ctif cfi

Belgian Financial Intelligence Processing Unit

25th Annual Report
2018

TABLE OF CONTENTS

I. PREFACE BY THE DIRECTOR

2018 AND CTIF-CFI OF TOMORROW

On 1 December 2018 CTIF-CFI celebrated its 25th anniversary. CTIF-CFI was created pursuant to the Law of 11 January 1993 but only commenced its activities on 1 December 1993.

A lot has changed in 25 years. The financial system of 2018 is not the same as the one of 1993.

Since the financial crisis of 2008 our financial landscape has changed significantly because of the arrival of new players and the rise of new financial technologies. These new players (PSP, virtual currency exchange platforms) offer new solutions for the financial market but also fragment this market.

Today banking secrecy seems to be a thing of the past, but some players seeking secrecy are drawn to new financial technologies and the anonymity they provide. So there is a risk that in the long run banking secrecy turns into tech secrecy.

Because of their increasing importance it is now vital to regulate these players and work closely with them to ensure that money laundering and terrorist financing is combatted effectively.

In recent years other technological developments have also resulted in significant benefits for the combating of money laundering and terrorist financing. These developments enable a different approach of the customer relationship (*Know Your Customer* (KYC)) and of the compliance role of financial institutions.

Detecting suspicious transactions increasingly relies on computer applications and algorithms. Understanding how these automated decision-making processes are developed is very important to be able to assess the risks related to these algorithms and correct any potential distortions they could create.

It is also essential to find a balance between the intensive use of the "machine" and an effective human intervention adapted to the ML/TF risks. This balance can only be struck if there is a voluntary and rigorous internal AML/CFT culture.

The scandals that have recently discredited some credit institutions, mainly from Nordic countries, clearly demonstrate this. It is essential that the regulatory and supervisory authorities ensure that these institutions have the adequate AML/CFT mechanisms in place and that there is an internal AML/CFT culture.

In recent years, just like the financial sector, CTIF-CFI has initiated an important transformation of increased automatisation of its analytical procedures of suspicious transactions it receives from the financial sector.

In 2018, CTIF-CFI launched several important projects, to improve the international flow of documents and information used by CTIF-CFI with a paperless FIU as the ultimate goal, as well as the increased use of information technology for receiving, enhancing and analysing the operational decision-making process, without replacing this process however.

2018 was also a successful year with regard to the relationship between CTIF-CFI and the Federal Public Prosecutor's Office. The latter is not solely involved in combating terrorist financing, it also plays a key role in combatting the most serious and complex crimes. Important money laundering files analysed by CTIF-CFI related to organised crime or corruption were reported to the Federal Public Prosecutor's Office because of its valuable expertise with regard to these crimes.

In 2018, partnerships with other AML/CFT authorities, such as the Federal Public Service Economy, were also enhanced.

This report provides an overview of CTIF-CFI's activities in 2018.

By means of the statistical data in this report the effectiveness of the AML/CFT system in Belgium can be analysed and assessed. The report also provides obliged entities and other authorities involved with an overview of the latest AML/CFT trends.

In 2018, the number of disclosures received rose by 7,6 %. In 2018, CTIF-CFI processed 33.445 disclosures or communications from other bodies that are considered to be disclosures.

These disclosures led to 993 new files being reported to the judicial authorities and a large number of additional reports with information from 2.972 disclosures, for a total amount of EUR 1.700,89 million.

I would like to thank CTIF-CFI's members and members of staff for the work done in 2018.

I hope you enjoy reading the report.

Brussels, 18 April 2019
Philippe de Koster
Director CTIF-CFI

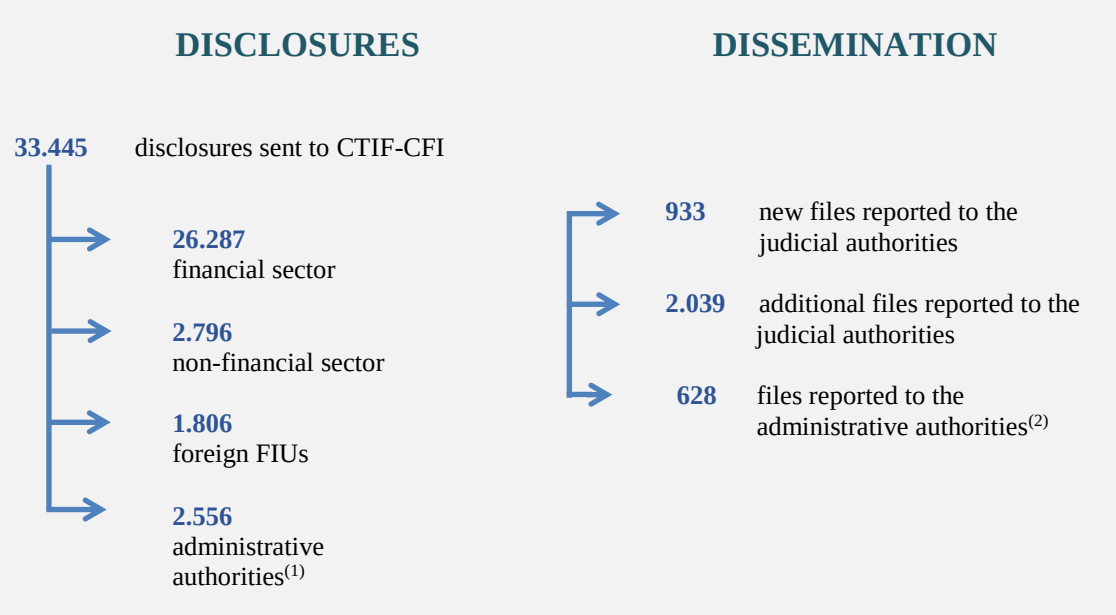
II. COMPOSITION OF CTIF-CFI[1]

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 2018.
[2] Deputy from 1 September 2017.

III. KEY FIGURES 2018

CTIF-CFI's mission is to receive disclosures of suspicious transactions from institutions and individuals (disclosing 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 or terrorist financing, CTIF-CFI forwards 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 Finance 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.

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

[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.

Public Prosecutor in labour matters when the notification to the Public Prosecutor contains information regarding 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 a 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.

- **33.445** disclosures sent to CTIF-CFI
- **933** new files reported to the judicial authorities in 2018 and information from **2.972** disclosures was used in files reported to the Public Prosecutor's Office and the Federal Public Prosecutor's Office for a total amount of **€ 1.700,89 million**.
- **628** information notes were also sent to the Public Prosecutor's Offices in labour matters, 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.

Part IV contains an overview of money laundering and terrorist financing trends in 2018. A detailed overview of the statistics of 2018 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. Files related to drug trafficking

The drug market in Belgium is multifaceted. Belgium is not only a country of destination, but for most of these illegal substances Belgium is also a transit country and a country of production. A record-breaking quantity of cocaine was intercepted[4] in Belgium in 2018: 50 tonnes of cocaine was intercepted, estimated to be worth EUR 2,5 billion. The quantities of heroin, cannabis and opiates intercepted were also on the rise. There are many drug trafficking networks, generating a large amount of money to be laundered.

The increased threat is reflected in the rising number of CTIF-CFI's files reported to the judicial authorities.

To tackle this issue several initiatives for cooperation were developed, to which CTIF-CFI was able to add its expertise.

CTIF-CFI has been involved in the so-called "*Stroomplan*" [Stream Plan] in Antwerp since 2018. The plan aims to have several partners work together and share information in order to comprehensively deal with the issue of drugs in the port of Antwerp, including aspects such as criminal law, labour law, tax law and administrative law. In practice, a multidisciplinary team called "KALI" was set up, comprised of police officers of the Federal Judicial Police and local detectives specialised in drugs, as well as financial investigators of Ecofin and strategic analysts, in order to carry out a broad analysis of the issue. CTIF-CFI takes part in discussions with the "KALI" team and other competent authorities, which take place every month and are coordinated by the Public Prosecutor's Office.

CTIF-CFI also cooperates with the police in Brussels as part of the so-called "*Kanaalplan/Plan du Canal*" [Canal Plan] on financial aspects of terrorism and drug trafficking. The "Global Drug Plan" is aimed at tackling the criminal structures involved in drug trafficking in the district of Brussels.

CTIF-CFI obviously focuses on the criminal organisations' money laundering activities, which do not only undermine the local economy but also have international implications.

Given the scope of this issue CTIF-CFI's strategic analysis department carried out a strategic analysis on laundering the proceeds of drug trafficking in 2018. The strategic analysis showed that various money laundering techniques are being used, ranging from simple to very complicated, which are carried out in the different money laundering stages.

Businesses used as a cover – offsetting technique – Trade-based money laundering (TBML)

In some files businesses are used as a cover, generally those generating a lot of cash (catering industry, distribution,…). Cash proceeds from drugs are combined with income from legitimate commercial activities, sometimes using fake invoices.

[4] https://finances.belgium.be/sites/default/files/Customs/FR/PDF/AADA/communiques/20190111_drugsvangsten2018-FR-FINAL.pdf

In larger files we find that money laundering networks are becoming increasingly professional. Offsetting schemes are used, in which companies in specific industries are involved as essential links in the money laundering chain[5]. In many files we have identified that the *construction industry* poses money laundering risks. CTIF-CFI has found that proceeds of drug trafficking are collected/transported (in particular by professional money launderers[6]) and subsequently handed over to construction companies, offset by transfers to counterparties located abroad (especially in China) disguised as international trade activities, ultimately intended for the drug traffickers.

Given that the funds are returned to the drug traffickers after the offsetting activities, these funds can then either be invested in property or be used to purchase luxury cars, luxury jewellery, consumer goods from wholesalers (textile / drinks). Their resale is part of the TBML practices.

TBML practices have been identified in several files related to the *car trade*, in particular the second-hand car trade. These practices are based on import or export activities of cars intended to conceal the laundering of proceeds of drug trafficking. Some export channels, in particular to West Africa, involve very active export networks. The proceeds of the resale of cars in West Africa are returned to the drug traffickers. Some European countries do not have a maximum amount for purchases in cash (such as Germany), so it is possible to purchase (new, second-hand, luxury) cars in cash. This is an additional money laundering vulnerability.

Investments in real estate – purchases of gold, diamonds, luxury goods

Investing in real estate is still one of drug traffickers' money laundering methods of choice. The properties purchased in Belgium can have various profiles. In case of modest properties renovation work is often conducted, carried out by undeclared workers paid in cash, these funds are actually the proceeds of drug trafficking. These properties can then be sold on for a higher price. The properties are sometimes also small catering businesses, which in turn can be used as a cover for new money laundering transactions. Properties are also purchased abroad, in particular in Spain, Morocco, Turkey and Dubai, generally for large amounts, sometimes for several million EUR.

With regard to transactions related to the purchase of property it is important to point out that notaries play a key role in the relationship with their client, in order to obtain as much information as possible on the client, his profile and the origin of the invested funds.

As mentioned before, proceeds of drug trafficking are also used to purchase high-value goods: luxury cars, luxury watches, diamonds, gold,… These high-value goods may also be resold, particularly abroad. As a result, the individuals involved can have large amounts of cash at their disposal, without having to move cash across borders. In doing so, money laundering can take place by means of the transport of liquid assets and not of cash.

[5] The offsetting technique has also been identified by Tracfin (*Rapport d'analyse* 2017-2018, pages 30-31).
[6] Cf. CTIF-CFI' 2017 Annual Report, pages 24-25.

1.1.2. Files related to smuggling of human beings and trafficking in human beings

Driven by demand, smuggling of human beings and trafficking in human beings have ranked among the most lucrative illegal activities in the European Union over the years. Given this evolution European Member States launched numerous initiatives, such as awareness-raising campaigns and legislative measures.

In Belgium, the national policy on this issue is coordinated by an interdepartmental unit, chaired by the Minister of Justice. CTIF-CFI has been a partner of this unit since 2014. The strategic instruments that have been developed[7] demonstrate the importance of financial investigations and show that raising the awareness of financial professionals with regard to these issues is required. To this end, a working group with different partners[8] was set up. CTIF-CFI committed to contributing to an awareness-raising leaflet for the banking sector. This leaflet, which was distributed via Febelfin, identifies a number of indicators of money laundering transactions that may be related to smuggling of human beings and trafficking in human beings.

The importance of financial investigations is also emphasised at European level, as illustrated by the EU's strategy in this regard: "Following the money throughout the trafficking chain is crucial to turning trafficking in human beings into a high-risk, low-return crime."[9]

Human smuggling and human trafficking networks are generally very mobile, often international and they have cells in the victims' countries of origin, transit and destination. Smugglers use the internet and social media for logistical purposes to recruit victims as well as a commercial platform for prostitution[10]. Links are also identified with other criminal networks, involved in illegal trafficking in drugs, migrants and weapons, serious fiscal fraud, cybercrime or terrorism[11]. The main individual involved in a file reported to the judicial authorities with regard to VAT carousel fraud was also known for human trafficking to the United Kingdom. The money was laundered by transferring it to the United Kingdom via a front company, using fake invoices. This company, with a letterbox address in Belgium, operated in the construction industry. Several transactions carried out on the company's account were not in keeping with the company's normal activity. Many card payments were carried out around ports and airports in Belgium and near Calais[12], including several transfers to car rental companies and transporters of containers. These transactions rather seemed to be part of road, sea or air transport that could be used to smuggle migrants to the United Kingdom.

The financial flows related to sexual exploitation identified by CTIF-CFI are often money remittance transactions sent to areas known to be susceptible to trafficking in human beings. Based on various pieces of information, such as the identification of common counterparties in transfers to several senders, together with police information, links with prostitution networks were able to be established.

---

[7] National Action Plan "Combatting trafficking in human beings 2015-2019" and "National Action Plan combatting smuggling of human beings 2015-2018".

[8] Board of Prosecutors General, Federal Public Service Finance, Federal Public Service Justice, Federal police and CTIF-CFI.

[9] COM/2017/0728 final Communication from the Commission to the European Parliament and the Council Reporting on the follow-up to the EU Strategy towards the eradication of trafficking in human beings and identifying further concrete actions.

[10] Belgian Federal Migration Centre Myria, 2017 Annual Report trafficking and smuggling of human beings: Online".

[11] Europol Internet Organised Crime Threat Assessment (IOCTA), Serious and Organised Crime Threat Assessment (SOCTA) 2017 and Situation Report, Trafficking in Human Beings in the EU (2016).

[12] The report by the European Migrant Smuggling Centre states that "smuggling networks are particularly active in places with a high concentration of irregular migrants, such as reception centres and main transportation hubs", *Two-year Activity Report of the European Migrant Smuggling Centre* (EMSC), 2017-2018, page 9.

The main European countries of origin of the victims are Romania, Hungary, Poland and Bulgaria. The principal third countries are Nigeria, Albania, Vietnam, China and Eritrea[13].

With regard to labour exploitation it should be noted that criminal groups respond to the increased demand for cheap labour identified in many Member States. Europol highlighted that criminals make use of differences in labour law and exploit victims in the grey area between legal employment and labour exploitation[14]. CTIF-CFI's experience shows there are links with social fraud[15]. Fraudulent schemes are set up in order to conceal exploitation: succession of subcontractors, improper use of the secondment procedure by using "letter box companies" in Eastern Europe. The schemes identified in 2018 reveal social dumping practices, in particular via the "Cyprus route": employees are registered with Cypriot companies and are then seconded to come and work in Belgium at a low price. The companies used are registered at a letter box address in Cyprus, do not pay taxes in Cyprus and do not have any activities apart from internal management or administration.

Connections with organised crime are also increasingly identified, as shown by the importance of files involving so-called Brazilian networks[16]. The FATF[17] also points to links with organised crime and states that "issues on trafficking in human beings can be more easily identified on the basis of indicators on the victims of human trafficking or on the basis of indicators of lower levels of criminal organisations. At higher levels of the criminal organisation indicators seem to less specifically bring human trafficking to light and more general reveal organised criminal activities".

1.1.3. Files related to corruption

The number of files reported to the judicial authorities in recent years relating to the laundering of proceeds of corruption or embezzlement by public officials[18] is rather limited, although the amounts involved in these files are very high. The average amount per file is in excess of EUR 2.5 million.

A possible explanation for the limited number of files could be that some aspects of corruption or embezzlement also frequently feature in files reported to the judicial authorities relating to other predicate offences. There are clear links between corruption and embezzlement, organised crime, drug trafficking and fiscal fraud. Elements of corruption were also identified in files related to the world of sports, but were reported to the judicial authorities based on indications of laundering the proceeds of organised crime.

Given the financial scope of this issue, in 2018 CTIF-CFI conducted a strategic analysis on laundering the proceeds of corruption and the embezzlement of public funds over the last six years.

This strategic analysis shows that a large part of those involved in these files are Belgian nationals. Other nationals that feature in these files are often from countries with a high (negative) score on Transparency International's corruption index (high perceived level of corruption in the public sector). The analysis also revealed that foreign nationals in files reported to the judicial authorities are almost exclusively PEPs, usually very high-level ones. When Belgian nationals are involved they are rarely PEPs.

[13] COM(2018) 777 final Report from the Commission to the European Parliament and the Council Second report on the progress made in the fight against trafficking in human beings (2018) as required under Article 20 of Directive 2011/36/EU on preventing and combating trafficking in human beings and protecting its victims.
[14] https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crimethreat-assessment-2017
[15] Cf. CTIF-CFI Annual Report 2017, section on files related to social fraud, pages 13-17.
[16] Cf. the section "Companies used as transit platforms for money laundering transactions".
[17] FATF - APG (2018), Financial Flows from Human Trafficking.
[18] Hereinafter referred to as embezzlement.

In these files one-shot transactions are often carried out: an account is opened that is exclusively used for credit transactions, immediately followed by debit transactions. The bank accounts are opened solely with the aim of carrying out money laundering transactions.

Several modi operandi were identified, which were often combined. In some files, suspicious transactions were carried out related to the purchase of real estate or luxury goods. Analysis showed that these funds were the proceeds of embezzlement of the Treasury by public officials or were payments of secret commissions for public procurement.

In other files complex schemes were used, bringing to light various techniques to conceal the ultimate beneficial owner. Intermediaries are used, in particular in files involving PEPs. Financial transactions take place through low-tax countries or jurisdictions or international trade or financial centres, often involving opaque corporate structures going beyond national borders. Often these are Limited companies, foundations, trusts or Free Zone Establishment (FZE). The involvement of multiple front companies, complex ownership structures and the division of legal entities make it even more difficult to trace financial transactions.

Fake invoices for the provision of services are often used as a justification for transactions from and/or to these corporate structures. The messages accompanying these transfers are generally vague and refer to consultancy fees. The use of fake invoices provides an appearance of economic rationale to money transfers related to a predicate offence and/or related money laundering.

The majority of disclosures reported to the judicial authorities related to corruption or embezzlement of public funds came from major credit institutions. The share of disclosures reported to the judicial authorities that came from private bankers, smaller banks, life insurance companies and non-financial professions was very low. Yet disclosures from all of the financial institutions and from non-financial professions are of crucial importance to combat corruption and money laundering. Accounting professionals are in an excellent position to detect any transactions that could point to corruption. Not only do they have an excellent insight into the financial flows, expenditure (travel and accommodation costs for instance) and cash payments, they also have access to documents (invoices, internal company code, annual accounts) enabling them to detect any anomalies. Notaries and real estate agents are also in an excellent position to detect suspicious real estate transactions.

A request for information from a foreign Financial Intelligence Unit (FIU) was the basis for several files reported to the judicial authorities. In four out of ten files reported to the judicial authorities CTIF-CFI reported information spontaneously or asked questions to one of more foreign FIUs.

Questions into the beneficial ownership of legal entities and the capacity of the persons involved in such files are highly relevant. We can assume that the new Article 20a of the Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing[19] will have a positive effect on the detection of PEPs and suspicious financial transactions involving PEPs from the EU.

Developments within the Egmont Group have also contributed to the above-mentioned strategic analysis on laundering the proceeds of corruption and the embezzlement of public funds. The role of FIUs in combating the laundering the proceeds of corruption was a key issue at the Egmont Group Meetings in March 2018 and various initiatives were adopted. CTIF-CFI took part in the meetings, contributed to

[19] Pursuant to the new Article 20a of Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing each Member State shall issue and keep up to date a list indicating the exact functions which, according to national laws, regulations and administrative provisions, qualify as prominent public functions.

developing a list of indicators to identify suspicious transactions and activities that could reveal corruption[20] and contributed to a typology project on laundering the proceeds of corruption.

Belgium was evaluated in 2018 on the implementation of the provisions of the United Nations Convention against Corruption (UNCAC) on preventive measures and asset recovery. A delegation of CTIF-CFI met with the assessment team during the on-site visit, which was coordinated by the Federal Public Service Foreign Affairs. The OECD Working Group on Bribery in International Business Transactions reported in 2018 on Belgium's progress in implementing earlier specific recommendations. Later this year Belgium will also be assessed by the Group of States against Corruption (GRECO) of the Council of Europe (preventing corruption and promoting integrity in central governments and law enforcement agencies).

We also refer to recent measures that can have a positive effect on reducing corruption and embezzlement. The scope of the Belgian mandate register was broadened on 1 January 2019 and agreement was reached on the protection of whistle-blowers in the European Union. Finally, the use of the UBO register[21] can also contribute to an improved detection of PEPs and corruption.

1.1.4. Files related to fraud

Analysis of the files reveals that networks specialising in large-scale fraud are involved. These dynamic and international networks are looking for new opportunities and regularly use different variations: fraud with fraudulent transfers, CEO fraud, fraud related to non-regulated trading, investments in diamonds, cryptocurrency trading platforms… These files show that often the same networks make use of the same type of fraud.

In 2018, it became apparent that the energy sector is a high-risk sector with regard to money laundering. Several files featured Belgian companies in this sector.

In one of these files the Belgian company A approached private individuals in Belgium with regard to installations using aggressive business practices. Over the period of a few months' time company A had collected several million EUR. Several elements seemed to indicate that the installations of this company, despite the very high price, were of poor quality and were part of fraudulent practices. Some of the funds were transferred to Mr X, who featured in a file that was reported to the judicial authorities due to serious indications of laundering the proceeds of fraud involving cryptocurrencies. Funds were also transferred to company B, operating in a completely different sector. CTIF-CFI's analysis revealed that company B was set up to funnel and launder money from company B using the offsetting system, the money was subsequently withdrawn in cash abroad.

Although fraud techniques evolve and change, money laundering transactions related to this mass fraud are based on international money laundering networks and often follow the same procedure: transferring money abroad (particularly to Eastern Europe and China), using (front) companies' transit accounts, using offsetting schemes with fake invoices.

Given the scope of mass fraud, the amounts involved, prevention and awareness-raising are crucial. We refer to the warnings that are regularly published by the FSMA[22] and Federal Public Service Economy[23] and the warnings on CTIF-CFI's website[24].

[20] The list of indicators is available on CTIF-CFI's website and the website of the Egmont Group (https://www.egmontgroup.org/en/content/new-publication-set-indicators-corruption-related-cases-fius-perspective).
[21] https://financien.belgium.be/sites/default/files/20181017_FAQ_FR_UBO.PDF
[22] https://www.fsma.be/en/news-articles
[23] https://economie.fgov.be/fr/publications/stop-aux-arnaques
[24] http://www.ctif-cfi.be

1.2. Evolution of money laundering techniques

1.2.1. Use of various types of cash transactions

The use of cash is not restricted to a certain type of predicate offence. Although cash is frequently linked to illegal trafficking (drugs, weapons, cigarettes), cash transactions are also used for other types of crime: corruption, social fraud, serious fiscal fraud, fraud,…

CTIF-CFI's statistics show that money laundering schemes involve large amounts of cash. Although bank accounts are still frequently used to carry out cash transactions, cash deposits as well as cash withdrawals, which can therefore be detected by financial institutions, we find that cash transactions are increasingly carried out through atypical channels, indicating that money launderers wish to circumvent the traditional banking system even more.

CTIF-CFI has found that cash is repeatedly withdrawn from ATMs. This is the case for files related to so-called Brazilian networks. Cash is not directly withdrawn in cash in Belgium but funds are first sent to Portuguese companies, subsequently re-transferred to Belgium to various natural persons, Portuguese or Brazilian nationals, and systematically withdrawn in cash from ATMs in Belgium. These withdrawals are not reported to CTIF-CFI by Belgian banks but by payment institutions detecting the cash withdrawals.

In other files foreign bank cards are used to repeatedly withdraw cash from different ATMs in Belgium. These cards are used to carry out substantial cash deposits abroad, linked to the trade in imported cars. Another finding is that the cards of different card holders are often used one after the other at the same ATM, which leads to believe there are links between the individuals involved. Finally, it was established that transactions are split by using different cards of the same cardholder or by family members of the same family. Given the frequency and the amounts it seems possible that the individuals involved were asked to launder money for several criminal organisations, concealed as trade in cars.

1.2.2. Use of corporate structures for money laundering purposes

Concealment of the beneficial owner through front companies

One of the key elements to combat money laundering and terrorist financing is the identification of the beneficial owners to eliminate anonymity and know who is actually behind the transactions and the activities on the account. Files reported to the judicial authorities by CTIF-CFI and the report "Concealment of Beneficial Ownership", recently jointly published by the FATF and the Egmont Group[25], show that money launderers use several techniques to hamper transparency.

One of the techniques is the use of intermediaries to carry out financial transactions, enabling the actual beneficial owner to remain in the background of the transactions. More in particular these are family members, close associates or front men appointed as administrators, managers or proxy holders.

Several files also feature intermediaries acting as agents when setting up legal persons or a head office, providing a commercial address, offices, an administrative address or a postal address. These files feature front companies with fictitious managers, fictitious head offices and vague corporate goals.

CTIF-CFI found that several companies were set up with the profile of front companies, led by front men and to be used for criminal purposes. Most often these were companies that had recently been set up with very broad corporate goals, including sectors such as the construction industry, the industrial cleaning industry, hotel and catering establishments, all of which are sectors vulnerable in terms of money laundering. These companies were generally set up as companies with limited liability (SPRL) or start-up companies with limited liability (SPRL Starter). It should be noted that the pattern of the memoranda of association was often completely identical. The majority of the companies were located in residential areas, which is not in keeping with the activities they claim to carry out. Other companies were located at "letterbox addresses", where the head office of numerous companies was established. The managers of these companies were often fairly young people, who presumably did not have the required business management skills. We also found that payments to the Belgian Official Gazette were carried out but it turned out that the fees for the publication of the memoranda of association were paid using accounts of unrelated companies, without any official link. After some time these companies run up fiscal and social debts, and are ultimately declared bankrupt.

Given that notaries are legally required to play a role in the establishment of companies they are in an excellent position to detect the establishment of companies or constructions aimed at conducting criminal activities and/or laundering the proceeds of criminal activities.

Since 1 September 2018 and since the compulsory registration with the Federal Public Service Economy came into force, domiciliation companies in Belgium have been fully subject to the AML/CFT legislation. This means that these service providers are subject to all legal requirements, i.e. the identification of their customers and suspicious transactions. Given the role they have to play it is essential to be able to turn to reliable partners that have been identified. These companies now also have to be registered with the Federal Public Service Economy.

In general, the different elements typical of the use of front companies should attract the attention of disclosing entities and arouse suspicions. It should be noted that due diligence requirements do not only comprise the identification and identity verification of customers and beneficial owners (Article 33) but also the ongoing due diligence of business relationships and transactions (Article 35-36) and the assessment of the customers' characteristics and the purpose and nature of the business relationship or of the intended occasional transaction (Article 34). Due diligence must be based on an individual assessment of ML/TF risks, taking into account the customer's specific characteristics and the business relationship or the transaction in question.

[25] FATF – Egmont Group (2018), Concealment of Beneficial Ownership.

Certain cases reveal complex and sophisticated arrangements using several legal arrangements in Belgium and abroad, aimed at concealing the actual beneficial owners and facilitating money laundering transactions. The concealment of beneficial owners is further reinforced by complex ownership arrangements and by splitting up legal entities with the following characteristics: the entity is owned by several legal persons (multistep property); the legal persons are located in various jurisdictions and hold numerous bank accounts in other jurisdictions.

After the entry into force of the Royal Decree of 30 July 2018 on the operating terms of the UBO register, the access to information of the ultimate beneficial owners will be facilitated. The UBO register will contain all information that companies, other legal persons and trusts themselves have collected (as legally required) on their ultimate beneficial owners. The General Administration of the Treasury of the Federal Public Service Finance manages this register. The creation of this register and the exact identification of the ultimate beneficial owners is aimed at guaranteeing the transparency of ownership structures.

We also find that opaque corporate structures such as Limited companies, foundations or trusts located abroad are used, in particular in low-tax countries or jurisdictions or international commercial or financial centres. This applies in particular to Dubai, which is the destination of numerous transfers, as shown in the statistics of the financial flows analysed in 2018. The files involving the largest amounts forwarded to the judicial authorities related to illicit trafficking in goods and merchandise, serious fiscal fraud and organised crime. CTIF-CFI often finds links with diamond companies established in Free Trade Zones. Several transactions were said to be carried out between accounts in the United Arab Emirates of these companies that were potentially involved in "round tripping", i.e. transferring money to each other and drawing up fake invoices to fictitiously boost turnover. Transactions were carried out without any economic rationale and in some cases no supporting documents were provided.

In addition, it is not unusual that these opaque corporate structures hold bank accounts with financial institutions in a jurisdiction with little banking transparency different from the jurisdiction where the structure is located. This way the structure is made even more opaque by increasing the number of links with different opaque jurisdictions. We identified structures in the British Virgin Islands, the Seychelles or Guernsey with bank accounts in various other countries with little banking transparency.

Companies used as transit platforms for money laundering transactions

For a number of years now, CTIF-CFI's cases have indicated that Brazilian of Portuguese nationals set up or take over Belgian companies in the construction or cleaning industry. These companies are used as a cover to employ non-declared workers in Belgium, some of whom are in Belgium illegally.

These companies are often part of a network of different companies with a similar profile and are generally used for a limited time only, the time needed to carry out specific transactions. They are then replaced by new structures with new managers in order to perpetuate the system.

The suspicious transactions on accounts of construction and cleaning companies were initially transfers from various companies in these sectors, followed by cash withdrawals. The funds were presumably intended to pay workers employed illegally. Numerous money remittance transactions to Brazil and Portugal were also identified.

Over the years files increasingly featured banking transactions conducted by construction or cleaning companies, mainly managed by Brazilian of Portuguese nationals.

In recent months files reported to the judicial authorities involving so-called Brazilian networks have shown that increasingly complex money laundering schemes are used, not only revealing links with social and/or fiscal fraud but also connections with organised crime.

These files have the following characteristics:

Profile of the companies involved

- These are Belgian companies officially operating in the construction or industrial cleaning industry;
- The companies were generally set up only recently;
- The address of the head office of the companies is often just a "letterbox address";
- The managers are generally nationals of the same country and they live in Belgium (sometimes also abroad);
- The managers often have the profile of front men (recently came to live in Belgium, no experience in business management,…) aimed at concealing the actual manager of the companies;
- The companies are sometimes set up on the same day, managed by the same individuals of the same nationality who arrived in Belgium at the same time;
- VAT returns are blank or not submitted at all;
- The companies do not comply with the obligation to submit their annual accounts.

CTIF-CFI's analysis shows that some companies have a withholding obligation with regard to the Federal Public Service Finance or are not registered with the National Social Security Office. When they are registered they only employ one member of staff, which is a low number given the significant transactions on the companies' accounts. The companies generally do not feature as Belgian customers of foreign companies in the Limosa register[26] in the Dolsis database[27].

Financial profile

- The companies use multiple banks, with the aim of splitting up the total amount of the suspicious transactions;
- Immediately after they have been opened, the accounts are used for a multitude of transactions;
- The financial transactions on various accounts are similar, generally with the same counterparties.

The financial transactions generally have the following characteristics:

Credit transactions

- The accounts of Belgian construction or industrial cleaning companies receive transfers;
- The funds originate from other Belgian (and to a lesser extent Portuguese) construction or industrial cleaning companies;
- These transfers refer to the payment of invoices / services;
- Some transfers mention the name of the individual with power of attorney as the beneficiary instead of the name of the company.

Debit transactions

Some of the funds are withdrawn in cash in Belgium from accounts held by Belgian companies. All or part of these withdrawals were presumably intended to pay workers employed illegally.

Another part is transferred. Some transfers go to natural persons with accounts in Belgium or Portugal and refer to the payment of salaries, although they were not registered through Dimona[28]. Other

[26] Prior notification for seconded employees and self-employed workers (www.limosa.be).
[27] When they are listed as Belgian customers of foreign companies, we find that these companies do not feature as beneficiaries of the transfers.
[28] Dimona (*Déclaration Immédiate/Onmiddellijke Aangifte*) is an electronic system for the employer to register an employee upon commencement or termination of employment with the National Social Security Office. https://www.socialsecurity.be/site_fr/employer/applics/dimona/general/about.htm

transfers are intended for Portuguese companies. Searches in the Limosa register revealed that these transfers were not justified[29].

Most of the counterparties were unfavourably known to CTIF-CFI as they feature in files reported to the judicial authorities related to social fraud and/or serious fiscal fraud. Various counterparties were also unfavourably known to counterpart FIUs for being part of a network of Portuguese companies. The accounts of these companies regularly receive international transfers from various Belgian construction companies managed by Brazilians.

Information from counterpart FIUs showed that the funds sent to Portuguese companies were subsequently sent to various Brazilian nationals and consistently withdrawn in cash from ATMs in Belgium. In some cases huge amounts were spent using prepaid cards of EUR 500.

Taking into account all of these elements it seems that several companies in Belgium were part of a large criminal network linked to serious social / fiscal fraud taking part in money laundering by carrying out transfers between accounts and cash withdrawals.

In addition to links with social fraud and/or serious fiscal fraud CTIF-CFI increasingly finds that numerous companies operate in a network as transit platforms to launder the proceeds of various predicate offences. Vast amounts are involved, million EUR per case over a period of a few months.

The debit transactions were transfers to Belgian or foreign companies (with accounts in Europe or in Asia, mainly in China and in Hong Kong) in various sectors (consumer goods, hotel and catering industry, telecommunication, international payment services,…). These transfers generally referred to, in a vague way and without any actual references, the purchase of goods or the payment of invoices. Discrepancies between the sectors of activity lead to suspect that the financial transactions on the accounts are based on fictitious service provision. These transactions are similar to the offsetting technique at national or international level[30].

[29] Sometimes invoices are presented as proof for debit transactions. These invoices often reveal irregularities (identical format).
[30] See CTIF-CFI's annual reports of 2016 and 2017 in this regard.

2. Terrorist financing trends

In 2018, CTIF-CFI forwarded a total of 47 files to the judicial authorities related to terrorist financing. The total amount reported to the judicial authorities was EUR 14 million.

CTIF-CFI's clear added value in these files often lies in detecting small amounts that could go unnoticed, in identifying links that can only be established on the basis of financial transactions and in elements that only come to light thanks to national and international cooperation. The relevance of financial information is not reflected in the number of files reported to the judicial authorities or the limited amounts typical of this phenomenon.

In 2017, the financing from Belgium of fighters in areas of conflict in Syria and Iraq[31] was extensively analysed, which led to a large number of files (164) reported to the Public Prosecutor's Office because of serious indications of terrorist financing. This explains the difference in the number of files reported to the judicial authorities related to terrorist financing in absolute figures in 2018.

In 2018, Article 83, §2, 4° with regard to the intelligence services and the Coordination Unit for Threat Analysis OCAM-OCAD was applied in 132 cases in the context of the radicalisation process. Pursuant to Article 83, §2, 4° of the Law of 18 September 2017, CTIF-CFI is able to forward relevant information to the intelligence services (the State Security Service [VSSE], the General Intelligence and Security Service of the Armed Forces [SGRS-ADIV], and the Coordination Unit for Threat Analysis [OCAM-OCAD], when this information, as part of the fight against the radicalisation process, can be useful to these services.

As the critical threat of the issue of terrorism in Belgium decreased compared to previous years, CTIF-CFI received a smaller number of disclosures of suspicious transactions/facts. This inevitably had an effect on the number of files reported to the judicial authorities.

Despite the fact that there is no longer a critical threat all bodies involved remain very vigilant and follow the issue very closely. This respite also provides the opportunity to assess the existing processes and cooperation and to refine these further in order to achieve an even more effective approach.

The issue of radicalisation in ***prisons*** remains an issue in 2018. Some prisoners convicted of terrorist offences are held in high regard in extremist circles because of their past and can have a great influence on their fellow prisoners who did not previously support a radical or extremist ideology. Some of them have now been released, but for the vast majority their imprisonment will come to end in the coming years, which will present new challenges for the authorities involved. Financial follow-up of individuals that pose a permanent risk is also advisable, together with the other competent authorities.

To better address the issue of payments to prisoners CTIF-CFI has intensified its cooperation with the Directorate General for Prisons [*Direction Générale des Établissements pénitentiaires / Directoraat Generaal Penitentiaire Instellingen*] (DG EPI)] of the Federal Public Service Justice since 2017. Just like other public services DG EPI can disclose information to CTIF-CFI in case of suspicions of terrorist financing. In August 2018, the AML/CFT law was amended and the provision was added[32] that CTIF-CFI may inform DG EPI of relevant files reported to the judicial authorities for which DG EPI provided information. Such amendments of the law show that even closer cooperation between all partners involved is required.

In recent years, attacks evolved into individual actions by persons inspired by a vague jihadist ideology or by persons with mental health problems and also planned in a short period of time. The competent authorities increasingly focus on potential instigators of terrorist acts: organisations spreading a (violent)

[31] See pages 34-35 of CTIF-CFI's annual report 2017.

[32] Article 83, §2, 9° of the Law of 18 September 2017, inserted by the Law of 30 July 2018, Belgian Official Gazette of 10 August 2018.

extremist vision that inspires susceptible individuals to commit such acts. Attention given to *radicalism* and *violent extremism* is seen as a more proactive approach of terrorism and is gradually more important in the current context. Also in terms of financing, extremism and radicalisation are increasingly viewed as a process that could potentially lead to terrorism.

CTIF-CFI clearly has a role to play in this regard. CTIF-CFI received a large number of disclosures stating that individuals carried out transfers for small amounts (often between EUR 5 and 20) to so-called Islamic-inspired humanitarian organisations. In many cases these were Dutch foundations. Based on close cooperation with foreign FIUs CTIF-CFI was able to determine whether the foreign organisation was part of radical circles or was even suspected of using part of the donations received for terrorist activities. Several suspicious organisations were identified, CTIF-CFI subsequently identified all Belgian ordering parties that donated money to these organisations. Although some of the ordering parties were known to the police as being radicalised, a large part was unknown. This way CTIF-CFI was able to identify a large number of natural persons who were not previously known to the police but who did donate money to suspicious foreign groups or organisations that spread a radical vision. Given that these organisations are often disguised as charities it is not always clear whether the Belgian ordering parties are aware of the malicious intent. Only by intensively using international cooperation mechanisms these types of files can be brought to successful completion.

In a separate part of this report (cf. Chapter V. section 8) we examine to what extent the current preventive system, aimed at tackling money laundering and terrorist financing, can also be used for detecting and analysing suspicious transactions that could be related to the proliferation of salafism and the radicalisation process.

CTIF-CFI also remains very alert to the risks that virtual currencies and new payments systems may pose with regard to terrorist financing, despite the limited number of disclosures in this regard. The perpetrators and suspects of the attacks in Paris and Brussels and other supporters of IS used the latest mobile applications, online payment systems, the Internet and social media, probably drawn to the perceived anonymity and pseudoanonymity these technologies claim to offer. It is a clear signal that these individuals are tech-savvy or at the very least use the latest information technologies[33].

Virtual currencies are used by criminals and terrorists to anonymously purchase items online such as weapons and stolen passports using illegal trading platforms hidden on the Dark Web[34]. Some cases have shown online fundraising was organised through specialised websites and that Payment Service Providers (PSPs) were involved. These PSPs increasingly operate as an online money remitter, which increases the importance of supervision and cooperation with these players, and the challenge will be to do so as quickly as possible. Recent press reports show that the Palestinian group Hamas allegedly used a British cryptocurrency platform to raise funds[35], which can only increase the attention given to this issue. In addition, drug trafficking conducted on an online platform paid in bitcoin or another virtual currency can be used as a source of financing by terrorists or a terrorist organisation.

CTIF-CFI has found that virtual currencies and new payment systems are used to carry out occasional and international ad hoc payments by (members of) a certain (terrorist) group as a way to move funds or to use for online crowdfunding campaigns, often disguised as humanitarian purposes. These types of online payments are promoted as a way to donate money anonymously. A very interesting study by the European Parliament, "Virtual currencies and terrorist financing: assessing the risks and evaluating responses[36]" carried out in May 2018 further explores the topic of terrorist financing through virtual currencies.

[33] Also see pages 31-32 of CTIF-CFI's annual report 2017.
[34] Also see page 32 of CTIF-CFI's annual report 2016.
[35] See https://8lock.io/blockchain-analysis-links-hamas-fundraising-to-coinbase-bitcoin-account/
[36] http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf

Supervising these rapidly evolving new payment systems and mitigating the risks of potential misuse for money laundering and terrorist financing purposes through these systems is a great challenge for disclosing entities, FIUs, intelligence and police services as well as the judicial authorities. The technical evolution is often way ahead of the regulatory framework. Once again, extensive international cooperation is essential to meet these new challenges.

The fifth European Directive provides a regulatory framework for new payment systems with concrete measures to subject providers of exchange services between virtual currencies and fiat currencies to better supervision and make them disclosing entities. The FATF already did a lot of work clarifying the AML/CFT requirements for virtual currencies. In October 2018 Recommendation 15 was revised and the concepts "virtual assets" and "virtual asset service providers" were clearly defined. The FATF will continue its work in June 2019 in order to adopt a new interpretative note to Recommendation 15 and Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers.

In recent years there was more international focus on hybrid, multicriminal organisations that combine political goals with criminal activities for financial gain. This overlap is apparent in files related to smuggling and trafficking of human beings. CTIF-CFI, together with the Federal Public Service Justice and Febelfin, published a brochure in 2018 to inform disclosing entities of this issue.

In the future financial investigation will have to remain flexible enough to be able to deal with the complex reality of the issue of terrorism. Often the perpetrators of terrorist attacks have/had a history of petty crime and (also for these very unfortunate events) CTIF-CFI repeatedly found that some forms of crime yielded funds that were ultimately used for terrorist purposes. Following the attacks in Europe it was necessary to set up specialised departments to respond to the events as quickly and efficiently as possible, although the current evolution has once again given prominence to an integrated approach.

V. AML/CFT CHALLENGES

1. Detecting financial flows

Towards the fifth Directive

The fifth European AML Directive (AMLD5) was published on 19 June 2018 in the Official Journal of the European Union and requires Member States to transpose this Directive into national law before 10 January 2020.

Platforms for exchanging virtual currencies and custodian wallet providers are currently not regulated in Belgium. As there is no legal framework in this regard these entities are not subject to the AML/CFT framework. As a result, CTIF-CFI does not receive any disclosures from exchange platforms established in Belgium.

Because of the fifth Directive these entities will soon be subject to the AML/CFT framework and they will have to apply customer due diligence, in particular identification verification and monitoring in accordance with the Know Your Customer (KYC) and Know Your Transaction (KYT) principles.

It should be noted that European rules on platforms for exchanging virtual currencies are limited to exchange transactions between fiat currencies and cryptocurrencies, i.e. "fiat to crypto". By strictly transposing the Directive, the Belgian law would not comprise the mutual exchange of virtual currencies and therefore create a legal vacuum that could facilitate money laundering as transactions remain anonymous when exchanging virtual currencies. The new Directive offers solutions for some difficulties identified in investigations related to cryptocurrencies but does not enable all shortcomings to be removed. Nevertheless, the Directive establishes a minimum framework and the transposition into national law could, depending on the Belgian political ambition, lead to stricter regulation of the sector.

Thanks to new legislation, users can have more confidence in these entities that will soon be subject to the AML/CFT legislation and therefore be subject to the supervision by state bodies. Moreover, these authorities will have a better understanding of the sector and have the possibility of working and dealing with many market players.

In addition, we find that the second European Payment Services Directive (PSD2)[37], stipulating that payment institutions should be subject to the European AML Directive[38] demonstrates an evolution in the rules by regulating account information services providers (AISPs) and payment initiation services providers (PISP)[39]. Although the latter are new players on the list of entities[40] subject to the AML/CFT Directive, there are still some differences between Members States, in particular as a result of the actual risks linked to these activities.

A few years ago the term Initial Coin Offering (ICO) was introduced, where cryptocurrency capital can be raised to start a project. As a result of this growing financing mechanism –with little or no regulation– some specialised companies, KYC providers, offer to check the identity of investors and the origin of the funds, without accepting responsibility for accepting or rejecting an investor.

[37] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015.
[38] See recital (37).
[39] Account information services providers provide instruments for account management with access to a consolidated overview of the accounts of the user with payment service providers (PSPs). Payment initiation services providers (PISPs) enable users to conduct payment transactions from an account with another payment service provider.
[40] Payment service providers meet the definition of a financial institution referred to in Article 3, 2), a) of AML/CFT Directive (EU) 2015/849 of 20 May 2015.

Payment service providers and cryptocurrencies

The constant evolution of payment institutions for electronic money requires vigilance with regard to payment cards linked to cryptowallets[41]. These cards have the same functions as a conventional bank card but with the amount in cryptocurrency[42] obtained by the card holder (*Crypto-To-Plastic*). The holder of such a card can then easily withdraw cash or carry out online payments with money from cryptocurrencies. This is an additional AML/CFT risk given that the transactions are no longer conducted through a financial institution in fiat currency subject to the AML/CFT framework. Through this missing link in the chain potential suspicious transactions could be missed by the AML/CFT supervisory framework (crypto-to-crypto-environment).

Brexit and information exchange

The exit of the United Kingdom from the European Union could have consequences for numerous financial players, in particular the Payment Service Providers (PSPs). These payment institutions, a large number of which are located in the United Kingdom, carry out services as part of the freedom to provide services in the European Union (passporting) and provide electronic payment solutions. Thanks to passporting they can provide services in all Member States of the European Union. Differences in national legislation regarding information exchange for AML/CFT purposes can sometimes hamper, in particular with the United Kingdom, potential exchange of information on individuals known to CTIF-CFI that use these PSPs. International cooperation assumes that financial intelligence units can share information and it is therefore important to harmonise national legal frameworks.

This being said, in case the United Kingdom would lose the European passporting system after it leaves the European Union, numerous players could be incited to move to another financial centre and request a license in that country. As matters stand, this new distribution could turn out to be an improvement in terms of information exchange with PSPs that were previously established in the United Kingdom, that is if they do not move to a country where the national regulations would not allow optimal information exchange.

Given the huge AML/CFT challenges it is crucial that international organisations such as the FATF and the Egmont Group ensure effective information exchange between financial intelligence units with regard to information held by these new financial players.

Harmonisation of KYC and KYT supervision

The current system, i.e. with the Egmont Group, enables to further develop international cooperation through information exchange between financial intelligence units. When CTIF-CFI wishes to obtain information on an individual with a link in a foreign jurisdiction, it can contact this financial intelligence unit and collect potential financial information of the individual involved. Given the rapid growth of the market of fintech companies registered in different countries it is all the more important that the resources used for KYC and KYT supervision are harmonised to meet the requirements of the international cooperation framework.

Someone could use the services of a PSP for money laundering purposes without any worries as a result of the lack of effective supervision carried out by the payment service provider involved because of the lower standards for monitoring transactions and identity compared to the country where the PSP is established. In these circumstances it is possible that the financial intelligence unit in this country was not made aware of a potential suspicion of ML/TF and as a result is not able to cooperate effectively by sharing information with other financial intelligence units.

[41] Wirex, for instance, is one of these new platforms with such products, replacing the former market leader WaveCrest.
[42] Bitcoin, Litecoin and Ethereum for example.

The constant evolution of ML/TF techniques in a financial world with endless technological innovation, urge various several financial players, in particular financial intelligence units, to continually review their approach for tackling these two issues effectively.

2. The new Criminal Code

A new Criminal Code was designed by Damien Vandermeersch, Advocate General at the Court of Cassation and professor at *Université Catholique de Louvain* and *Université Saint-Louis*, and Joëlle Rozie, professor at *Universiteit Antwerpen*. The reform that these two authors have put forward is unprecedented as it comprises both the rules and basic principles of criminal law, included in Book I of the Criminal Code, as well as the offences in Book II. One of these offences is money laundering, laid down in Article 505, first subparagraph, 2°, 3° and 4°, of the current Criminal Code.

The series of changes made to Article 505 made it very complex and difficult to read, so it requires more than a "superficial clean-up"[43]. The main outline of the reform is as follows[44]: a clearer description of money laundering behaviour[45], criminalisation of self-laundering, regardless of the nature of the intended behaviour, the requirement of a period of traceability of a maximum of ten years for third parties[46] and, with regard to the predicate offence, removing the distinction –introduced by the Law of 10 May 2007– between ordinary fiscal fraud and organised fiscal fraud[47] (this –unfounded– distinction led to difficulties in the application and controversies surrounding the scope of these two concepts).

CTIF-CFI, with a key role in the prevention of combatting money laundering, fully supports the authors' vision of reforming the enforcement component. By improving the legibility of the criminalisation it will be easier to implement by the judiciary, which will lead to an improved follow-up of the reports that CTIF-CFI forwards to the judicial authorities.

The connection between the preventive and enforcement components of combatting money laundering is at stake, and CTIF-CFI hopes that this topic will be dealt with in the next term to be able to put Damien Vandermeersch and Joëlle Rozie's project into practice as quickly as possible.

---

[43] D. VANDERMEERSCH, "*Les infractions de recel et de blanchiment à l'heure de la réforme du Code pénal"*, *Libertés, (l)égalité, humanité. Mélanges offerts à Jean Spreutels*, [The offence of handling stolen goods and money laundering when the Criminal Code is being reformed, Liberty, (l)egality, humanity. Compilation in honour of Jean Spreutels], Brussels, Bruylant, 2019, page 1001 ff., p. 1017 in particular.

[44] Cf. D. VANDERMEERSCH, *op. cit.*, pages 1007 to 1016.

[45] "Money laundering is (1°) keeping, managing or transferring proceeds of crime, of goods or assets put in their place or of income from these invested assets; (2) purchasing, exchanging or receiving free of charge or converting one of the items referred to in 1°, or (3°) concealing or disguising the nature, the origin, the location, the disposal, the moving or the ownership of the items referred to in 1°" (Text of the preliminary draft of the Commission for the reform of criminal law regarding the criminalisation of money laundering – version of 31 March 2018).

[46] "Except when the offence is committed by the perpetrator of the offence from which the proceeds of crime originate, the money laundering is only liable to punishment when this refers to proceeds derived from the offence less than ten years ago, to goods that were transferred or substituted less than ten years ago or were substituted as from the last substitution or transfer, or to income from such proceeds." (Text of the preliminary draft of the Commission for the reform of criminal law regarding the criminalisation of money laundering – version of 31 March 2018).

[47] "With regard to predicate money laundering offences, the draft text suggests removing the distinction – introduced by the Law of 10 May 2007 on various measures regarding handling of stolen goods and seizure– between ordinary fiscal fraud and organised fiscal fraud, except for the former as predicate offence that can lead to the criminalisations referred to under 2° and 4°, first subparagraph, of Article 505 who did not act as perpetrator, accomplice or accessory to the predicate offence." (D. VANDERMEERSCH, *op. cit.*, page 1009).

3. Checks and balances: the European Public Prosecutor's Office and cooperation between financial intelligence units

For over twenty years, there have been discussions on establishing a European Public Prosecutor's Office to prosecute offences detrimental to the financial interests of the European Union. These discussions have led to Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office.

Although not all Members States were involved in this initiative, Belgium was one of the countries arguing in favour of closer cooperation in this respect.

The European Public Prosecutor's Office, which will operational at the end of 2020, will be competent to investigate the following offences: misappropriation of funds and subsidies made available by the European Union (by procurement or not), fraudulently reducing receipts owed to the European Union (from VAT or not), active and passive corruption and misappropriation by European public officials[48]. The European Public Prosecutor's Office will also be competent to deal with offences which are "inextricably linked" to the aforementioned offences.

Will these dynamics that have led to the creation of the European Public Prosecutor's Office by analogy lead to closer cooperation between European financial intelligence units? CTIF-CFI is in favour of specific forms of cooperation based on the model of Joint Investigation Teams, which are already used for police and judicial investigations. These joint teams of financial analysts would be used in emblematic cross-border cases featuring complex money laundering mechanisms and very serious predicate offences (organised crime, international social dumping networks, gangmasters or drug traffickers).

The emergence of closer cooperation between financial intelligence units, for which the practical arrangements still need to be developed, would be an essential addition to the European Public Prosecutor's Office and would make it possible to better tackle serious and complex cross-border crime.

[48] These offences are mentioned in Articles 3 and 4 of Directive (EU) 2017/1371 of the European Parliament and of the Council of 5 July 2017 on the fight against fraud to the Union's financial interests by means of criminal law.

4. Assessing good faith of obliged entities disclosing to CTIF-CFI

Article 57 of the Law of 18 September 2017 offers obliged entities civil, criminal and disciplinary immunity in case a disclosure was sent in good faith to CTIF-CFI.

This provision was criticised due to the alleged legal insecurity it would entail for obliged entities. FEBELFIN, the body representing the banking sector, argues for an amendment to Article 57 "to increase legal security for obliged entities that have disclosed certain funds or transactions to CTIF-CFI in good faith (…) Compensation is only justified when it is established that no other obliged entity, in the same circumstances, would have provided the information to CTIF-CFI"[49].

CTIF-CFI wishes to stress that the system laid down in Article 57 of the Law of 18 September 2017 already ensures maximum protection of disclosing entities.

Disclosing in good faith, as currently referred to in Article 57, is only possible when the obliged entity did not manifestly breach its obligation to carefully examine transactions carried out or its obligation to analyse atypical transactions and when it cannot be considered that it should have known or in any case that it could not be unaware of the fact that the transactions for which a disclosure was sent were not related to money laundering or terrorist financing. This means that, when examining the transaction in question the obliged entity must take proper account of all relevant information at its disposal with regard to the customer, the business relationship and the transaction.[50]

In other words, if the obliged entities, on the basis of the facts at its disposal, cannot reasonably suppose that its customer carries out transactions related to money laundering or terrorist financing but nevertheless does send a disclosure to CTIF-CFI this disclosure can be considered to be sent in bad faith.

CTIF-CFI does not see how amending Article 57 of the Law of 18 September 2017 would better protect obliged entities than is currently already the case.

5. Public-private partnership (PPP)

Experience has shown that financial analysis can be of great importance for a criminal investigation or to prevent or anticipate potential terrorist activities that are being prepared.

With regard to terrorism financial analysis can only produce results when contextual elements on transactions, geographical areas and suspects are available.

Several countries recently introduced a mechanism for greater cooperation between the public and private sector in detecting and combatting terrorism and terrorist financing and platforms were created to exchange information with the banking sector. Examples include the United Kingdom (JMLIT), France (*Appel à la vigilance*), the Netherlands (CT infobox), the United States (*FinCEN Fusion Center*) and Hong Kong (FMLIT). These mechanisms could be extended to the entire financial, or even the non-financial sector.

Because of the specifics of each country there is not one single cooperation mechanism with the private sector.

Although most of the countries have set up these synergies with the private sector in order to prevent terrorism and terrorist financing, the scope of the French system *Appel à la vigilance* is broader. The French FIU Tracfin can inform obliged entities of general (nature of the high-risk transaction or

[49] Memorandum by FEBELFIN for the regional, federal and European elections 2019, page 32.
[50] Bill on the prevention of money laundering and terrorist financing and on the restriction of the use of cash, Chamber of Representatives, Doc. 54/2566, 6 July 2017, page 175.

transactions related to specific geographical areas) or high-risk individual situations (natural persons or legal persons) in terms of ML/TF.

Belgium could develop a mechanism enabling the Federal Public Prosecutor's Office and the intelligence services to request CTIF-CFI to launch a call for vigilance under their responsibility regarding persons or entities suspected of terrorism or terrorist financing, with the possibility of asking the credit institutions involved to maintain the business relationship and exempting them from any civil, criminal or administrative sanctions when they operate as part of the call for vigilance. This mechanism can be introduced under the Law of 18 September 2017.

6. Digitalisation: CTIF-CFI 4.0

The increase in the number of disclosures that CTIF-CFI receives on a daily basis is one of the challenges and is an incentive to improve the effectiveness of the information and document flow of CTIF-CFI. The communication channels used with disclosing entities, external bodies, judicial authorities or foreign counterparts should be able to cope with this increased flow of information and in the past months development projects were started to anticipate future flows. The effectiveness of the information flow of the different players involved in processing CTIF-CFI's files –taking into account the security of the information exchanged– is a crucial element of CTIF-CFI's operations.

The increasingly complex links between the individuals involved and cases, in particular as a result of new money laundering techniques, require keeping up to date with new technologies to support the operational decision-making process. Early identification of risks in files with the use of more intelligent IT tools should be kept as up-to-date as possible. To facilitate the processing of the increasing amounts of information and to put in place analytical tools to fully utilise this structured information, developments in databases are continually being implemented.

To increase the efficiency of information exchange between these players it seems of utmost importance to continue efforts for a transition to paperless communication.

7. Interaction/relationship between CTIF-CFI and disclosing entities and their supervisory authorities

In accordance with the new legal AML/CFT provisions CTIF-CFI and various supervisory authorities have increased their cooperation from the end of 2017 but especially in the course of 2018 and have exchanged information with each other that is useful for carrying out their respective tasks as provided for by law.

This increased cooperation between CTIF-CFI and the supervisory authorities was put into action by organising meetings where the future cooperation was discussed, focussing on the nature of information that can be exchanged and the rules for this information exchange.

Several other meetings followed, during which some supervisory authorities informed CTIF-CFI of the first results of their risk assessment of the various bodies under their supervision, of the identification of priority profiles to plan off-site and on-site checks, of findings of the most recent checks or of recently conducted or planned awareness-raising campaigns for specific obliged entities who send very few or no disclosures to CTIF-CFI.

CTIF-CFI also took the opportunity to provide feedback to several supervisory authorities on the disclosure activities of various entities under their supervision. Information was provided on the number and the amount of disclosures of suspicious transactions to CTIF-CFI over the last three years, to monitor the evolution over time of this activity and on the quality of disclosures following an assessment of whether they are relevant, proactive, complete and properly substantiated.

In order to assess the relevance of disclosures CTIF-CFI also communicated the level of files reported to the judicial authorities of disclosures under their supervision, even though this is an indicator that should be used with the greatest caution.

Moreover, the quality of disclosures is assessed on the basis of the following elements:

- Clarity, summary and structure of the disclosure;
- Time when disclosure is sent to CTIF-CFI (in time or late);
- Full identification of customers and beneficial owners;
- Clear and precise description of the transactions, funds or suspicious transactions (summary of the suspicious transactions, unusual or atypical transactions, details on the origin and suspected destination of suspicious transactions, unusual factors or circumstances,…);
- Motivation of the suspicion (disclosure based on an analysis that led to a suspicion or a disclosure based on objective and automatic criteria (such as transaction thresholds) or a disclosure to "cover" oneself, following a request for information from CTIF-CFI for example;
- Research via open sources;
- Documents attached to the disclosure, in particular account history (with data enabling the identification of counterparties and their banking details, in a format that can be processed by computer) and supporting documents provided by customers.

To ensure the assessment of the items above for all disclosures that CTIF-CFI receives, the FIU has set up an internal communication channel that is used to report and centralise any shortcomings or weaknesses that were to be identified, regardless of whether this occurs at the time of receipt of the disclosure or when being processed by the operational analysts.

Such feedback on the quality of disclosures can only be provided to the supervisory authorities when the entities involved show some disclosing activity, which was not always the case. Some, sometimes even entire sectors, showed signs of little or no activity at all. In this case it was then discussed how awareness could be raised for these sectors regarding their AML/CFT obligations or how to assist in improving the detection of potential suspicious transactions.

This enhanced cooperation between CTIF-CFI and the supervisory authorities as stipulated in the new provisions of the Law of 18 September 2017, aimed at improving the disclosing activities of obliged entities, undoubtedly led to a number of obliged entities (mainly credit institutions and payment institutions) asking CTIF-CFI for information on the quality of their disclosures and how to improve this, the disclosing entities had been asking for such feedback.

These different meetings with the disclosing entities also enabled CTIF-CFI to insist on the need to use the online disclosure system for all disclosures. With this system the disclosed information can be secured and part of the process can be automated.

It was also stressed that the fields in online disclosures should be completed as much as possible, in particular the fields for the disclosure of suspicious transactions, especially when the disclosure refers to a limited number of suspicious transactions.

It was also a chance to remind disclosing entities that from 1 January 2019 onwards some specific fields in the online declaration have a fixed structure (Belgian national register number, business number, IBAN number, nationality of the individual involved).

This new phase in structuring data is aimed at managing the large amounts of information CTIF-CFI receives, to ensure they are compatible with the requests that may soon be sent to the Central Point of Contact (CPC) of the National Bank of Belgium and follow up on international cooperation with other (European) financial intelligence units.

8. Clarification of CTIF-CFI's role with regard to the issues of radicalism and extremism

The Law of 18 September 2017 completes the enforcement approach of money laundering (Article 505 of the Criminal Code) and terrorist financing (Articles 140 and 141 of the Criminal Code) by adding a number of preventive measures and administrative sanctions.

Obliged entities subject to the preventive legislation are required to cooperate with the aim of detecting suspicious transactions and facts and disclosing these to CTIF-CFI. Disclosure to CTIF-CFI is the basis of the preventive system to combat money laundering and terrorist financing. CTIF-CFI has extensive powers to conduct financial investigation but can only use these powers after receiving a disclosure of suspicious transactions or facts from the categories of the disclosing entities listed exhaustively in Article 79 of the aforementioned law.

CTIF-CFI cannot on its own initiative or merely based on open-source information start an investigation into the financing or the financial situation of specific organisations or individuals.

Cooperation with the intelligence services and the Coordinating Unit for Threat Analysis OCAM-OCAD

The Law of 18 September 2017 does not, nor does the definition of terrorist financing in the law, refer to extremism or radicalism. The legislator did create the possibility for CTIF-CFI to share all information relating to radicalism in accordance with Article 83, § 2, 4° with the Coordinating Unit for Threat Analysis OCAM-OCAD and the intelligence services (State Security Department VSSE and the General Intelligence and Security Service of the Armed Forces SGRS-ADIV).

This channel of communication, which already exists between these bodies with the aim of combating terrorism, terrorism financing and related money laundering transactions, an exception to CTIF-CFI's strict professional secrecy[51], remains in Article 83, §2, 4° of the new Law and was extended to combating the radicalisation process, with the same objective.

The aim is to increase the efficiency of CTIF-CFI's preventive role in combating radicalism by extending its possibilities of forwarding information to the intelligence services and the Coordinating Unit for Threat Analysis OCAM-OCAD, even when no information is reported to the judicial authorities. Although the Public Prosecutor's Office does not deal with radicalism given that this phenomenon is not an offence, this information can be very useful to the intelligence services and the Coordinating Unit for Threat Analysis OCAM-OCAD.

In accordance with Article 83, §2, 4°, CTIF-CFI can share all information on radicalised persons or organisations and with the intelligence services and the Coordinating Unit for Threat Analysis OCAM-OCAD.

If analysis carried out by CTIF-CFI points to radicalism all relevant information will be shared with the intelligence services and the Coordinating Unit for Threat Analysis OCAM-OCAD, regardless of whether the file was forwarded to the judicial authorities or closed by CTIF-CFI.

The reference to only money laundering and terrorist financing in Article 79 of the Law of 18 September 2017 does not prevent an intelligence service or the Coordinating Unit for Threat Analysis

[51] The members of CTIF-CFI and members of its staff, the members of the police services and other officials seconded to CTIF-CFI as well as the external experts it calls upon are bound by strict professional secrecy. Even in the circumstances referred to in Article 29 of the Code of Criminal Procedure and except for the case where they are called upon to testify in criminal proceedings, they may not disclose the information collected in the performance of their tasks, with the exception of forwarding information as stipulated in the law.

OCAM-OCAD of disclosing suspicious transactions or facts (related to extremism/radicalism or not) in good faith to CTIF-CFI.

In practice there are few legal limitations to the information CTIF-CFI may receive. The starting point for analysis by CTIF-CFI is the disclosure of suspicious transactions or facts, either by a financial institution and other private non-financial disclosing entity, or by a (federal) government body.

Not only the Coordinating Unit for Threat Analysis OCAM-OCAD and the intelligence services can disclose to CTIF-CFI, officials from various Federal Public Services can send disclosures to CTIF-CFI as well.

As part of its analysis following a disclosure based on Article 79, CTIF-CFI can request addition information from disclosing entities – financial institutions, non-financial disclosing entities and government bodies, as well as foreign counterparts. CTIF-CFI is part of an international network of FIUs and takes part in activities and projects of global organisations such as the FATF and the Egmont Group[52]. Communication networks between FIUs, such as FIU.net for European countries and the Egmont Secure Web at world level ensure swift information exchange. CTIF-CFI also signed MOUs with various foreign counterparts, which promote bilateral cooperation.

Bodies such as the Federal Public Service Foreign Affairs and Federal Public Service Justice, can disclose atypical transactions or facts suspected to be related to money laundering or terrorist financing, in accordance with Article 79, but can only be informed of the results of the investigation through an assessment of the Coordinating Unit for Threat Analysis OCAM-OCAD, the State Security Department VSSE or the General Intelligence and Security Service of the Armed Forces SGRS-ADIV, which will probably also contain other elements than financial flows.

The results of CTIF-CFI's financial investigation can be used by the Coordinating Unit for Threat Analysis OCAM-OCAD and/or the intelligence services in an assessment, gaining a better insight into the issue of radicalism, enabling political authorities to use diplomatic pressure if need be.

In 2017, the competent authorities (CTIF-CFI, Federal Public Prosecutor's Office, Federal Police, the Coordinating Unit for Threat Analysis OCAM-OCAD, the State Security Department VSSE and the General Intelligence and Security Service of the Armed Forces SGRS-ADIV, the Federal Public Service Economy and the Federal Public Service Finance - General Administration of the Treasury) assembled in the "terrorist financing platform" chaired by CTIF-CFI, carried out the first national risk assessment, as requested by Strategic Committee for Intelligence and Security. The results of this analysis were provided to the National Security Council in July 2017. In July 2018, the platform developed an action plan with measures to mitigate the identified TF risks as much as possible.

[52] International grouping of FIUs, established in 1995 by CTIF-CFI and the American FIU FinCEN.

9. CTIF-CFI and personal data protection

2018 was an important year with regard to personal data protection.

The General Data Protection Regulation (GPDR) (EU) 2016/679 applies from 25 May 2018.

Moreover, the Law of 30 July 2018 on the protection of natural persons with regard to the protection of personal data was published on 5 September 2018. This framework law repeals the privacy legislation, provides for implementation of a number of provisions of the GDPR and transposes Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences into Belgian law.

Both the General Data Protection Regulation and the Framework Law of 30 July 2018 stipulate that a Data Protection Officer (DPO) must be designated when the processing is done by a public authority or body.

In order to comply with this requirement, CTIF-CFI designated a DPO internally in 2018.

VI. ANNEX: Statistics 2018

Table of contents

1. KEY FIGURES

1.1. Disclosures sent to CTIF-CFI

In 2018, CTIF-CFI received 33.445 disclosures from obliged entities. The number of disclosures sent to CTIF-CFI has risen sharply since 2016 (+23 %).

	2016	2017	2018
Number of disclosures	27.264	31.080	33.445
	-3,5 %	+14 %	+7,6 %

16.308 disclosures were new money laundering or terrorist financing cases. 17.137 disclosures were additional reports related to existing files.

Section 2 below provides a detailed overview of these 33.445 disclosures.

The 16.308 disclosures received can be "subjective" disclosures or "objective" disclosures.

CTIF-CFI 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[53] and estate agents[54]. 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 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 2018 were grouped into 15.670 files.

	2016	2017	2018
Number of new files opened because of ML or TF suspicions	9.360	10.646	15.670

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

[53] In accordance with Article 66 of the Law of 18 September 2017.
[54] Ibid.

1.3. Files reported to the judicial authorities

In 2018, 933 new files or cases, for a total amount of EUR 1.432,73 million, were reported to the judicial authorities after CTIF-CFI's analysis revealed serious indications of money laundering or terrorist financing. The reported files refer to files opened in 2018 as well as in previous years.

In 2018, data or information from 2.972 disclosures, received in 2018 or in previous years, were reported to the judicial authorities following analysis. These 2.972 disclosures related to money laundering or terrorist financing transactions for a total amount of EUR 1.700,89 million.

	2016	**2017**	**2018**
Number of files reported to the judicial authorities	831	1.192	933
Amounts in the files reported to the judicial authorities(1)	1.146,82	1.108,68	1.432,73
Number of disclosures reported to the judicial authorities(2)	2.577	3.285	2.972
Amounts(1) in disclosures reported to the judicial authorities(2)	1.285,68	1.415,95	1.700,89

(1) Amounts in million EUR.

(2) CTIF-CFI does not forward 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 2018, CTIF-CFI used its power to oppose execution of a transaction on 8 occasions. CTIF-CFI temporarily froze assets worth EUR 0,68 million.

	2016	**2017**	**2018**
Number of freezing orders	17	12	8
Total amount of freezing orders(1)	2,69	0,99	0,68

(1) Amounts in million EUR.

2. SOURCES OF DISCLOSURES SENT TO CTIF-CFI

2.1. Disclosures[55]

	2016	2017	2018	% 2018
Currency exchange offices, payment institutions and issuers and institutions for electronic money	9.392	11.120	14.302	42,76
Credit institutions	8.662	11.533	9.980	29,84
Notaries	1.094	1.076	1.270	3,80
Operators of games of chance	930	995	1.103	3,30
Company under public law *bpost*	1.118	1.363	1.066	3,19
National Bank of Belgium	603	568	616	1,84
Life insurance companies	320	317	229	0,68
External accountants, external tax advisors, external licensed accountants, external licensed tax specialists-accountants	178	263	212	0,63
Bailiffs	81	58	69	0,21
Company auditors	68	64	60	0,18
Estate agents	35	40	55	0,16
Stock broking firms	63	63	37	0,11
Mortgage credit institutions	13	19	26	0,08
Companies for consumer credit	42	20	22	0,07
Dealers in diamonds	35	11	18	0,05
Lawyers	4	10	8	0,02
Insurance intermediaries	6	11	4	0,01
Lease-financing companies	3	3	3	0,01
Settlement institutions	2	0	2	0,01
Security firms	0	1	1	-
Branch offices of investment companies in the EEA	1	2	0	-
Branch offices of investment companies outside the EEA	0	0	0	-
Payment institutions issuing or managing credit cards	0	0	0	-
Branch offices of management companies of collective investment undertakings in the EEA	2	0	0	-
Intermediaries in banking and investment services	1	0	0	-

[55] 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 operators of games of chance.

	2016	2017	2018	% 2018
Portfolio management and investment advice companies	0	0	0	-
Management companies of collective investment undertakings	0	0	0	-
Branch offices of management companies of collective investment undertakings outside the EEA	0	0	0	-
Collective investment undertakings	0	0	0	-
Public Trustee Office	1	0	0	-
Market operators	0	0	0	-
Mutual guarantee societies	-	0	0	-
Management companies of alternative investment funds	-	0	0	-
Debt investment firms	-	0	0	-
Alternative funding platforms	-	0	0	-
Independent financial planners	-	0	0	-
Company service providers	-	0	0	-

2.2. Requests for information received from FIU counterparts

	2016	2017	2018	% 2018
FIU counterparts(1)	2.028	2.123	1.806	5,40

(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

	2016	2017	2018	% 2018
Federal Public Service Finance	1.163	19[56]	1.250	3,74
Customs and Excise(1)	1.387	1.282	1.135	3,39
Flemish tax authority	-	13	70	0,21
Federal Public Prosecutor's Office	1	31	28	0,08
State Security Department [VSSE]	12	28	12	0,04
Federal Public Service Economy	5	7	13	0,04
Trustees in a bankruptcy	8	5	4	0,01
General Intelligence and Security Service [SGRS-ADIV]	2	6	3	0,01

[56] The low number of disclosures in 2017 is due to the fact that the Federal Public Service Economy 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 reported by Federal Public Service Economy.

	2016	2017	2018	% 2018
Federal Public Service Foreign Affairs	-	-	3	0,01
Public Prosecutor's Office Antwerp	-	-	1	-
Coordinating Unit for Threat Analysis [OCAM-OCAD]	2	17	1	-
European Anti-Fraud Office of the European Commission (OLAF)	-	1	-	-
Federal Public Service Interior	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

	2016	2017	2018	% 2018
Supervisory authorities	1	11	36	0,11
GRAND TOTAL (2.1 – 2.4)	**27.264**	**31.080**	**33.445**	**100**

2.5. Number of entities having submitted disclosures

Financial professions	**2016**	**2017**	**2018**
Credit institutions	66	64	56
Currency exchange offices, payment institutions, and issuers and institutions for electronic money	31	35	36
Life insurance companies	16	18	20
Stock broking firms	8	9	8
Companies for consumer credit	5	6	5
Mortgage credit institutions	5	6	9
Payment institutions issuing or managing credit cards	0	0	0
Insurance intermediaries	6	5	4
Management companies of collective investment undertakings	0	0	0
Company under public law *bpost*	1	1	1
National Bank of Belgium	1	1	1
Branch offices of investment companies in the EEA	1	2	0
Branch offices of management companies of collective investment undertakings in the EEA	1	0	0
Intermediaries in banking and investment services	1	0	0
Clearing institutions	1	0	2
Lease-financing companies	2	3	2
Portfolio management and investment advice companies	0	0	0
Public Trustee Office	1	0	0
Branch offices of investment companies outside the EEA	0	0	0
Market operators	0	0	0
Branch offices of investment companies outside the EEA	0	0	0
Collective investment undertakings	0	0	0
Mutual guarantee societies	-	0	0
Management companies of alternative investment funds	-	0	0
Alternative funding platforms	-	0	0
Independent financial planners	-	0	0
Company service providers	-	0	0
Total	**146**	**150**	**144**

Non-financial professions	**2016**	**2017**	**2018**
Notaries	320	294	290
Accounting and tax professions	93	142	136
Estate agents	18	29	25
Company auditors	22	21	21
Bailiffs	12	16	16
Operators of games of chance	9	9	11
Lawyers	4	6	4
Dealers in diamonds	4	2	2
Security companies	0	1	1
Trustees in a bankruptcy	-	-	3
Total	**482**	**520**	**506**

3. FILES REPORTED 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 reported to the competent Public Prosecutor or the Federal Public Prosecutor.

In 2018, CTIF-CFI reported 933 new files to the judicial authorities for a total amount of EUR 1.432,73 million.

If after reporting 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 report these new suspicious transactions in an additional file.

In 2018, CTIF-CFI reported a total of 2.972 disclosures (new files and additional reported files) to the judicial authorities for a total amount of EUR 1.700,89 million.

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

3.1. Files reported to the judicial authorities by type of disclosing entity

Evolution of the number of files reported to the judicial authorities by category of disclosing entity in the past 3 years

	2016	**2017**	**2018**	**% 2018**
Credit institutions	557	752	688	73,74
Currency exchange offices and payment institutions	98	193	111	11,90
Company under public law *bpost*	89	131	46	4,93
FIU counterparts	39	52	43	4,61
Accounting and tax professions	11	9	12	1,29
Operators of games of chance	8	6	8	0,86
Notaries	6	3	7	0,75
National Bank of Belgium	6	5	5	0,54
Federal Public Prosecutor's Office	-	4	2	0,21
Stock broking firms	-	3	2	0,21
Federal Public Service Economy	1	-	2	0,21
State Security Department [VSSE]	1	10	1	0,11
Federal Public Service Finance	4	4	1	0,11
Dealers in diamonds	2	3	1	0,11
Company auditors	-	1	1	0,11
Bailiffs	1	-	1	0,11
Supervisory authorities	2	-	1	0,11
European Anti-Fraud Office of the European Commission (OLAF)	-	-	1	0,11
Customs	3	7	-	-

Life insurance companies	1	6	-	-
Coordinating Unit for Threat Analysis [OCAM-OCAD]	1	3	-	-
General Intelligence and Security Service [SGRS-ADIV]	1	-	-	-
Total	**831**	**1.192**	**933**	**100**

Evolution of the amounts*[(1)] *in the files reported to the judicial authorities in the past 3 years

	2016	**2017**	**2018**	**% 2018**
Credit institutions	1.035,67	926,89	1.245,84	86,96
Supervisory authorities	4,09	-	87,04	6,08
FIU counterparts	48,90	81,19	48,34	3,37
Accounting and tax professions	7,06	5,61	15,78	1,10
Company under public law *bpost*	3,33	5,97	2,75	0,19
Currency exchange offices and agents of payment institutions	27,58	40,58	19,09	1,34
Notaries	4,06	1,05	5,22	0,36
Stock broking firms	-	32,46	2,73	0,19
Bailiffs	0,03	-	2,20	0,15
Operators of games of chance	0,76	1,14	1,77	0,12
National Bank of Belgium	0,57	0,82	1,09	0,08
Federal Public Service Economy	0,27	-	0,38	0,03
European Anti-Fraud Office of the European Commission (OLAF)	-	-	0,12	0,01
Company auditors	-	1,14	0,10	0,01
Federal Public Service Finance	3,08	1,04	0,09	0,01
Federal Public Prosecutor's Office	-	0,09	0,08	-
Dealers in diamonds	0,11	0,92	0,06	-
State Security Department [VSSE]	-	0,05	0,05	-
Life insurance companies	0,98	7,54	-	-
Customs	10,29	2,08	-	-
Coordinating Unit for Threat Analysis [OCAM-OCAD]	0,02	0,11	-	-
General Intelligence and Security Service [SGRS-ADIV]	0,02	-	-	-
Total	**1.146,82**	**1.108,68**	**1.432,73**	**100**

(1) Amounts in million EUR.

Breakdown per category of disclosing institution for disclosures reported to the judicial authorities in 2016, 2017 and 2018

	2016		2017		2018	
	Number	**Amount**[(1)]	**Number**	**Amount**[(1)]	**Number**	**Amount**[(1)]
Credit institutions	1.278	1.148,89	1.749	1.181,04	1.625	1.430,77
Currency exchange offices and payment institutions	713	29,36	832	63,81	819	22,74
Company under public law *bpost*	167	3,72	211	7,92	103	16,52
FIU counterparts	120	51,11	138	82,69	122	70,93
Operators of games of chance	85	1,81	120	1,48	133	5,71
Life insurance companies	23	1,42	33	8,04	15	0,62
Customs	78	11,44	24	2,13	7	0,10
Accounting and tax professions	19	8,01	22	7,02	42	16,56
Federal Public Service Finance	8	3,08	21	20,38	11	0,10
Federal Public Prosecutor's Office	-	-	16	0,09	6	0,10
National Bank of Belgium	30	0,90	14	0,88	32	1,64
State Security Department [VSSE]	1	-	14	0,04	2	-
Stock broking firms	2	-	12	32,46	4	36,47
Notaries	23	8,24	10	1,09	25	5,78
Dealers in diamonds	5	0,11	8	1,01	1	0,06
General Intelligence and Security Service of the Armed Forces [SGRS-ADIV]	1	0,02	3	-	-	-
Coordinating Unit for Threat Analysis [OCAM-OCAD]	-	-	3	0,12	-	-
Other	24	17,57	55	5,75	25	92,79
Total	**2.577**	**1.285,68**	**3.285**	**1.415,95**	**2.972**	**1.700,89**

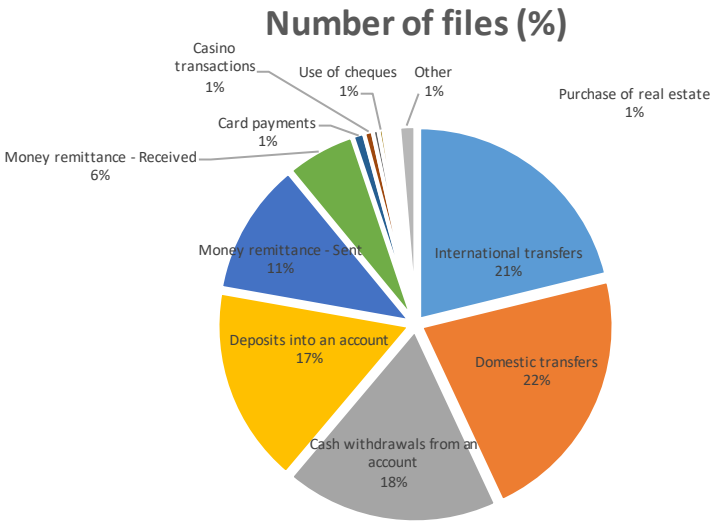
(1) Amounts in million EUR

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 suspcious transactions

The table below specifies the nature of the suspicious transactions in files reported to the judicial authorities in 2018. A file reported to the judicial authorities may include various types of suspicious transactions.

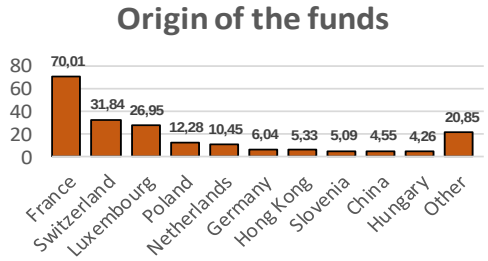
Type of transactions	Number of files	% 2018
International transfers	267	18,55
Domestic transfers	276	19,18
Cash withdrawals from an account	228	15,84
Deposits into an account	210	14,59
Money remittance – Sent	142	9,87
Money remittance – Received	73	5,07
Card payments	12	0,83
Casino transactions	9	0,63
Purchase of real estate	6	0,42
Use of cheques	5	0,35
Currency exchange transactions	4	0,28
Exchange of small-denomination banknotes	4	0,28
E-money	4	0,28
Fiscal regularisation	4	0,28
Other	17	1,18

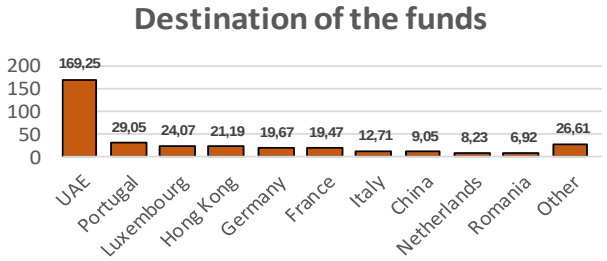


3.3. Financial flows

The table below provides an overview of the financial flows outside of Belgium in the files that CTIF-CFI reported to the judicial authorities in 2018, 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)**	**%**
France	70,01	35,42	United Arab Emirates	169,25	48,89
Switzerland	31,84	16,11	Portugal	29,05	8,39
Luxembourg	26,95	13,64	Luxembourg	24,07	6,95
Poland	12,28	6,21	Hong Kong	21,19	6,12
Netherlands	10,45	5,29	Germany	19,67	5,68
Germany	6,04	3,06	France	19,47	5,62
Hong Kong	5,33	2,70	Italy	12,71	3,67
Slovenia	5,09	2,58	China	9,05	2,61
China	4,55	2,30	Netherlands	8,23	2,38
Hungary	4,26	2,16	Romania	6,92	2,00
Other	20,85	10,55	Other	26,61	7,69
Total	**197,65**	**100**	**Total**	**346,22**	**100**



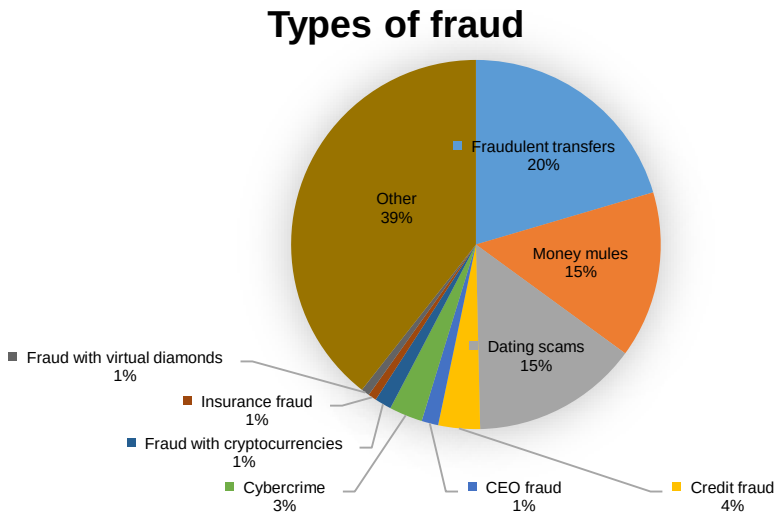


3.4. Files reported to the judicial authorities by main predicate offence

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

Predicate offence	2016	2017	2018	% 2018
Fraud	186	274	154	16,51
Social fraud[(1)]	-	18	137	14,68
Illicit trafficking in narcotics	76	130	119	12,75
Serious fiscal fraud	54	100	118	12,65
Organised crime	36	72	75	8,04
Fraudulent bankruptcy	74	89	63	6,75
Misappropriation of corporate assets	80	96	55	5,89
Terrorism, terrorist financing, including proliferation financing	112	164	48	5,14
Illicit trafficking in arms, goods and merchandise	48	42	40	4,29
Exploitation of prostitution	35	25	27	2,89
Breach of trust	15	27	24	2,57
Trafficking in human beings	20	30	20	2,14
Smuggling of human beings	-	-	17	1,83
Embezzlement and corruption	6	13	15	1,61
Theft or extortion	12	23	9	0,96
Trafficking in illegal workers	71	83	-	-
Other	6	6	12	1,30
Total	**831**	**1.192**	**933**	**100**

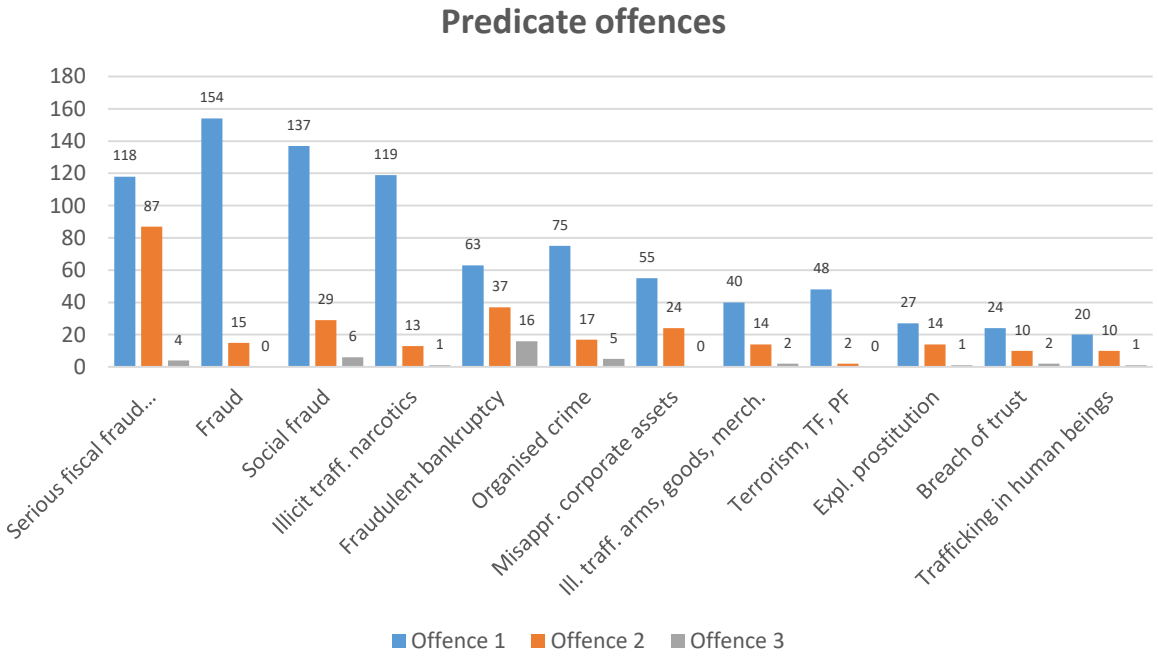
(1) Since the Law of 18 September 2017 entered into force.



Number of files reported by CTIF-CFI to the judicial authorities in 2018 according the main, second and third most important predicate offence

In one 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 2018	Main offence	Second offence	Third offence
Serious fiscal fraud, whether organised or not	205	118	87	4
Fraud	169	154	15	-
Social fraud	166	137	29	6
Illicit trafficking in narcotics	132	119	13	1
Fraudulent bankruptcy	100	63	37	16
Organised crime	92	75	17	5
Misappropriation of corporate assets	79	55	24	-
Illicit trafficking in arms, goods and merchandise	54	40	14	2
Terrorism, terrorist financing, including proliferation financing	50	48	2	-
Exploitation of prostitution	41	27	14	1
Breach of trust	34	24	10	2
Trafficking in human beings	30	20	10	1
Embezzlement and corruption	19	15	4	-
Smuggling of human beings	17	16	1	1
Theft or extortion	15	9	6	-
Trafficking in illegal workers	1	1	-	-
Other	23	12	9	2
	1.227	**933**	**292**	**41**



Predicate offences that most often occur together

The following table provides an overview of predicate offences that most often occurred together in files reported to the judicial authorities in 2018.

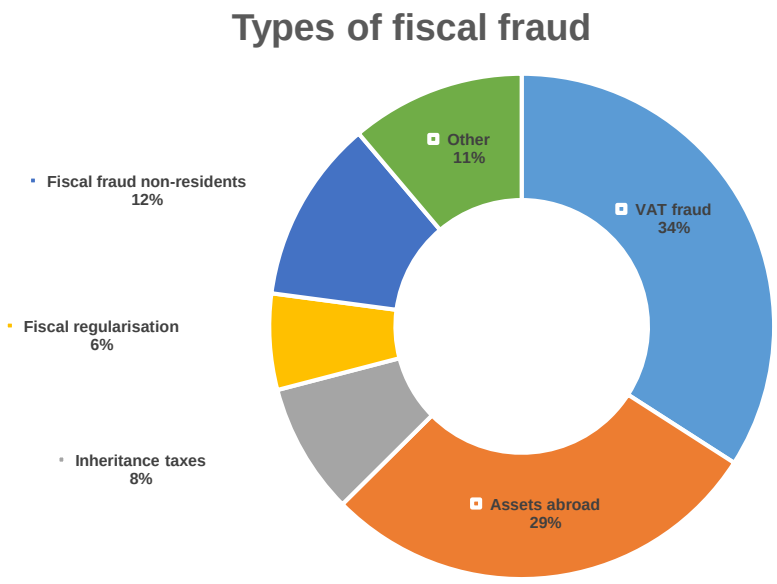
Second and third offence ---------- *First offence*	Fraud	Fiscal fraud	Social fraud	Illicit trafficking in goods and merchandise	Illicit trafficking in narcotics	Smuggling of human beings	Trafficking in human beings	Misappropr. of corporate assets	Breach of trust	Fraudulent bankruptcy	Organised crime	Exploitation of prostitution	Terrorism and TF	Other	Total
Fraud		1	3					2	5	4	4			5	24
Fiscal fraud			7	8				8	1	8				1	33
Social fraud		71			1		2	2		20	6				102
Illicit trafficking in goods and merchandise		5	3		3			2		1	1	1		3	19
Illicit trafficking in narcotics				2				2		1	5	1		2	13
Trafficking in human beings			2			1				3		8			14
Smuggling of human beings			1							1	1	3			6
Misappropriation of corporate assets	2	2	2		1			1	1	9	1				19
Breach of trust	3				1			2		2					7
Fraudulent bankruptcy	1	4	6	1	1		1	3	1					2	20
Organised crime	3	7	6	4	4		1	1		2	1		1	2	32
Exploitation of prostitution					1		8	1							10
Terrorism and TF	1														1

The offences fiscal fraud, social fraud, fraudulent bankruptcy, illicit trafficking in goods and merchandise, organised crime and misappropriation of corporate assets are the offences that most often occur together. The offences of fraudulent bankruptcy, misappropriation of corporate assets, fiscal fraud and social fraud also often linked, as well as trafficking in human beings and exploitation of prostitution. Finally, we also find that illicit trafficking in narcotics and organised crime are two offences that often occur together.

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

Predicate offence	2016	2017	2018	% 2018
Serious fiscal fraud	150,37	300,66	573,41	40,02
Illicit trafficking in arms, goods and merchandise	23,04	19,99	180,97	12,63
Social fraud[2]	-	38,65	169,17	11,81
Trafficking in human beings	14,63	9,79	120,74	8,43
Organised crime	63,14	112,14	112,23	7,83
Fraud	34,92	34,49	75,49	5,27
Illicit trafficking in narcotics	14,22	38,25	29,03	2,03
Fraudulent bankruptcy	28,70	23,90	24,94	1,74
Misappropriation of corporate assets	56,12	37,77	22,30	1,56
Embezzlement and corruption	658,99	382,77	19,85	1,39
Breach of trust	22,22	41,17	16,46	1,15
Terrorism, terrorist financing, including proliferation financing	6,66	1,20	10,89	0,76
Exploitation of prostitution	9,12	8,68	5,87	0,41
Smuggling of human beings	-	-	4,50	0,31
Theft or extortion	1,71	1,78	1,69	0,12
Trafficking in illegal workers	57,49	55,99	-	-
Other	5,49	1,45	65,19	4,54
Total	**639,36**	**1.146,82**	**1.432,73**	**100**

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



Disclosures in the files reported to the judicial authorities in 2016, 2017 and 2018 by predicate offence

	2016		2017		2018	
Predicate offence	**Number**	**Amount**[1]	**Number**	**Amount**[1]	**Number**	**Amount**[1]
Serious fiscal fraud	188	193,06	296	419,10	309	694,84
Illicit trafficking in arms, goods and merchandise	162	45,55	144	34,76	137	188,25
Social fraud[2]	-	-	42	38,65	335	184,52
Organised crime	316	81,87	384	137,44	385	162,30
Trafficking in human beings	100	15,06	103	12,84	70	122,34
Fraud	428	38,03	671	52,65	452	85,51
Fraudulent bankruptcy	138	32,72	156	25,48	145	33,96
Trafficking in illegal workers	286	74,19	226	76,69	82	32,47
Illicit trafficking in narcotics	155	16,49	328	51,03	383	31,68
Misappropriation of corporate assets	160	25,73	227	53,73	101	30,16
Breach of trust	61	58,09	105	43,07	74	21,82
Embezzlement and corruption	22	676,42	24	446,92	98	20,55
Terrorism, terrorist financing, including proliferation financing	350	10,55	448	5,97	202	14,10
Exploitation of prostitution	126	9,62	75	14,29	113	7,44
Smuggling of human beings	-	-	-	-	43	3,52
Theft or extortion	31	1,84	42	1,89	14	1,82
Other	6	2,01	14	1,44	29	65,61
Total	**2.577**	**1.285,7**	**3.285**	**1.415,95**	**2.972**	**1.700,89**

(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 reported to the judicial authorities

The table below provides the breakdown by nationality of the main person involved in the files reported to the judicial authorities in 2016, 2017 and 2018.

Nationality	2016	2017	2018	% 2018
Belgian	498	659	572	61,31
Dutch	30	53	48	5,14
Romanian	12	17	38	4,07
French	30	46	27	2,89
Portuguese	18	26	22	2,36
Brazilian	14	28	15	1,61
Turkish	17	30	11	1,18
Italian	13	30	11	1,18
Moroccan	23	26	11	1,18
Bulgarian	10	11	10	1,07
Albanian	-	5	9	0,96
Russian	10	10	8	0,86
Congolese (DRC)	7	8	8	0,86
British	3	5	7	0,75
Polish	3	5	7	0,75
Spanish	8	7	6	0,64
Nigerian	9	9	5	0,54
Iraqi	4	1	5	0,54
Hungarian	1	2	5	0,54
Pakistani	8	8	4	0,43
Guinean	-	2	4	0,43
Cameroonian	4	4	3	0,32
Swedish	-	1	3	0,32
German	1	2	3	0,32
Ivorian	10	18	-	-
Tunisian	7	11	-	-
Algerian	4	7	-	-
Syrian	3	5	-	-
Ghanaian	3	5	-	-
Malian	1	4	-	-
Beninese	-	3	-	-
Other	80	144	91	9,75
Total	**831**	**1.192**	**933**	**100**

3.6. Place of residence of the main person involved

The tables below provide the breakdown by place of residence of the main person involved in the files reported to the judicial authorities in 2018. 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 823 files reported to the judicial authorities in which the main person involved resided in Belgium.

	Number of files	**%**
Brussels	250	30,38
Antwerpen	152	18,47
Oost-Vlaanderen	69	8,38
Hainaut	65	7,90
West-Vlaanderen	58	7,05
Limburg	53	6,44
Halle-Vilvoorde	53	6,44
Liège	51	6,20
Brabant Wallon	31	3,77
Vlaams-Brabant	16	1,94
Namur	16	1,94
Luxembourg	9	1,09
Total	**823**	**100**

3.6.2. Residence abroad

The table below presents the breakdown for the 110 files reported to the judicial authorities in 2018 in which the main individual involved resided abroad.

Country of residence	From 1 January 2018 until 31 December 2018	%
France	11	10,38
Netherlands	4	3,77
Luxembourg	3	2,83
Romania	3	2,83
Switzerland	2	1,89
Albania	1	-
Algeria	1	-
Benin	1	-
Colombia	1	-
Cyprus	1	-
Czech Republic	1	-
Hungary	1	-
Israel	1	-
Kenya	1	-
Liechtenstein	1	-
Malta	1	-
Mauritania	1	-
Montenegro	1	-
New Zealand	1	-
Nigeria	1	-
Poland	1	-
Portugal	1	-
Spain	1	-
Thailand	1	-
United Kingdom	1	-
United States of America	1	-
Unknown	66	58,49
Total	**110**	**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[57]. 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 reported 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[58] for specific fraud schemes. CTIF-CFI also considers this exchange of information to be spontaneous information exchange.

In 2018, CTIF received and processed 1.798 requests for assistance from counterpart FIUs[59].

Africa (13)
Burkina Faso (1), Cabo Verde (1), Cameroon (1), Democratic Republic of the Congo (1), Ghana (2), Mali (3), Mauritius (1), Niger (1), Togo (1), Zimbabwe (1)

Americas (1.030)
Anguilla (1), Argentina (1), Aruba (1), Bermuda (1), Brazil (1), Canada (5), Chile (1), Costa Rica (1), Ecuador (1), Panama (1), Paraguay (1), United States of America (1.015)

Asia Pacific (254)
Australia (247), Bangladesh (2), Japan (1), Malaysia (1), Singapore (2), South Korea (1)

Eurasia (7)
Belarus (1), Kazakhstan (1), Russia (4), Uzbekistan (1)

Europe (488)
Albania (2), Armenia (1), Austria (2), Bulgaria (4), Croatia (1), Cyprus (5), Czech Republic (3), Denmark (2), Estonia (1), Finland (5), France (76), Georgia (1), Germany (57), Gibraltar (1), Greece (1), Guernsey (8), Hungary (2), Iceland (1), Ireland (3), Isle of Man (4), Israel (2), Italy (13), Jersey (7), Latvia (3), Liechtenstein (3), Lithuania (2), Luxembourg (131), Malta (9), Moldova (1), Montenegro (1), Netherlands (60), North Macedonia (1), Poland (4), Portugal (2), Romania (4), San Marino (1), Serbia (1), Slovakia (9), Slovenia (1), Spain (8), Sweden (2), Switzerland (13), Turkey (6), Ukraine (2), United Kingdom (22)

Middle East and North Africa (6)
Algeria (1), Lebanon (1), Saudi Arabia (1), Syria (1), United Arab Emirates (2)

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

In 2018, CTIF-CFI sent 958 requests for information to counterpart FIUs[60].

Africa (18)

Benin (3), Burkina Faso (1), Cameroon (2), Democratic Republic of the Congo (2), Gabon (1), Kenya (1), Mauritius (2), Senegal (1), South Africa (4), Tanzania (1)

Asia Pacific (59)

Afghanistan (1), Australia (2), China (9), Hong Kong (19), India (7), Indonesia (2), Japan (1), Macao (1), Marshall Islands (1), Mongolia (1), New Zealand (2), Singapore (6), Sri Lanka (1), Taiwan (2), Thailand (4)

Eurasia (17)

Belarus (1), Kyrgyzstan (1), Russia (14), Uzbekistan (1)

Europe (771)

Albania (5), Austria (6), Bulgaria (16), Croatia (1), Cyprus (7), Czech Republic (5), Denmark (3), Estonia (4), Finland (2), France (197), Germany (48), Gibraltar (3), Greece (8), Guernsey (4), Hungary (5), Ireland (3), Isle of Man (2), Israel (9), Italy (24), Jersey (2), Kosovo (3), Latvia (7), Liechtenstein (4), Lithuania (3), Luxembourg (60), Malta (7), Monaco (7), Montenegro (2), Netherlands (140), Norway (5), Poland (10), Portugal (17), Romania (13), Serbia (1), Slovakia (4), Slovenia (2), Spain (28), Sweden (4), Switzerland (29), Turkey (20), Ukraine (4), United Kingdom (47)

Middle East and North Africa (35)

Bahrain (1), Egypt (1), Iraq (1), Lebanon (6), Morocco (7), Saudi Arabia (3), Tunisia (2), United Arab Emirates (14)

Americas (58)

Argentina (2), Bahamas (3), Brazil (2), British Virgin Islands (6), Canada (4), Colombia (1), Curaçao (1), Ecuador (1), Mexico (1), Panama (5), Paraguay (1), United States of America (29), Uruguay (1), Venezuela (1)

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.

[60] Ibid.

5. JUDICIAL FOLLOW-UP

5.1. Breakdown by Public Prosecutor's Office of files reported to the Public Prosecutor between 1 January 2014 and 31 December 2018 and follow-up action by the judicial authorities[61]

	Total	%	Conv.	Ref.	Inv.	Dis.	FJA	Clos.	Enq.
Brussels	**1459**	**28,55**	**13**	**4**	**19**	**0**	**7**	**514**	**902**
Antwerpen	**772**	**15,11**	**7**	**3**	**17**	**1**	**1**	**102**	**641**
Antwerpen	609	11,92	6	3	13	1	1	82	503
Mechelen	90	1,76	0	0	4	0	0	7	79
Turnhout	73	1,43	1	0	0	0	0	13	59
Oost-Vlaanderen	**464**	**9,08**	**1**	**3**	**2**	**0**	**2**	**54**	**402**
Gent	237	4,64	0	1	1	0	1	39	195
Dendermonde	188	3,68	0	2	1	0	1	11	173
Oudenaarde	39	0,76	1	0	0	0	0	4	34
Federal Public Prosecutor's Office	**464**	**9,08**	**12**	**0**	**9**	**0**	**2**	**51**	**390**
Hainaut	**444**	**8,69**	**0**	**2**	**7**	**0**	**2**	**21**	**412**
Charleroi	199	3,89	0	0	4	0	1	7	187
Mons	152	2,97	0	1	3	0	0	5	143
Tournai	93	1,82	0	1	0	0	1	9	82
West-Vlaanderen	**323**	**6,32**	**2**	**0**	**8**	**0**	**1**	**36**	**276**
Brugge	169	3,31	1	0	2	0	0	8	158
Kortrijk	97	1,90	0	0	3	0	1	26	67
Veurne	33	0,65	0	0	2	0	0	1	30
Ieper	24	0,47	1	0	1	0	0	1	21
Liège	**296**	**5,79**	**1**	**4**	**13**	**0**	**2**	**68**	**208**
Liège	236	4,62	1	4	9	0	2	56	164
Verviers	36	0,70	0	0	4	0	0	6	26
Huy	24	0,47	0	0	0	0	0	6	18
Limburg	**246**	**4,81**	**1**	**3**	**3**	**2**	**0**	**61**	**176**
Hasselt	131	2,56	1	1	2	2	0	38	87
Tongeren	115	2,25	0	2	1	0	0	23	89
Halle-Vilvoorde	**185**	**3,62**	**0**	**2**	**0**	**1**	**0**	**54**	**128**
Nivelles	**141**	**2,76**	**1**	**1**	**1**	**0**	**0**	**18**	**120**
Namur	**114**	**2,23**	**0**	**0**	**2**	**0**	**0**	**5**	**107**
Namur	88	1,72	0	0	1	0	0	5	82
Dinant	26	0,51	0	0	1	0	0	0	25
Leuven	**111**	**2,17**	**1**	**0**	**0**	**0**	**1**	**3**	**106**
Luxembourg	**74**	**1,45**	**0**	**0**	**2**	**0**	**0**	**7**	**65**
Arlon	33	0,65	0	0	0	0	0	4	29
Neufchâteau	22	0,43	0	0	2	0	0	2	18
Marche-en-Famenne	19	0,37	0	0	0	0	0	1	18
Eupen	**17**	**0,33**	**0**	**0**	**0**	**0**	**0**	**5**	**12**
	5.110	**100**	**39**	**22**	**83**	**4**	**18**	**999**	**3.945**

Key:
Conv.: conviction
Acq.: acquittal
Ref. : referred to the Criminal Court
Inv. : ongoing judicial investigation
Dis. : court dismissal
FJA : case handed over by the Belgian judicial authorities to foreign judicial authorities
Clos. : case closed by the Public Prosecutor's Office
Enq. : ongoing police enquiry

[61] This table was drawn up based on the information and the copies of judgments held by CTIF-CFI on 31 January 2019 and that were spontaneously sent to CTIF-CFI in accordance with Article 82 § 3.

5.2. Judicial follow-up – fines and confiscations

The table[62] below provides an overview of the fines and confiscations imposed by courts and tribunals, (amounts in EUR) in files reported to the judicial authorities in the past five years (2014 to 2018) 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 five years. This is the case for files related to economic and financial crime, which account for more than 50% of the reported files. Moreover, for some decisions an appeal was lodged.

	Fines 2014 to 2018	**Confiscations 2014 to 2018**	**Total**
Brussels	**2.332.645**	**27.826.182**	**30.158.827**
Antwerpen	**1.086.400**	**43.620.765**	**44.707.165**
Antwerpen	1.006.500	41.604.830	42.611.330
Turnhout	73.900	2.105.935	2.179.835
Mechelen	6.000	-	6.000
Oost-Vlaanderen	**2.338.950**	**9.955.167**	**12.294.117**
Gent	2.338.950	9.887.822	12.226.772
Dendermonde	-	67.345	67.345
Oudenaarde	-	-	-
West-Vlaanderen	**125.800**	**-**	**125.800**
Brugge	125.800	-	125.800
Veurne	-	-	-
Hainaut	**314.800**	**234.755**	**549.555**
Mons	55.600	234.755	290.355
Charleroi	259.200	-	259.200
Tournai	-	-	-
Limburg	**59.000**	**359.000**	**418.000**
Hasselt	59.000	359.000	418.000
Tongeren	-	-	-
Liège	**78.700**	**9.497.047**	**9.575.747**
Liège	70.200	9.497.047	9.567.247
Huy	8.500	-	8.500
Verviers	-	-	-
Namur	**12.750**	**239.400**	**252.150**
Namur	5.250	221.900	227.150
Dinant	7.500	17.500	25.000
Brabant Wallon	-	-	-
Leuven	-	-	-
Luxembourg	-	-	-

[62] This table was drawn up based on the information and the copies of judgments held by CTIF-CFI on 31 January 2019 and that were spontaneously sent to CTIF-CFI in accordance with Article 82 § 3.

Marche-en-Famenne	-	-	-
Total	**6.349.045**	**91.732.316**	**98.081.361**

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.