Numerous small amounts are transferred by Belgians who are also known to the police or intelligence services as radical individuals. These investigations are a fine example of the usefulness of financial intelligence when conducting network analysis. By following a financial flow to an association / foundation and then checking which other individuals also send money to this association / foundation, a large part of its financing network can be revealed. Moreover, it became clear that a number of Belgians featuring in terrorist investigations also sent money to several associations / foundations.

It should be noted that these associations are mainly supported in cash, without using the traditional banking system, making detection impossible.

c. Other issues related to terrorist financing

Apart from religious terrorism, politically inspired terrorism is an increasing threat to society according to the police and intelligence services. In recent years CTIF-CFI received disclosures relating to left-wing extremism as well as right-wing extremism. Cooperation with intelligence services on this topic is crucial to be able to assess whether extremist organisations or individuals could commit violent acts and whether their financial transactions should be considered as potential terrorist financing. In 2019, CTIF-CFI dealt with a limited number of files on this issue. The cooperation with counterpart FIUs was also of great importance.

The files with the largest amounts disseminated to the judicial authorities in 2019 time and again illustrated the fine line between potential terrorist financing and laundering the proceeds of organised crime. Organisations may have a political aim, but also have an organised network of companies at their disposal to launder money from extortion, drug trafficking, social fraud and other types of crime, and de facto act like a criminal organisation. Numerous files were disseminated to the Public Prosecutor's Office indicating that construction companies located abroad generated large amounts from fiscal and social fraud. The money was moved through Belgian corporate accounts of domestic and foreign construction companies to accounts of companies established in different European countries. These companies were building and developing a propaganda machine of a terrorist organisation.

Finally, in 2019 CTIF-CFI once again also processed several files in which money was transferred to prisoners sentenced for terrorism-related offences. The existing mechanisms for cooperation with the Directorate General for Prisons [*Direction Générale des Établissements pénitentiaires*] (DG EPI)] of the Federal Public Service Justice and with the police, intelligence services and OCAM-OCAD were fully utilised to further investigate these transactions.

Action taken

a. Cooperation with partner countries on the issue of "collectors"

For these files CTIF-CFI worked closely with the French FIU TRACFIN, as the FIU of our neighbouring country France, one of the main foreign partners in the fight against terrorist financing. Information was exchanged mutually and as a result several beneficiaries of money remittance were able to be identified as collectors. This was particularly the case when no direct link, such as a family link or police information link, could be established between the ordering party and the FTF. Moreover it should be noted that since the fall of Baghuz, the last ISIL stronghold, there was a resurgence of money remittance to collectors. The money does seem to be ultimately intended for FTFs in prisoner camps.

CTIF-CFI sends a continually updated list of money collectors identified as part of its analyses to partner FIUs.

b. Cooperation between CTIF-CFI and FIU Netherlands related to the issue of Dutch foundations

To be able to adequately respond to the issue of Dutch foundations CTIF-CFI organised several meetings in 2018 with the Dutch FIU. According to our Dutch colleagues the threshold for setting up a foundation is low, which could possibly explain why this type of organisation is so popular in radical religious communities. The attention in Belgium for the terrorist financing risk through non-profit organisations in 2016 possibly also resulted in financial support for radical and salafist organisations ending up with Dutch foundations.

c. Cooperation between CTIF-CFI and domestic and international partner bodies

Cooperation with domestic and international partner bodies will continue to be one of the cornerstones of CTIF-CFI's policy on the fight against terrorist financing. To be able to play a proactive role and assess the terrorist threat, information from CTIF-CFI's partners is of vital importance. Conversely, financial information that CTIF-CFI receives from different types of disclosing entities can clearly provide added value for intelligence and investigative proceedings. This integrated approach is the best way to correctly assess future trends with regard to terrorism and terrorist financing.

V. DRAFT LEGISLATION TRANSPOSING THE FIFTH AML/CFT DIRECTIVE: OVERVIEW OF THE MAIN CHANGES

The European Union has substantially strengthened its legal framework for preventing money laundering and terrorist financing (hereinafter "ML/TF") in recent years.

The fourth anti-money laundering Directive[21] was adopted in May 2015 and was transposed into Belgian law by the Law of 18 September 2017 on the prevention of money laundering and terrorist financing and on the restriction of the use of cash ("hereinafter "the Law of 18 September 2017").

As part of the Action Plan[22] presented in February 2016 for strengthening the fight against terrorist financing and in response to the revelations in the Panama Papers of April 2016, the fifth anti-money laundering Directive[23] was adopted in May 2018, which needed to be transposed into national law by January 2020.

The fifth Directive mainly ensures more transparent information on the ultimate beneficiaries, gives financial intelligence units (FIUs) more access to information, intensifies the cooperation between supervisory authorities and regulates virtual assets and prepaid card to better prevent terrorist financing. We will elaborate on this below.

The work for transposing the fifth Directive by the Working group for the transposition of the fifth Directive, under the auspices and coordinated by the Federal Public Service Finance, was finalised. The legislative work for the parliamentary approval of the draft transposition law had just started at the time of publication of this annual report.

Subject to any changes that could arise, in particular from the Council of State or members of parliament, we can already provide an overview of the main changes to the Law of 18 September 2017.

A. Extension of the scope *ratione personae*

The list of entities subject to the Law of 18 September 2017 will be extended to include:

- *providers of exchange services between virtual currencies and fiat currencies established in Belgium, and custodian wallet providers established in Belgium.*

Until the fifth Directive came into force, providers of exchange services between virtual currencies and fiat currencies[24] and custodian wallet providers were not required to identify suspicious transactions. So terrorist groups were able to move money within the financial system of the European Union or within virtual currency networks by concealing transfers, due to the certain degree of anonymity available on these platforms. So it was essential to extend the scope of the fourth Directive to providers of exchange services between virtual currencies as well as fiat currencies and custodian wallet providers.

Virtual currencies are defined as a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does

[21] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (OJ L 141 of 5 June 2015, page 73).
[22] COM(2016) 50 final
[23] Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU (OJ L 156 of 19 June 2018, page 43).
[24] Fiat currency: coins and banknotes that are designated as legal tender and electronic money, of a country, accepted as a medium of exchange in the issuing country.

not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically.

A custodian wallet provider is defined as an entity that provides services to safeguard private cryptographic keys on behalf of its customers, to hold, store and transfer virtual currencies.

The FSMA is designated as their supervisory authority. The King shall, upon advice of the FSMA, determine the rules and conditions for their registration with the FSMA.

- Natural or legal persons purchasing, selling or acting as intermediaries in the trade in works or art or moveable property of more than fifty years old, when the sales price of one or an entity of these works or goods is equal or greater than EUR 10 000. The intermediaries include art galleries, auction houses and organisers of fairs and exhibitions.

The term work of art is not defined in the fifth Directive. The term used in the draft law is the one as defined in Article XI.175, § 1, second subparagraph, of the Code of Economic Law. Pursuant to this Article, an original work of art is "a work of graphic or plastic art such as images, collages, paintings, engravings, prints, lithographs, sculptures, tapestries, glassware and photos, provided that this work is the creation of the artist himself, or a specimen regarded as an original work of art. Copies of works of art in this section and that have been created by the artist himself or by his order in limited edition, are considered to be original works of art in the sense of this section. As a rule such copies are numbered, signed or marked as authentic by the artist."

The reason for the draft law also applying to old goods, which are characterised as antiquities in several legislations when they are 100 years old or older, or as cultural goods, is that some of these goods (such as zoological, botanical, archaeological objects, part of monuments that have not been preserved in their entirety, stamps, archives, musical instruments, etc.) are not works of art, but goods with a significant ML/TF risk, in particular antiquities stolen in the Middle East arriving in Europe.

The sector of the art trade is a high-risk sector with regard to ML/FT. The FT risk has increased sharply given the situation in Iraq and Syria, where museums and archaeological sites on UNESCO's world heritage list were affected by organised raids or illegal digging, thus contributing to the financing of terrorist organisations. Furthermore, the art trade, given the opaqueness of certain practices, is an important risk factor for money laundering and fraud.

- natural persons or legal persons owning or managing warehouses, including customs warehouses or warehouses located in free ports, that specifically provide a storage service for works of art or moveable property of more than fifty years old and only for such goods and works

Ratione personae, the scope of the Law of 18 September 2017 is extended to warehouses and customs warehouses, where works of art or goods of more than fifty years old are stored. Such warehouses entail certain risks similar to those of free ports, in particular with regard to long-term storage of works of art.

Free ports are added to the scope of the law to transpose Article 2, 1., 3), j) of the fourth Directive even though there are currently no free ports or free zones[25] in Belgium.

The Federal Public Service Economy is designated as their supervisory authority. Again the King, upon advice of the Federal Public Service Economy, shall determine the rules and conditions for registering with this authority.

[25] A free port is a free zone (originally a port, hence the name) where goods can be unloaded, processed, distributed and re-sent without custom supervision and free from duties and taxes (custom duties, VAT, etc.). Free ports create anonymity and tax exemptions for transactions and can be at the centre of different types of illegal trade, in particular plundered or stolen antiques.

It is necessary for these Royal Decrees to be applicable as soon as possible to ensure the effective implementation of the law. Prior identification of these new obliged entities, which were not regulated until now, is a *conditio sine qua non* for an effective implementation of the Law of 18 September 2017.

Firstly, this prior identification is necessary because for the FSMA and the Federal Public Service Economy to carry out their supervisory and sanctioning tasks in accordance with the Law of 18 September 2017 with regard to clearly identified entities. Secondly, this identification is necessary to ensure that CTIF-CFI receives a valid disclosure when it receives a disclosure from these entities pursuant to Article 47 of this Law. That is why a list of these professionals is required, identified on the basis of criteria determined by the King.

- *Natural or legal persons on the separate list of the public register as referred to in Article 29, § 2 of the aforementioned Law of 17 March 2019, committing to providing as their main economic or professional activity, directly or through other persons linked to him, material aid, assistance or advice related to tax matters*

In the field of taxation currently only the professional title of fiscal accountant or certified tax advisor are protected. Advice and assistance in the field of taxation and the representation of taxpayers is not restricted to a regulated profession.

As a result, anyone can provide tax-related advice as their main economic or professional activity.

The fifth Directive wanted to close this loophole that could lead to fiscal fraud and laundering related to this fraud with respect to the regulated professionals providing such advice and who are subject to the obligations of the Law of 18 September 2017.

As a result, every non-certified consultant / tax service provider will have to register with the Institute for Tax Advisors and Accountants (hereinafter "ITAA") to enable the ITAA to check and sanction AML compliance. The ITAA is designated as their supervisory authority.

B. Extension of the scope *ratione materiae*

Although the fifth Directive does not amend the predicate money laundering offences the draft legislation introduces the following changes:

- *illicit trafficking in narcotic drugs and psychotropic substances*

The term "illicit drug trafficking" referred to in Article 4, 23°, c) of the Law of 18 September 2017 is replaced by "illicit trafficking in narcotic drugs and psychotropic substances", as a result of the request by the European Commission in the reasoned opinion no. 2017/0516 sent to the Kingdom of Belgium pursuant to Article 258 of the Treaty on the Functioning of the European Union for non-communication of the measures for transposing the fourth Directive into national law.

Not only targeting illicit drug trafficking but also illicit trafficking in narcotic drugs and psychotropic substances ensures a formally more compliant transposition of Article 3, 4. b) of the fourth Directive, without any change in substance given that the criminal phenomenon of illicit drug trafficking as referred to in the Law of 18 September 2017 already covers all offences referred to in Article 3, paragraph 1, point, a) of the 1988 United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances without having to explicitly having to refer to this.

- *Computer crime*

The term "computer fraud" as a criminal activity, referred to in Article 4, 23°, bb) of the Law of 18 September 2017 will be replaced by the term "computer crime".

When the fourth Directive was transposed by the Law of 18 September 2017 computer fraud was added to the list of criminal activities. At present, it seems to be just as important to broaden the sometimes too narrow term "computer fraud" to the broader term "computer crime".

Computer crime often has an international dimension, perpetrators can act with a certain degree of anonymity and the criminal activity can take many forms (privacy breaches, espionage, sabotage, hacking, incitement to hatred or racism, paedophilia, fraud, or even cyberterrorism,…) Broadening the term computer fraud to computer crime (or "cybercrime") will make it possible to deal with new criminal phenomena that CTIF-CFI faces during its operational work of analysing disclosures.

C. Lower maximum transaction limits for some prepaid instruments

Prepaid cards for general use can be used legitimately and are an instrument that contributes to social and financial inclusion. However, anonymous prepaid cards can also easily be used to finance terrorist attacks and terrorist logistics.

To deprive terrorists from this instrument that could be used for financing their operations, the fifth Directive further lowered the limits and maximum amounts, below which obliged entities are allowed to waive certain customer due diligence measures established under the fourth Directive.

Article 25 of the Law of 18 September 2017 states the conditions under which obliged entities issuing electronic money, based on an appropriate assessment of the ML/TF risks demonstrating that these risks are low may deviate from their customer identification and verification obligations when issuing electronic money.

This article is amended as follows in accordance with these new limits:

- The maximum amount for payments per month is lowered from EUR 250 to EUR 150;
- The maximum amount that can be stored electronically is lowered to EUR 150;
- The amount above which repayment or cash withdrawal of the monetary value of the electronic money requires the identification and identification verification of the person involved, is lowered from EUR 100 to EUR 50.

- It is stated that the obligation to identify and verify the identity also applies to remote payment transactions (through the internet or initiated on a device that can be used for remote communication) in case the amount exceeds EUR 50.

Although the use of anonymous prepaid cards in the European Union is essentially limited to the territory of the Union, this is not always the case for similar cards issued in third countries. So it is important that anonymous prepaid cards issued outside the European Union can only be used in the Union when they are deemed to meet requirements similar to requirements laid down in European Union law.

Article 25 is amended to clarify that credit institutions and financial institutions providing a payment service consisting of the acceptance of payment transactions, will only accept payments with anonymous prepaid cards issued in third countries if these cards meet the requirements equivalent to those laid down in Article 25, as amended by the draft legislation.

D. Improved cooperation between FIUs and their direct access to AML/CFT information

The fifth Directive aims to strengthen the powers of the FIU, CTIF-CFI in Belgium, and facilitate the cooperation between FIUs.

The fifth Directive stresses the important role FIUs play in detecting financial transactions of terrorist networks. FIUs greatly contribute to the cross-border detection of financial transactions by these networks

and the financiers identified. Financial intelligence is essential to uncover assistance to terrorist offences, and networks and mechanisms of terrorist organisations.

Due to the lack of binding international standards there are big differences between FIUs with respect to their tasks, competences, powers and access to information. These differences are an impediment to the exchange of information and international cooperation between FIUs. The fifth Directive fully aligns these rules for FIUs' access to information to the FATF Recommendations revised in 2012, in particular with Recommendation 29 and its interpretative note on the competences and powers of FIUs, and with Recommendation 31 requiring countries to have effective mechanisms in place to identify, in a timely manner, whether natural or legal persons hold or control accounts and to also have mechanisms to identify assets without prior notification to the owner.

When carrying out their tasks all FIUs, in accordance with the FATF's Recommendation 29, FIUs should be able to obtain additional information from reporting entities, and should have access on a timely basis to the financial, administrative and law enforcement information required to undertake their functions properly.

In all cases of suspicions of criminality, in particular in cases of terrorist financing, the information must be transmitted directly and without undue delay between the reporting entities and FIUs, not indirectly or after they have obtained permission of a third party (this was still possible pursuant to Article 33.1, b) of the fourth Directive, prior to the amendment by the fifth Directive removing the possibility of providing information "indirectly" to the FIU.

The impediments to the access to information, the exchange and the use of information and operational cooperation between FIUs are listed in the EU FIU's Platform mapping report of 15 December 2016. It was therefore essential to increase the effectiveness and efficiency of FIUs by clarifying their competences and mutual cooperation at European level.

- Obtaining additional information without prior disclosure

FIUs must be able to obtain directly from each reporting entity, and not only from the one reporting a suspicious transaction, all necessary information related to their tasks. They must have free access to information. This is essential to ensure that financial flows can be traced appropriately and networks and illegal flows can be detected at an early stage.

The need for FIUs to obtain additional information from obliged entities based on a suspicion of money laundering or terrorist financing may arise from a previous disclosure of a suspicious transaction to the FIU, as well as subsequent elements such as an analysis of the disclosure by the FIU itself, information provided by competent authorities or information held by another FIU.

The possibility of asking additional questions in some Member States, as stated in the aforementioned EU FIU's Platform mapping report, is currently restricted due to the requirement of a prior disclosure of a suspicious transaction from the same obliged entity.

As part of their tasks FIUs must henceforth, pursuant to the new paragraph 9 of Article 32 of the fourth Directive, be able to obtain information from each obliged entity, even if this entity did not send a disclosure. This does not mean that any information can be requested from any reporting entity. The information requests must be based on sufficiently precise elements. An FIU must also be able to obtain information following a request from another FIU in the European Union and must be able to share this information with the FIU that is at the basis of the request.

Moreover, obliged entities must, pursuant to the new Article 33,1.b) of the fourth Directive, as in the past, cooperate fully with the FIU, by quickly and upon request providing all information required to carry out its task. However, to increase the effectiveness of this cooperation this information must be provided "directly" to the FIU, so not through indirect channels.

Given that CTIF-CFI already has these competences and prerogatives, specifically pursuant to Article 81 of the Law of 18 September 2017, it is no longer necessary to transpose the new subparagraph 9 of Article 32 of the new subparagraph 1, item b) of Article 33.

- Facilitating information exchange between FIUs

CTIF-CFI is tasked with compiling and analysing the information it receives to link suspicious transactions with predicate offences in order to prevent and combat ML/TF, and disseminating the result of its analyses and all other additional information to the competent authorities when there are reasons to suspect money laundering, related predicate offences and terrorist financing.

FIUs reported difficulties in exchanging information due to differences in the national definitions of certain predicate offences such as tax offences, which have not been harmonised under European Union law.

As a result, an FIU, pursuant to the updated Articles 53, paragraph 1, 55, paragraph 2 and 57 of the fourth Directive, will no longer be able to invoke the lack of the identification of a money laundering-related predicate offence, some specific characteristics of national criminal law provisions, differences between definitions of related predicate offences to refrain from or refuse, spontaneously or upon request, the exchange of information with another FIU. An FIU will also have to provide prior consent to another FIU to disseminate this information to the competent authorities, regardless of the type of the suspected related predicate offence, in order to ensure that the dissemination of the information takes place effectively.

All of these principles are included in the draft legislation.

- Direct access by FIUs and other competent authorities to information on the identity of holders of bank accounts, payment accounts and safe-deposit boxes

Delays in the access of FIUs and other competent authorities to information about the identity of holders of bank accounts, payment accounts and safe-deposit boxes, in particular when they are anonymous, are an impediment at European level for the detection of transfers of funds related to terrorism.

In accordance with the old recital 57 of the fourth Directive, Member States were encouraged to put in place systems of banking registries or electronic data retrieval systems that would provide FIUs with access to information on bank accounts. Although such mechanisms were introduced in a number of Member States, there was no obligation at EU level to do so.

Due to a lack of such a centralised system, FIUs must send requests to all banks of the country when they need information on a bank account. This is a cumbersome process for banks as well as for the FIU involved and may lead to problems related to data confidentiality. As not all Member States had mechanisms in place enabling FIUs' timely access to information on the identity of holders or bank accounts or payment accounts, some FIUs were hampered in detecting criminal or terrorist financial flows at national level. Furthermore, the FIUs involved were not able to exchange such information with their EU counterparts or those established in third countries, which hampers cross-border preventive action.

In the Council conclusions on the fight against the financing of terrorism of 12 February 2016 the Council of the European Union underlined the importance of achieving rapid progress on legislative actions identified by the Commission, in particular the strengthening of the access to information, such as access to bank and payment account information by FIUs.

The new article 32*bis* of the Fourth Directive therefore requires all Member States to put in place centralised automated mechanisms, such as central registries or central electronic data retrieval systems, allowing that effective and timely access to information on the identity of the holders of bank accounts, payment accounts and safe-deposit boxes, their proxy holders and beneficial owners can be obtained.

National FIUs shall have immediate unfiltered access to the information under investigation.

In Belgium, the Central Point of Contact (CPC) of accounts and financial contracts, established within the National Bank of Belgium (NBB) pursuant to the Law of 14 April 2011 on various provisions, is the main instrument taking on the role of such centralised automated mechanism.

To meet the requirements of the fifth Directive, the Law of 8 July 2018 on the organisation of a central contact point for accounts and financial contracts and on extending access to the central file of notices of seizure, delegation, transfer, collective settlement of debts and recourse created a completely new legal framework for the CPC (Article 2 to 13). As a result, no further transposition was required for the draft legislation.

By 26 June 2020 the European Commission needs to submit a report to the European Parliament and to the Council on assessing the conditions and the technical specifications and procedures for ensuring the safe and efficient interconnection of the central automated mechanisms. Where appropriate, this report shall be accompanied by a legislative proposal.

- Direct access of FIUs and other competent authorities to land registry data

In accordance with FATF Recommendation 31, the new Article 32*ter* of the Fourth Directive states: "Member States shall provide FIUs and competent authorities with access to information which allows the identification in a timely manner of any natural or legal persons owning real estate, including through registers or electronic data retrieval systems where such registers or systems are available."

CTIF-CFI already has electronic access to land registry data held by the Federal Public Service Finance for their tasks of combating ML/FT, as a result of the discussion by the sectoral committee for the federal government of 3 May 2018 (discussion federal government nr. 18/2018 of 3 May 2018). Given the new Article 32*ter* access by CTIF-CFI and the supervisory authorities, referred to in Article 85 of the Law of 18 September 2017, to the information held by the General Administration Patrimonial Documentation of the Federal Public Service Finance is legally enshrined in a legal provision transposing Article 32*ter* into the current draft law.

Access to the information held in the land registry with regard to persons featuring in a disclosure of suspicions of ML/TF makes it possible to confirm or refute whether the serious indications of ML/TF originate from trafficking in human beings (slum landlords) or to confirm or deny the statement of a person claiming that his income originates from the sale of buildings, or determine a person's property portfolio with a view to seizing the property.

E. Clarifying and improving the access to information on beneficial owners

Article 30 and 31 of the fourth Directive already included rules on collecting, saving and accessing information on the beneficial owner(s) of companies, trusts and other types of arrangements.

Such entities are currently obliged to keep accurate information on their beneficial owners. A central register of beneficial owners (UBO register) held with the General Administration of Treasury of the Federal Public Service Finance was created pursuant to Article 73 ff. of the Law of 18 September 2017.

Pursuant to Article 30 of the fourth Directive all competent authorities, including FIUs, could already – without any restrictions– and obliged entities as part of customer due diligence measures have access to the information on beneficial owners of companies established in their country and other legal entities. However, any other person or organisation had to demonstrate a legitimate interest to have access to information on the beneficial owners of aforementioned companies and other legal entities. This changed with the fifth Directive given that the access to information on the beneficial owners is made publicly available.

The fifth Directive also introduces a number of necessary clarifications for applying Article 31 related to trusts and other legal arrangements such as *fiducie*, some types of *Treuhand* or *fideicomiso*.

In accordance with Article 31 of the fourth Directive, Member States shall require that trusts "governed under their law" obtain and hold adequate, accurate and up-to-date information on the trustee in particular. The same Article required Member States to set up a national central register of beneficial owners of trusts "with fiscal consequences".

These criteria with regard to "applicable law" and "fiscal consequences" were not interpreted uniformly. As a result, when a Member State did not recognise trusts under its law, there was no obligation for monitoring and registration of trusts managed in that Member State. The limitation of the registration requirement for trusts with fiscal consequences was not consistent with a more comprehensive obligation by the fourth Directive to identify all types of trusts prior to establishing a business relationship.

The fifth Directive clarifies which specific factor is used to determine which Member State is responsible for monitoring and registering the information on the beneficial owners of trusts and similar legal arrangements.

The information on the beneficial owner of express trusts and similar legal arrangements needs to be kept in the UBO register of the Member State where the trust's trustee or the person with a similar position in a similar legal arrangement is established or resides.

If the place of establishment or place of the residence of the trust's trustee or the person with a similar position in a similar legal arrangement is located outside of the European Union, the information on the beneficial owner shall be kept in the UBO register of the Member State where the trust's trustee or the person with a similar position in a similar legal arrangement establishes a business relationship or acquires property in name of the trust or the similar legal arrangement.

When the trust's trustees or the persons with a similar position in a similar legal arrangement are established in or reside in various Member States or in case the trust's trustee or the person with a similar position in a similar legal arrangement establishes several business relationships in several Member States in name of the trust or the similar legal arrangement, the proof of registration or an excerpt of the information on the beneficial owner kept by one Member State in a UBO register can be deemed sufficient to assume that the registration obligation is fulfilled.

Each Member State requires that trustees of an express trust governed in that Member State obtain and hold adequate, accurate and up-to-date information on the beneficial owners of the trust.

Access to information on the beneficial owners of trusts and similar legal arrangements is not granted to every citizen but only to those that can demonstrate a legitimate interest and those that submit a written request with regard to a trust or similar legal arrangement with a controlling interest in a company or another legal entity.

The transposition of these obligations was no longer necessary by this draft law as these were already implemented by the Royal Decree of 30 July 2018 on the operating procedures of the UBO register.

Interconnecting the national UBO registers as laid down in the fifth Directive by means of the European Central Platform, set up under Article 22, subparagraph 1, of Directive (EU) 2017/1132 of the European Parliament and of the Council of 14 June 2017 relating to certain aspects of company law will enable access to this information in the entire territory of the European Union. The European Commission must ensure this interconnection by 10 March 2021 at the latest.

Given the wide range of type of trusts that currently exist in the European Union and the even greater diversity of similar legal arrangements, it is up to the Member States to decide if a trust or a similar legal arrangement is similar to companies or other legal entities, and to notify the European Commission. The

list of trusts and similar legal arrangements governed under the law of the Member States as notified to the European Commission was published in the Official Journal of the European Union on 27 December 2019.

For Belgium "fidéo-commis de residuo" is mentioned as a legal arrangement similar to a trust.

F. Harmonised approach of high-risk third countries

Pursuant to Article 18 of the fourth Directive, obliged entities must apply enhanced customer due diligence measures to natural persons or legal persons established in high-risk third countries. Article 9 of the fourth Directive gives the European Commission the competence to – by means of a delegated act– to identify high-risk third countries which have strategic deficiencies in their national AML/CFT regimes, and therefore pose a significant terrorist financing risk.

Yet Member States were not obliged to include and comply with a specific list of enhanced customer due diligence measures, so such measures with regard to countries with deficiencies were implemented in different ways.

The fifth Directive, as well as the draft law, harmonise these measures. Harmonisation of these measures will prevent or at least reduce the risk of "forum shopping", checking whether a jurisdiction applies stricter or less strict rules with respect to high-risk third countries. Gaps in the legislation that can be misused for ML/TF activities will be closed. The non-exhaustive list of suggested enhanced customer due diligence measures is fully aligned with the lists developed by the FATF for such measures.

It is therefore suggested to replace Article 38 of the Law of 18 September 2017 as follows:

"Article 38. § 1. Obliged entities shall apply the following enhanced customer due diligence measures for their business relationships or occasional transactions with natural persons or legal persons or with legal arrangements such as trusts or *fiducies* linked to a high-risk third country:

1° obtaining additional information on the customer and on the beneficial owner(s);
2° obtaining additional information on the intended nature of the business relationship;
3° obtaining information on the source of funds and source of wealth of the customer and of the beneficial owner(s);
4° obtaining information on the reasons for the intended or performed transactions;
5° obtaining the approval of senior management for establishing or continuing the business relationship;
6° conducting enhanced monitoring of the business relationship by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination;
7° where applicable, ensuring that the first payment be carried out through an account in the customer's name with a credit institution subject to customer due diligence standards that are not less robust than the standards laid down in Law.

§ 2. Without prejudice to Article 14 and 54 the King may, by Decree deliberated in the Council of Ministers, upon advice of the supervisory authorities of the obliged entities involved:

1° require obliged entities to apply, one or more additional mitigating measures to persons and legal entities carrying out transactions involving high-risk third countries. Those measures may consist of:

a) the introduction of enhanced relevant reporting mechanisms or systematic reporting of financial transactions; and/or

b) the limitation of business relationships or transactions with natural persons or legal entities from the high-risk third countries;

2° apply one or more of the following measures with regard to high-risk third countries:

a) refusing the establishment of subsidiaries, branches or representative offices of obliged entities from the country concerned, or otherwise taking into account the fact that the relevant obliged entity is from a country that does not have adequate AML/CFT regimes;

b) prohibiting obliged entities from establishing branches or representative offices in the country concerned, or otherwise taking into account the fact that the relevant branch or representative office would be in a country that does not have adequate AML/CFT regimes;

c) requiring increased prudential supervision or increased external audit requirements for branches and subsidiaries of obliged entities located in the country concerned;

d) requiring increased external audit requirements for financial groups with respect to any of their branches and subsidiaries located in the country concerned;

e) requiring the obliged entities referred to in Article 5, § 1, 4° to 7°, 9° to 14° and 16° to 22 to review and amend, or if necessary terminate, correspondent relationships with respondent institutions in the country concerned.

The application of measures as referred to in the provision under 1°, a), is required by the King upon advice of CTIF-CFI."

G. Identification and verification of customers can now also take place using electronic identification means

Accurate identification and verification of data on natural persons and legal persons are essential for combating ML/TF. The latest technological developments on the digitalisation of transactions and payments enable safe or electronic identification. Electronic identification means and trust services under the eIDAS Directive[26] are important when opening bank accounts or for getting access to means and/or tracing electronic transactions. The eIDAS framework is one of the cornerstones of the digital single market, containing all elements of electronic identification and authentication.

The fifth Directive, as well as the draft law, take into account the new legal framework for the mutual recognition of electronic identification and authentication, with a clear reference to the technical means laid down in the eIDAS Directive in order to ensure the principle of technology neutrality when due diligence measures are applied. Other safe identification processes, which take place remotely or electronically, and are regulated, recognised, approved or accepted at national level by a nationally competent authority, can also be considered. In Belgium, the Federal Public Service Policy and Support manages an authentication service, called Federal Authentication Service or FAS.

References to the electronic identification means were included in Article 27 and 44 of the Law of 18 September 2017 (verification of identity), in Article 60 (keeping data and supporting documents) and in Annex III of the Law of 18 September 2017 (indicative factors of a higher risk linked to products, transactions or delivery channels).

H. Legal framework for the exchange of information and cooperation between authorities designated for AML/CFT purposes for supervising financial institutions and credit institutions and prudential supervisory authorities

Information of a prudential nature relating to credit institutions and financial institutions, such as information relating to the fitness and properness of directors and shareholders, to the internal control mechanisms, to governance or to compliance and risk management, is essential for the adequate

[26] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

AML/CFT supervision of such institutions. AML/CFT information is also important for the prudential supervision of these institutions.

The fifth Directive establishes the adequate legal basis for the exchange of confidential information and cooperation between authorities in charge of the supervision of financial institutions and credit institutions as part of the AML/CFT obligations, as well as prudential supervisory authorities. These authorities must be able to cooperate without any impediments, at national level as well as at European level, regardless of their respective nature or status.

A clarification of the legal framework was all the more important given that prudential supervision in some cases is carried out by supervisory authorities that are not in charge of AML/CFT, such as the European Central Bank (ECB).

The draft law revises Book IV of the Law of 18 September 2017 to combine all provisions on national and international cooperation in Title V entitled "Professional secrecy and cooperation".

I. New Annex IV to the Law of 18 September 2017: List of prominent public functions

To identify politically exposed persons in the European Union, Members States are required under the fifth Directive to establish a list with specific functions that, in accordance with national law, qualify as prominent public functions. So this is a list with functions considered to be prominent public functions, not a list of persons.

The new Annex IV to the Law of 18 September 2017 transposes this obligation.

Member States shall request each international organisation accredited on their territory to establish and keep up to date a list of prominent public functions at that international organisation. The draft law states that the Federal Public Service Foreign Affairs is in charge of this task.

The lists established by Belgium and the international organisations need to be sent to the European Commission, which can make these lists public. The European Commission shall subsequently assemble the lists sent by Member States and international organisations and its own list into one list and make this list public.

VI. ANNEX: Statistics 2019

Table of contents

1. KEY FIGURES

1.1. Disclosures sent to CTIF-CFI

In 2019, CTIF-CFI received 25.991 disclosures from obliged entities. This is a significant decrease of 22% compared to 2018. This drop is the result of a positive change in 2019 in the way one obliged entity disclosed to CTIF-CFI.

	2017	2018	2019
Number of disclosures	31.080	33.445	25.991
	+14 %	+7,6 %	-22,2 %

17.166 disclosures were new money laundering or terrorist financing cases. 8.825 disclosures were additional reports related to existing files.

Section 2 below provides a detailed overview of these 25.991 disclosures.

The 17.166 disclosures received as new cases can be "subjective" disclosures or "objective" disclosures.

CTIF-CFI mainly receives "subjective" disclosures. These disclosures are based on a suspicion of money laundering or terrorist financing.

CTIF-CFI also receives "objective" disclosures, these are disclosures inter alia based on legal indicators or criteria.

"Objective" disclosures include disclosures from the Customs and Excise Administration (cross-border transportation of currency), casinos, notaries[27] and estate agents[28]. These disclosing entities are required to inform CTIF-CFI of facts, even if they do not have any suspicions. Some disclosures of payment institutions or currency exchange offices related to international transfers (money remittance) are generally also part of this category.

1.2. Newly opened files

A large number of disclosures can relate to separate transactions related to the same case. Various disclosures from one single disclosing entity can relate to the same case. Furthermore, the same case can involve disclosures from various separate institutions.

CTIF-CFI groups disclosures of suspicious transactions that relate to one case into one file.

The disclosures received in 2019 were grouped into 13.796 files.

	2017	2018	2019
Number of new files opened because of ML or TF suspicions	10.646	15.670	13.796

In order to process disclosures effectively, CTIF-CFI classifies each disclosure upon receipt according to its importance (amount involved, nature of the transactions, politically exposed persons involved,…) and priority (urgent when funds can be frozen or seized or in case of an ongoing judicial investigation). These two criteria will determine the extent of research carried out and how quickly this research will have to

[27] In accordance with Article 66 of the Law of 18 September 2017.
[28] Ibid.

be carried out. This selection process enables CTIF-CFI to balance any large variations in the number of disclosures or the number of files.

1.3. Files disseminated to the judicial authorities

In 2019, 1.065 new files or cases, for a total amount of EUR 1.158,66 million, were disseminated to the judicial authorities after CTIF-CFI's analysis revealed serious indications of money laundering or terrorist financing. The disseminated files refer to files opened in 2019 as well as in previous years.

In 2019, data or information from 2.945 disclosures, received in 2019 or in previous years, were disseminated to the judicial authorities after analysis. These 2.945 disclosures related to money laundering or terrorist financing transactions for a total amount of EUR 1.538,83 million.

	2017	2018	2019
Number of files disseminated to the judicial authorities	1.192	933	1.065
Amounts in the files disseminated to the judicial authorities[1]	1.108,68	1.432,73	1.158,66
Number of disclosures disseminated to the judicial authorities[2]	3.285	2.972	2.945
Amounts[1] in disclosures disseminated to the judicial authorities[2]	1.415,95	1.700,89	1.538,83

(1) Amounts in million EUR.
(2) CTIF-CFI does not disseminate any copies of disclosures, but only information on suspicious transactions mentioned in these disclosures, in addition to its analysis.

1.4. Number of freezing orders

In 2019, CTIF-CFI used its power to oppose execution of a transaction on 26 occasions. CTIF-CFI temporarily froze assets worth EUR 3,77 million.

	2017	2018	2019
Number of freezing orders	12	8	26
Total amount of freezing orders[1]	0,99	0,68	3,77

(1) Amounts in million EUR.

2. SOURCES OF DISCLOSURES SENT TO CTIF-CFI

2.1. Disclosures[29]

	2017	2018	2019	% 2019
Credit institutions	11.533	9.980	11.237	43,23
Payment institutions	10.834	14.079	5.814	22,37
Company under public law *bpost*	1.363	1.066	1.470	5,66
Notaries	1.076	1.270	1.239	4,77
National Bank of Belgium	568	616	456	1,75
Gaming establishments	995	1.103	396	1,52
Life insurance companies	317	229	308	1,19
External accountants, external tax advisors, external licensed accountants, external licensed tax specialists-accountants	263	212	248	0,95
Companies for consumer credit	20	22	132	0,51
Currency exchange offices	286	223	117	0,45
Institutions for electronic money	0	0	90	0,35
Mortgage credit institutions	19	26	83	0,32
Company auditors	64	60	73	0,28
Estate agents	40	55	52	0,20
Stock broking firms	63	37	49	0,19
Bailiffs	58	69	44	0,17
Dealers in diamonds	11	18	15	0,06
Lawyers	10	8	11	0,04
Insurance intermediaries	11	4	4	0,02
Lease-financing companies	3	3	2	0,01
Branch offices of investment companies in the EEA	2	0	2	0,01
Company service providers	0	0	2	0,01
Branch offices in Belgium of life insurance companies in the EU	0	0	1	-
Intermediaries in banking and investment services	0	0	1	-
Public Trustee Office	0	0	-	-
Central securities depositaries	-	-	0	-
Security firms	1	1	0	-
Market operators	0	0	0	-

[29] Some professions have only been subject to the law since the Law of 18 September 2017 entered into force. This is the case for the mutual guarantee societies, the alternative funding platforms, the company service providers, the audit companies and anyone carrying out the profession of legal auditor and the independent trainees of all accounting professions referred to in the Law. The Law of 18 September 2017 also broadened the scope of the Law to all gaming establishments.

Payment institutions issuing or managing credit cards	0	0	0	-
Settlement institutions	0	2	-	-
Collective investment undertakings	0	0	0	-
Independent financial planners	0	0	0	-
Alternative funding platforms	0	0	0	-
Debt investment firms	0	0	0	-
Mutual guarantee societies	0	0	0	-
Management companies of collective investment undertakings	0	0	0	-
Management companies of alternative investment funds	0	0	0	-
Portfolio management and investment advice companies	0	0	0	-
Branch offices of management companies of collective investment undertakings in the EEA	0	0	0	-
Branch offices of management companies of collective investment undertakings outside the EEA	0	0	0	-
Branch offices of investment companies outside the EEA	0	0	0	-

2.2. Requests for information received from FIU counterparts

	2017	2018	2019	% 2019
FIU counterparts(1)	2.123	1.806	1.463	5,63

(1) In accordance with Article 22 §2 of the Law of 11 January 1993 and Article 79 § 3 1° the Law of 18 September 2017.

2.3. Notifications received from other competent authorities

	2017	2018	2019	% 2019
Customs and Excise(1)	1.282	1.135	1.794	6,90
Department for Advance Tax Rulings [*Service décisions anticipées en matière fiscale*]	1[30]	1239	665	2,56
Flemish tax authority [*Vlaamse belastingdienst*]	13	70	44	0,17
Federal Public Service Finance	18	11	29	0,11
Federal Public Service Economy	7	13	28	0,11
Federal Public Prosecutor's Office	31	28	12	0,05
State Security Department [VSSE]	28	12	8	0,03

[30] The low number of disclosures in 2017 is due to the fact that the Federal Public Service Finance had technical problems connecting to CTIF-CFI's online disclosure system. Given that the issues had not been resolved by the start of 2018, CTIF-CFI decided to manually process the information disclosed by the Federal Public Service Finance.

Trustees in a bankruptcy and temporary administrators	5	4	8	0,03
Coordinating Unit for Threat Analysis [OCAM-OCAD]	17	1	3	0,01
Prisons	-	-	1	-
Information and advice centre on harmful sectarian organisations [*Centre d'Information et d'avis sur les organisations sectaires*]	-	-	1	-
General Intelligence and Security Service [SGRS-ADIV]	6	3	-	-
Federal Public Service Foreign Affairs	-	3	-	-
Public Prosecutor's Office Antwerp	-	1	-	-
European Anti-Fraud Office (OLAF)	1	-	-	-

(1) In accordance with Directive (EC) no 1889/2005 of 26 October 2005 and the Royal Decree of 26 January 2014 on supervisory measures for the physical cross-border transportation of currency.

2.4. Notifications received from supervisory, regulatory or disciplinary authorities

	2017	**2018**	**2019**	**% 2019**
Supervisory authorities	11	36	89	0,34
GRAND TOTAL (2.1 – 2.4)	**31.080**	**33.445**	**25.991**	**100**

2.5. Number of entities having submitted disclosures

Financial professions	**2017**	**2018**	**2019**
Credit institutions	64	56	60
Currency exchange offices, payment institutions, and issuers and institutions for electronic money	35	36	37
Life insurance companies	18	20	16
Mortgage credit institutions	6	9	12
Companies for consumer credit	6	5	10
Stock broking firms	9	8	9
Insurance intermediaries	5	4	3
Branch offices of investment companies in the EEA	2	0	2
Lease-financing companies	3	2	2
Company service providers	0	0	2
Company under public law *bpost*	1	1	1
National Bank of Belgium	1	1	1
Intermediaries in banking and investment services	0	0	1
Payment institutions issuing or managing credit cards	0	0	0
Management companies of collective investment undertakings	0	0	0
Branch offices of investment companies in the EEA	0	0	0
Settlement institutions	0	2	-
Central securities depositories	-	-	0
Portfolio management and investment advice companies	0	0	0
Public Trustee Office	0	0	0
Branch offices of investment companies outside the EEA	0	0	0
Market operators	0	0	0
Branch offices of management companies of collective investment undertakings outside the EEA	0	0	0
Collective investment undertakings	0	0	0
Mutual guarantee societies	0	0	0
Management companies of alternative investment funds	0	0	0
Debt investment firms	0	0	0
Alternative funding platforms	0	0	0
Independent financial planners	0	0	0
Total	**150**	**144**	**157**

Non-financial professions	**2017**	**2018**	**2019**
Notaries	294	290	345
Accounting and tax professions	142	136	142
Estate agents	29	25	29
Company auditors	21	21	27
Bailiffs	16	16	15
Lawyers	6	4	8
Gaming establishments	9	11	14
Trustees in a bankruptcy and the temporary administrators	-	3	6
Dealers in diamonds	2	2	3
Security companies	1	1	0
Total	**520**	**506**	**589**

3. FILES DISSEMINATED TO THE JUDICIAL AUTHORITIES

CTIF-CFI groups disclosures of suspicious transactions that relate to one case into one file. In case of serious indications of money laundering or terrorist financing, this file is disseminated to the competent Public Prosecutor or the Federal Public Prosecutor.

In 2019, CTIF-CFI disseminated1.065 new files to the judicial authorities for a total amount of EUR 1.158,66 million.

If after disseminating a file to the judicial authorities CTIF-CFI receives new or additional disclosures on transactions that relate to the same case and there are still indications of money laundering or terrorist financing, CTIF-CFI will disseminate these new suspicious transactions in an additional file.

In 2019, CTIF-CFI disseminated a total of 2.945 disclosures (new files and additional disseminated files) to the judicial authorities for a total amount of EUR 1.538,83 million.

These disseminated files and disclosures are presented below by type of disclosing entity, type of transaction and predicate offence.

3.1. Files disseminated to the judicial authorities by category of disclosing entity

Number of files disseminated to the judicial authorities by category of disclosing entity – Evolution in the past 3 years

	2017	**2018**	**2019**	**% 2019**
Credit institutions	752	688	783	73,52
Currency exchange offices	7	3	2	0,19
Payment institutions	186	108	102	9,58
Institutions for electronic money	-	-	1	0,09
FIU counterparts	52	43	68	6,38
Company under public law *bpost*	131	46	37	3,47
Accounting and tax professions	9	12	14	1,31
Federal Public Prosecutor's Office	4	2	9	0,85
Supervisory authorities	-	1	9	0,85
National Bank of Belgium	5	5	6	0,56
Federal Public Service Finance	4	1	6	0,56
Notaries	3	7	4	0,38
Mortgage credit institutions	-	-	3	0,28
Dealers in diamonds	3	1	3	0,28
Customs	7	-	3	0,28
Stock broking firms	3	2	2	0,19
State Security Department [VSSE]	10	1	2	0,19
Department for Advance Tax Rulings [*Service décisions anticipées en matière fiscale*]	-	-	2	0,19
Bailiffs	-	1	2	0,19

Coordinating Unit for Threat Analysis [OCAM-OCAD]	3	-	2	0,19
Gaming establishments	6	8	1	0,09
Company auditors	1	1	1	0,09
Lawyers	-	-	1	0,09
Flemish tax authority [*Vlaamse belastingdienst*]	-	-	1	0,09
Estate agents	-	-	1	0,09
Federal Public Service Economy	-	2	-	-
European Anti-Fraud Office (OLAF)	-	1	-	-
Life insurance companies	6	-	-	-
General Intelligence and Security Service [SGRS-ADIV]	-	-	-	-
Total	**1.192**	**933**	**1.065**	**100**

Amounts*[(1)] *in the files disseminated to the judicial authorities – Evolution in the past 3 years

	2017	**2018**	**2019**	**% 2019**
Credit institutions	926,89	1.245,84	807,77	69,72
Supervisory authorities	-	87,04	219,91	18,98
FIU counterparts	81,19	48,34	85,70	7,40
Accounting and tax professions	5,61	15,78	15,50	1,34
Currency exchange offices	0,34	1,82	0,04	0,00
Payment institutions	40,58	17,27	8,67	0,75
Institutions for electronic money	-	-	0,04	0,00
Federal Public Service Finance	1,04	0,09	4,43	0,38
Notaries	1,05	5,22	3,03	0,26
Company under public law *bpost*	5,97	2,75	2,81	0,24
Mortgage credit institutions	-	-	2,58	0,22
Bailiffs	-	2,20	1,28	0,11
Department for Advance Tax Rulings [*Service décisions anticipées en matière fiscale*]	-	-	1,21	0,10
Company auditors	1,14	0,10	1,02	0,09
Flemish tax authority [*Vlaamse belastingdienst*]	-	-	0,86	0,07
Stock broking firms	32,46	2,73	0,83	0,07
Dealers in diamonds	0,92	0,06	0,78	0,07
Customs	2,08	-	0,74	0,06
Estate agents	-	-	0,65	0,06
Coordinating Unit for Threat Analysis [OCAM-OCAD]	0,11	-	0,38	0,03
Lawyers	-	-	0,21	0,02
National Bank of Belgium	0,82	1,09	0,15	0,01
Gaming establishments	1,14	1,77	0,04	-
Federal Public Prosecutor's Office	0,09	0,08	0,03	-
Federal Public Service Economy	-	0,38	-	-
European Anti-Fraud Office of the European Commission (OLAF)	-	0,12	-	-
State Security Department [VSSE]	0,05	0,05	-	-
Life insurance companies	7,54	-	-	-
General Intelligence and Security Service [SGRS-ADIV]	-	-	-	-
Total	**1.108,68**	**1.432,73**	**1.158,66**	**100**

(1) Amounts in million EUR.

Breakdown per category of disclosing institution for disclosures disseminated to the judicial authorities in 2017, 2018 and 2019

	2017		2018		2019	
	Number	**Amount**[(1)]	**Number**	**Amount**[(1)]	**Number**	**Amount**[(1)]
Credit institutions	1.749	1.181,04	1.625	1.430,77	1.829	1.075,52
Federal Public Service Economy	-	-	5	87,04	16	218,19
FIU counterparts	138	82,69	122	70,93	139	119,86
Currency exchange offices	33	16,10	37	3,09	44	50,73
Payment institutions	799	47,71	782	19,65	526	28,08
Accounting and tax professions	22	7,02	42	16,56	34	16,24
Federal Public Service Finance	8	18,61	3	0,10	8	5,84
Notaries	10	1,09	25	5,78	30	4,29
Company under public law *bpost*	211	7,92	103	16,52	103	3,93
Company auditors	1	1,14	3	0,10	6	1,84
FSMA	1	0,03	2	-	5	1,74
National Bank of Belgium	14	0,88	32	1,64	23	1,62
Department for Advance Tax Rulings [*Service décisions anticipées en matière fiscale*]	13	1,77	8	-	19	1,21
Institutions for electronic money	-	-	-	-	1	1,01
Flemish tax authority [*Vlaamse belastingdienst*]	-	-	-	-	1	0,86
Stock broking firms	12	32,46	4	36,47	4	0,83
Customs	24	2,13	7	0,10	18	0,81
Dealers in diamonds	8	1,01	1	0,06	9	0,78
Coordinating Unit for Threat Analysis [OCAM-OCAD]	3	0,12	-	-	2	0,38
Gaming establishments	120	1,48	133	5,71	63	0,25
Federal Public Prosecutor's Office	16	0,09	6	0,10	14	0,04
Life insurance companies	33	8,04	15	0,62	25	0,02
State Security Department [VSSE]	14	0,04	2	-	6	0,01
Federal Public Service Foreign Affairs	-	-	-	-	2	-
General Intelligence and Security Service [SGRS-ADIV]	3	-	-	-	-	-
Other	53	4,58	15	5,65	18	4,75
Total	**3.285**	**1.415,95**	**2.972**	**1.700,89**	**2.945**	**1.538,83**

(1) Amounts in million EUR.

The amounts above are the sum of actual money laundering transactions and potentially fictitious commercial transactions. With these transactions (including files related to VAT carousel fraud) it is very difficult to determine which part is laundered and which part consists of potentially fictitious commercial transactions.

3.2. Nature of the suspicious transactions

The table below specifies the nature of the suspicious transactions in files disseminated to the judicial authorities in 2019. A file disseminated to the judicial authorities may include various types of suspicious transactions.

Type of transactions	Number of files	% 2019
International transfers	213	26,46
Domestic transfers	207	25,71
Cash withdrawals from an account	128	15,90
Cash deposits into an account	104	12,92
Money remittance – Sent	77	9,57
Money remittance – Received	45	5,59
Purchase of real estate	4	0,50
E-money	4	0,50
Transport of cash	3	0,37
Currency exchange transactions	3	0,37
Consumer credit	2	0,25
Casino transactions	2	0,25
Fiscal regularisations	2	0,25
Mortgage credit	1	0,12
Life insurance	1	0,12
Cash payments	1	0,12
Use of cheques	1	0,12
Exchange of small-denomination banknotes	1	0,12
Other	6	0,75

3.3. Financial flows

The table below provides an overview of the financial flows outside of Belgium in the files that CTIF-CFI disseminated to the judicial authorities in 2019, including the main countries of origin and destination of the international transfers.

Origin of the funds	Amounts (million EUR)	%	Destination of the funds	Amounts (million EUR)	%
Switzerland	30,55	22,12	Poland	25,07	18,86
France	22,93	16,60	Portugal	22,36	16,82
Luxembourg	22,83	16,53	Netherlands	11,42	8,59
Netherlands	8,80	6,37	United Kingdom	9,56	7,19
Zambia	8,19	5,93	France	9,08	6,83
Liechtenstein	8,06	5,83	Germany	8,49	6,39
Bulgaria	7,39	5,35	Bulgaria	7,04	5,30
Germany	3,71	2,69	China	6,52	4,91
Spain	3,47	2,51	Luxembourg	5,26	3,96
Slovakia	3,07	2,22	Romania	5,19	3,90
Italy	3,00	2,17	Hong Kong	3,41	2,57
Portugal	2,37	1,72	Turkey	3,30	2,48
Turkey	1,78	1,29	United Arab Emirates	2,03	1,53
Monaco	1,56	1,13	Switzerland	1,50	1,13
United Arab Emirates	1,47	1,06	Denmark	1,44	1,08
India	1,01	0,73	Mexico	1,23	0,93
Other	7,95	5,76	Other	10,01	7,53
Total	**138,14**	**100**	**Total**	**132,91**	**100**

3.4. Files disseminated to the judicial authorities by main predicate offence

Number of files disseminated to the judicial authorities by main predicate offence

Predicate offence	2017	2018	2019	% 2019
Fraud	274	154	210	19,72
Social fraud[(1)]	18	137	197	18,50
Illicit trafficking in narcotics	130	119	119	11,17
Organised crime	72	75	103	9,67
Serious fiscal fraud	100	118	99	9,30
Misappropriation of corporate assets	96	55	64	6,01
Fraudulent bankruptcy	89	63	57	5,35
Terrorism, terrorist financing, including proliferation financing	164	48	57	5,35
Illicit trafficking in arms, goods and merchandise	42	40	46	4,32

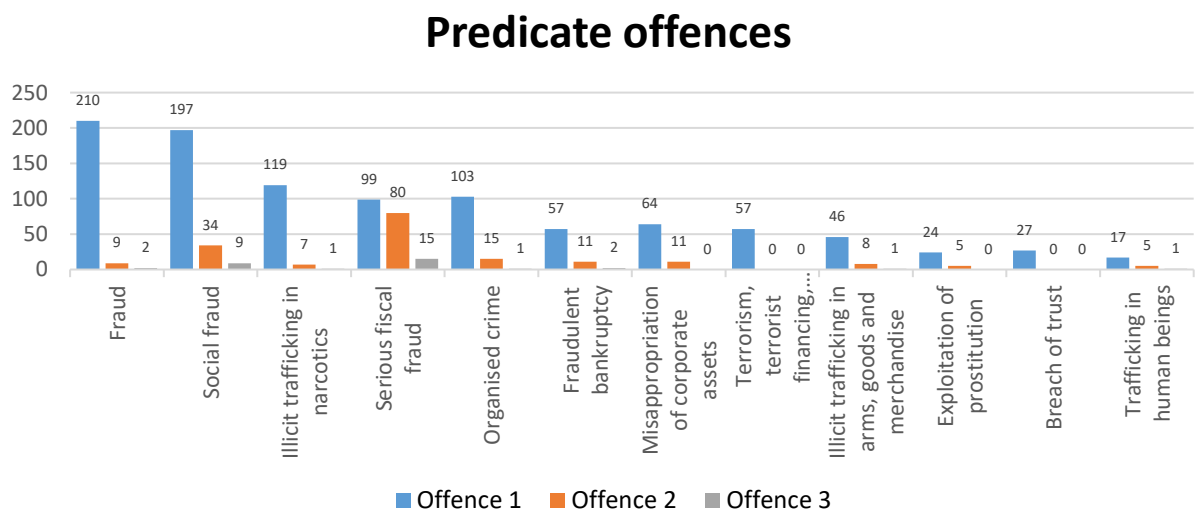
Breach of trust	27	24	27	2,54
Exploitation of prostitution	25	27	24	2,25
Trafficking in human beings	30	20	17	1,60
Smuggling of human beings	-	17	13	1,22
Theft or extortion	23	9	12	1,13
Embezzlement and corruption	13	15	10	0,94
Trafficking in illegal workers	83	-	-	-
Other	6	12	10	0,94
Total	**1.192**	**933**	**1.065**	**100**

(1) Since the Law of 18 September 2017 entered into force.

Number of files disseminated by CTIF-CFI to the judicial authorities in 2019 according the main, second and third most important predicate offence

In one same file CTIF-CFI may have serious indications of money laundering related to one or more predicate offences. CTIF-CFI can also identify one main predicate offence and one or more other predicate offences.

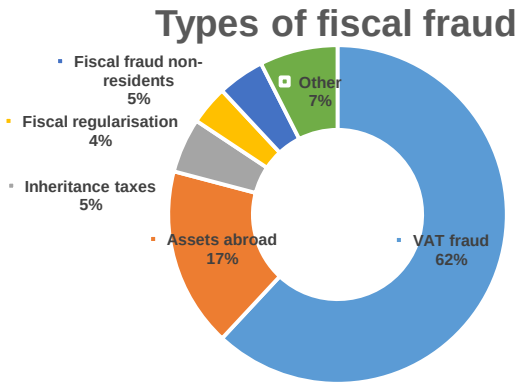
Offence	Total 2019	Main offence	Second offence	Third offence
Social fraud (1)	240	197	34	9
Fraud	221	210	9	2
Serious fiscal fraud	194	99	80	15
Illicit trafficking in narcotics	127	119	7	1
Organised crime	119	103	15	1
Misappropriation of corporate assets	75	64	11	-
Fraudulent bankruptcy	70	57	11	2
Terrorism, terrorist financing, including proliferation financing	57	57	-	-
Illicit trafficking in arms, goods and merchandise	55	46	8	1
Exploitation of prostitution	29	24	5	-
Breach of trust	27	27	-	-
Trafficking in human beings	23	17	5	1
Theft or extortion	16	12	4	-
Smuggling of human beings	14	13	1	-
Embezzlement and corruption	12	10	1	1
Other	14	10	4	-
Total	**1.293**	**1.065**	**195**	**33**



Amounts in files disseminated to the judicial authorities by main type of predicate offence [1]

Predicate offence	**2017**	**2018**	**2019**	**% 2019**
Serious fiscal fraud	300,66	573,41	311,87	26,92
Illicit trafficking in arms, goods and merchandise	19,99	180,97	299,71	25,87
Social fraud [2]	38,65	169,17	228,42	19,71
Organised crime	112,14	112,23	151,09	13,04
Fraud	34,49	75,49	61,05	5,27
Misappropriation of corporate assets	37,77	22,30	30,49	2,63
Embezzlement and corruption	382,77	19,85	18,65	1,61
Fraudulent bankruptcy	23,90	24,94	16,98	1,47
Illicit trafficking in narcotics	38,25	29,03	11,51	0,99
Breach of trust	41,17	16,46	7,77	0,67
Exploitation of prostitution	8,68	5,87	4,66	0,40
Terrorism, terrorist financing, including proliferation financing	1,20	10,89	4,05	0,35
Trafficking in human beings	9,79	120,74	3,77	0,33
Smuggling of human beings	-	4,50	2,56	0,22
Theft or extortion	1,78	1,69	1,33	0,11
Trafficking in illegal workers	55,99	-	-	-
Other	1,45	65,19	4,75	0,41
Total	**1.146,82**	**1.432,73**	**1.158,66**	**100**

(1) Amounts in million EUR.
(2) Since the Law of 18 September 2017 entered into force.



Disclosures in the files disseminated to the judicial authorities in 2017, 2018 and 2019 by predicate offence

	2017		2018		2019	
Predicate offence	**Number**	**Amount**[1]	**Number**	**Amount**[1]	**Number**	**Amount**[1]
Social fraud [2]	42	38,65	335	184,52	520	305,71
Fraud	671	52,65	452	85,51	485	66,83
Organised crime	384	137,44	385	162,30	467	249,70
Serious fiscal fraud	296	419,10	309	694,84	260	386,74
Illicit trafficking in narcotics	328	51,03	383	31,68	242	13,79
Terrorism, terrorist financing, including proliferation financing	448	5,97	202	14,10	168	4,58
Illicit trafficking in arms, goods and merchandise	144	34,76	137	188,25	162	355,36
Fraudulent bankruptcy	156	25,48	145	33,96	141	22,34
Misappropriation of corporate assets	227	53,73	101	30,16	140	33,95
Trafficking in human beings	103	12,84	70	122,34	132	4,43
Breach of trust	105	43,07	74	21,82	57	9,79
Exploitation of prostitution	75	14,29	113	7,44	56	5,30
Embezzlement and corruption	24	446,92	98	20,55	36	30,96
Smuggling of human beings	-	-	43	3,52	23	2,57
Theft or extortion	42	1,89	14	1,82	18	7,09
Trafficking in illegal workers	226	76,69	82	32,47	11	4,03
Other	14	1,44	29	65,61	27	35,66
Total	**3.285**	**1.415,95**	**2.972**	**1.700,89**	**2.945**	**1.538,83**

[1] Amounts in million EUR.
[2] Since the Law of 18 September 2017 entered into force.

3.5. Nationality of the main person involved in files disseminated to the judicial authorities

The table below provides the breakdown by nationality of the main person involved in the files disseminated to the judicial authorities in 2017, 2018 and 2019.

Nationality	2017	2018	2019	% 2019
Belgian	659	572	651	65,49
Portuguese	26	22	59	5,94
Romanian	17	38	42	4,23
French	46	27	29	2,92
Dutch	53	48	26	2,62
Turkish	30	11	23	2,31
Italian	30	11	20	2,01
Brazilian	28	15	16	1,61
Bulgarian	11	10	12	1,21
Albanian	5	9	10	1,01
Spanish	7	6	10	1,01
Moroccan	26	11	9	0,91
Syrian	5	-	9	0,91
Nigerian	9	5	7	0,70
Israeli			7	0,70
Congolese (DRC)	8	8	5	0,50
Pakistani	8	4	4	0,40
Cameroonian	4	3	4	0,40
Russian	10	8	3	0,30
Polish	5	7	3	0,30
Hungarian	2	5	3	0,30
Indian			3	0,30
British	5	7	2	0,20
German	2	3	2	0,20
Tunisian	11	-	2	0,20
Chinese			2	0,20
Ghanaian	5	-	2	0,20
Macedonian			2	0,20
Thai			2	0,20
Afghan			1	0,10
Algerian	7	-	1	0,10
Angolan			1	0,10
Armenian			1	0,10
Bosnian			1	0,10
Iraqi	1	5	1	0,10
Austrian			1	0,10

Beninese	3	-	-	-
Guinean	2	4	-	-
Ivorian	18	-	-	-
Malian	4	-	-	-
Swedish	1	3	-	-
Other	144	91	89	8,95
Total	**1.192**	**933**	**994**	**100**

3.6. Residence of the main person involved

The tables below provide the breakdown by place of residence of the main person involved in the files disseminated to the judicial authorities in 2019. These tables are intended to help disclosing entities apply the statutory compliance measures.

3.6.1. Residence in Belgium

The table below provides the breakdown for the 982 files disseminated to the judicial authorities in which the main person involved resided in Belgium.

	Number of files	%
Brussels	311	31,67
Antwerp	182	18,53
Oost-Vlaanderen	93	9,47
Hainaut	72	7,33
West-Vlaanderen	64	6,52
Limburg	48	4,89
Halle-Vilvoorde	67	6,82
Liège	63	6,42
Brabant wallon	31	3,16
Vlaams-Brabant	21	2,14
Namur	21	2,14
Luxembourg	9	0,91
Total	**982**	**100**

3.6.2. Residence abroad

The table below presents the breakdown for the 83 files disseminated to the judicial authorities in 2019 in which the main individual involved resided abroad.

Country of residence	From 1 January 2019 until 31 December 2019	%
France	9	10,84
Netherlands	9	10,84
Bulgaria	7	8,43
Romania	6	7,23
Albania	3	3,61
Israel	3	3,61
Luxembourg	3	3,61
Portugal	2	2,41
Austria	1	1,20
Brazil	1	1,20
Burkina Faso	1	1,20
Costa Rica	1	1,20
Côte d'Ivoire	1	1,20
Cyprus	1	1,20
Democratic Republic of the Congo	1	1,20
Estonia	1	1,20
Ethiopia	1	1,20
Gabon	1	1,20
Germany	1	1,20
Ghana	1	1,20
Kosovo	1	1,20
Lithuania	1	1,20
Malaysia	1	1,20
Monaco	1	1,20
Russia	1	1,20
Slovenia	1	1,20
South Africa	1	1,20
Suriname	1	1,20
Sweden	1	1,20
Tunisia	1	1,20
United Arab Emirates	1	1,20
United Kingdom	1	1,20
Other	17	20,48
Total	**83**	**100**

4. INTERNATIONAL COOPERATION

As the statistics below indicate, this year CTIF-CFI again sent several requests abroad and also received numerous requests from foreign FIUs.

The operational cooperation with foreign FIUs is usually based on written agreements between different FIUs (MOU or Memorandum of Understanding). Sometimes requests for information are sent to FIUs with which no MOU has been signed when this is useful for operational purposes and when the exchanged information is protected by strict confidentiality[31]. It should nevertheless be stressed that information is always exchanged in a secure way. The exchanged information may never be used without prior consent of the FIU providing the information and permission may only be granted on the basis of reciprocity.

The figures below on the number of requests received from and sent to foreign FIUs not only refer to normal requests but also to spontaneous requests for information exchange. Spontaneous information exchange takes place when CTIF-CFI informs foreign FIUs that a file was disseminated and links were identified with the country of this foreign FIU, even if CTIF-CFI did not query the FIU beforehand. Conversely, CTIF-CFI sometimes received information from foreign FIUs on individuals with an address in Belgium who fell prey to fraud in the country of that FIU or with warnings[32] for specific fraud schemes. CTIF-CFI also considers this exchange of information to be spontaneous information exchange.

In 2019, CTIF received and processed 1.463 requests for assistance from counterpart FIUs[33].

Africa (19)
Benin (2), Cameroon (1), Cote d'Ivoire (1), Democratic Republic of the Congo (2), Ghana (1), Mali (3), Mauritius (2), Senegal (2), Seychelles (2), South Africa (2), Zimbabwe (1)

Americas (844)
Argentina (4), Bermuda (2), Canada (1), Dominican Republic (1), Ecuador (1), Paraguay (2), United States (833)

Asia Pacific (81)
Australia (71), Hong Kong (1), India (4), Malaysia (1), Mongolia (1), Philippines (1), Singapore (1), Taiwan (1)

Eurasia (13)
Kyrgyzstan (1), Russia (12)

Europe (493)
Albania (1), Austria (2), Bosnia and Herzegovina (3), Bulgaria (3), Cyprus (4), Czechia (1), Denmark (4), Estonia (1), Finland (7), France (76), Germany (44), Gibraltar (4), Greece (5), Guernsey (6), Hungary (6), Ireland (2), Isle of Man (3), Israel (4), Italy (6), Jersey (6), Latvia (5), Lithuania (3), Luxembourg (142), Macedonia (1), Malta (16), Moldova (1), Monaco (3), Montenegro (1), Netherlands (63), Norway (1), Poland (5), Portugal (2), Romania (10), Serbia (1), Slovakia (6), Slovenia (5), Spain (11), Sweden (1), Switzerland (2), Turkey (2), Ukraine (1), United Kingdom (23)

Middle East and North Africa (12)
Algeria (1), Bahrain (1), Egypt (1), Lebanon (2), Morocco (2), Saudi Arabia (1), Syria (1), Tunisia (1), United Arab Emirates (2)

[31] Article 125 of the Law of 18 September 2017
[32] Warnings or information on money laundering techniques are published on CTIF-CFI's website or in its annual report.
[33] Grouped on the basis of the regional groups of the Egmont Group and the FATF (FSRBs).

In 2019, CTIF-CFI sent 1.103 requests for information to counterpart FIUs[34].

Africa (28)
Angola (2), Burkina Faso (1), Cabo Verde (1), Cameroon (3), Democratic Republic of the Congo (4), Ghana (1), Mauritius (3), Niger (3), Senegal (3), Seychelles (1), South Africa (5), Uganda (1)

Americas (58)
Argentina (2), Aruba (1), Bahamas (2), Barbados (1), Belize (2), Bermuda (1), Brazil (5), British Virgin Islands (3), Canada (3), Cayman Islands (2), Cuba (1), Curaçao (3), Ecuador (1), El Salvador (1), Mexico (3), Panama (3), Paraguay (1), Saint Kitts and Nevis (1), United States (19), Uruguay (1), Venezuela (2)

Asia Pacific (58)
Australia (2), Bangladesh (2), China (9), Hong Kong (21), India (3), Indonesia (3), Japan (1), Malaysia (2), Philippines (3), Singapore (5), Taiwan (5), Thailand (2)

Eurasia (18)
Belarus (1), Kazakhstan (2), Russia (14), Uzbekistan (1)

Europe (882)
Albania (4), Austria (7), Azerbaijan (1), Bosnia and Herzegovina (4), Bulgaria (23), Croatia (1), Cyprus (4), Czechia (8), Denmark (4), Estonia (7), Finland (6), France (183), Georgia (3), Germany (65), Gibraltar (3), Greece (5), Guernsey (6), Hungary (11), Iceland (2), Ireland (6), Israel (11), Italy (22), Jersey (2), Kosovo (5), Latvia (7), Liechtenstein (8), Lithuania (9), Luxembourg (61), Malta (8), Moldova (2), Monaco (6), Montenegro (1), Netherlands (139), Norway (2), Poland (22), Portugal (20), Romania (16), San Marino (1), Serbia (4), Slovakia (6), Slovenia (6), Spain (38), Sweden (10), Switzerland (35), Turkey (22), Ukraine (9), United Kingdom (57)

Middle East and North Africa (59)
Algeria (4), Egypt (3), Lebanon (7), Morocco (6), Saudi Arabia (4), Tunisia (5), United Arab Emirates (30)

The international fight against money laundering and terrorist financing benefits from a strong and effective joint European approach. Close cooperation between EU FIUs is therefore very important. EU FIUs, including CTIF-CFI, use FIU.net as a tool for exchanging operational data.

Since 1 January 2016 FIU.Net has been embedded in Europol, yet without losing its decentralised nature. This embedding was also approved by the European Commission as synergies between the FIUs and the police could be broadened. CTIF-CFI contributed by being part of the AG (Advisory Group) of the EU FIUs within Europol. However, since the end of 2019 the European Data Protection Supervisor (EDPS) put a ban on Europol regarding its role in FIU.Net due to the processing of personal data said to be beyond Europol's competence.

Given that FIU.Net is crucial to FIUs we were given until 19 December 2020 to continue working under the current conditions. By 20 December 2020 at the latest another entity has to take over this (decentralised) management. As Chair of the AG CTIF-CFI will play an important role in the transition process. One possible option is the takeover by the European Commission itself, this task will then be part of a new European cooperation and coordination mechanism for FIUs.

[34] Ibid.

5. JUDICIAL FOLLOW-UP

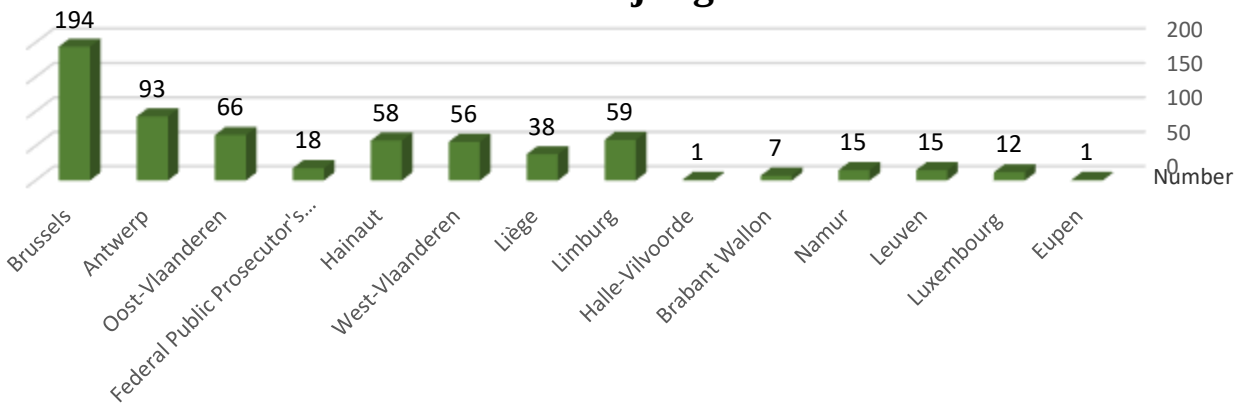
5.1. Judgments

CTIF-CFI is informed of the follow-up of cases by the Public Prosecutor's Offices and the Federal Public Prosecutor's Office. When a judgment is pronounced in a disseminated case then the Public Prosecutor sends a copy of this judgment to CTIF-CFI. The table and graph below were drawn up based on the judgments reported by the Public Prosecutor to CTIF-CFI. The table and graph contain the judgements pronounced in the past ten years in CTIF-CFI's files disseminated to the judicial authorities as well as before. This statistical approach of judgments over a period of ten years takes into account the potential long period between the dissemination of a file to the Public Prosecutor, the investigation and the delivery of the judgment, especially when parties appeal a decision of the court of first instance.

The table below provides an overview per judicial district of the 633 judgments pronounced in the files disseminated by CTIF to the judicial authorities in the last ten years.

	2010-2019	%
Brussels	**194**	**30,64**
Antwerp	**93**	**14,69**
Antwerp	77	
Mechelen	10	
Turnhout	6	
Oost-Vlaanderen	**66**	**10,42**
Gent	43	
Dendermonde	17	
Oudenaarde	6	
Federal Public Prosecutor's Office	**18**	**2,84**
Hainaut	**58**	**9,16**
Charleroi	27	
Mons	17	
Tournai	14	
West-Vlaanderen	**56**	**8,85**
Brugge	32	
Kortrijk	19	
Veurne	-	
Ieper	5	
Liège	**38**	**6,00**
Liège	30	
Verviers	3	
Huy	5	
Limburg	**59**	**9,32**
Hasselt	22	
Tongeren	37	
Halle-Vilvoorde	**1**	**-**
Nivelles	**7**	**1,10**
Namur	**15**	**2,37**
Namur	11	
Dinant	4	
Leuven	**15**	**2,37**
Luxembourg	**12**	**1,90**
Arlon	-	
Neufchâteau	7	
Marche-en-Famenne	5	
Eupen	**1**	**-**
Total	**633**	**100**

Number of judgments



Main predicate offence[35]

	%	Number
Fraud	19,43	123
Fiscal fraud	16,27	103
Illicit trafficking in narcotics	12,48	79
Fraudulent bankruptcy	10,43	66
Illicit trafficking in goods and merchandise	8,85	56
Organised crime	6,64	42
Misappropriation of corporate assets	5,85	37
Trafficking in human beings	5,53	35
Breach of trust	3,79	24
Exploitation of prostitution	2,84	18
Trafficking in illegal workers	1,74	11
Terrorist financing	1,58	10
Theft or extortion	1,26	8
Improper public offering of securities	0,95	6
Use or illicit of hormonal substances	0,79	5
Corruption	0,79	5
Provision of banking services, financial services, insurance services or funds transfer services, or currency trading without having the required licence	0,32	2
Counterfeiting of goods	0,32	2
Stock market-related offence	0,16	1
Total	**100**	**633**

[35] As identified by CTIF-CFI when disseminating the file to the judicial authorities.

5.2. Judicial follow-up – fines and confiscations

The table[36] below provides an overview of the fines and confiscations imposed by courts and tribunals, (amounts in EUR) in files disseminated to the judicial authorities in the past ten years (2010 to 2019) and of which CTIF-CFI was informed. When examining these figures it should be noted that for a large number of files securing evidence may take longer than ten years. This is the case for files related to economic and financial crime, which account for more than 50% of the files disseminated by CTIF-CFI. Moreover, for some decisions an appeal was lodged.

	Fines 2010 to 2019	**Confiscations 2010 tot 2019**	**Total**
Brussels	€ 8.259.707	€ 86.853.558	€ 95.113.265
Antwerp	€ 42.614.371	€ 101.272.163	€ 143.886.534
Antwerp	€ 42.385.846	€ 85.880.768	€ 128.266.614
Turnhout	€ 216.525	€ 15.385.545	€ 15.602.070
Mechelen	€ 12.000	€ 5.850	€ 17.850
Hainaut	€ 655.052	€ 32.680.021	€ 33.335.073
Mons	€ 191.052	€ 31.231.672	€ 31.422.724
Tournai	€ 110.000	€ 1.264.870	€ 1.374.870
Charleroi	€ 354.000	€ 183.479	€ 537.479
Oost-Vlaanderen	€ 349.800	€ 10.552.171	€ 10.901.971
Gent	€ 176.575	€ 7.609.954	€ 7.786.529
Dendermonde	€ 165.575	€ 2.942.217	€ 3.107.792
Oudenaarde	€ 7.650	€ 0	€ 7.650
West-Vlaanderen	€ 128.800	€ 10.935.958	€ 11.064.758
Brugge	€ 117.800	€ 10.396.964	€ 10.514.764
Veurne	€ 5.500	€ 529.419	€ 534.919
Ieper	€ 0	€ 9.575	€ 9.575
Kortrijk	€ 5.500	€ 0	€ 5.500
Limburg	€ 329.250	€ 1.274.946	€ 1.604.196
Hasselt	€ 8.250	€ 133.762	€ 142.012
Tongeren	€ 321.000	€ 1.141.184	€ 1.462.184
Liège	€ 365.888	€ 8.695.060	€ 9.060.948
Liège	€ 357.388	€ 8.695.060	€ 9.052.448
Huy	€ 8.500	€ 0	€ 8.500
Verviers	€ 0	€ 0	€ 0
Namur	€ 25.275	€ 2.741.653	€ 2.766.928
Namur	€ 25.275	€ 2.741.653	€ 2.766.928
Dinant	€ 0	€ 0	€ 0
Brabant Wallon	€ 60.982	€ 551.991	€ 612.973
Leuven	€ 30.285	€ 400.000	€ 430.285

[36] This table was drawn up based on the information and the copies of judgments held by CTIF-CFI on 31 January 2020 and that were spontaneously sent to CTIF-CFI in accordance with Article 82 § 3.

Eupen	€ 0	€ 0	€ 0
Luxembourg	€ 0	€ 0	€ 0
Neufchâteau	€ 0	€ 0	€ 0
Arlon	€ 0	€ 0	€ 0
Marche-en-Famenne	€ 0	€ 0	€ 0
Total	€ 52.819.410	€ 255.957.521	€ 308.776.931

BELGIAN FINANCIAL INTELLIGENCE PROCESSING UNIT

Gulden Vlieslaan 55, bus 1 – 1060 Brussel – Belgium
Avenue de la Toison d'Or 55, boîte 1 – 1060 Bruxelles – Belgium

Phone: +32 (0)2 533 72 11 – Fax: + 32 (0)2 533 72 00

Email: info@ctif-cfi.be – http://www.ctif-cfi.be/

Published by
Philippe de KOSTER
Gulden Vlieslaan 55, bus 1 – 1060 Brussel – Belgium
Avenue de la Toison d'Or 55, boîte 1 – 1060 Bruxelles – Belgium

Additional information on this report and statistics can be obtained by sending a written request to info@ctif-cfi.be.