23RD ANNUAL REPORT
2016

Belgian Financial Intelligence Processing Unit

ctif cfi

Belgian Financial Intelligence Processing Unit

23rd Annual Report
2016

TABLE OF CONTENTS

I. PREFACE BY THE DIRECTOR

Since the anti-terrorist raids in Verviers, the attacks in Paris in November 2015 and the attacks in Brussels in March 2016, Belgium has faced an increased terror threat. The evolution of Daesh in Iraq and Syria, combined with the issue of Foreign Terrorist Fighters who went to war zones controlled by Daesh, has considerable impact on the threat level in our country and in Europe.

CTIF-CFI has paid particular attention to terrorism and terrorist financing in 2016 and also dedicated a large part of its resources to these issues. The number of files related to terrorist financing that CTIF-CFI analysed and reported to the judicial authorities rose sharply in 2015 and 2016. The files related to terrorist financing make up 13,48 % of the files reported to the judicial authorities in 2016 (112 files), compared to only 7,6 % in 2015 (75 files) and 3,3 % in 2014 (37 files).

Financial intelligence is becoming an essential part of criminal investigations related to organised crime and terrorist financing, as was recently highlighted by Europol.

Recent events in London, in Berlin in December, in the Notre-Dame Cathedral in Paris, and at Central Station in Brussels not so long ago demonstrated that the terrorist threat is increasingly fragmented and therefore harder to predict. As a result, there is a great need for synergies between the various competent authorities.

To meet this need for synergies CTIF-CFI has strengthened its cooperation with the Federal Public Prosecutor's Office and the Belgian (civil and military) intelligence services, as well as its foreign counterparts, including the French, Luxembourgish, Dutch, German, British, Swiss and American FIUs, who face the same challenges in terms of security.

The Minister of Justice is currently examining the feasibility of setting up a Joint Intelligence Task Force, a partnership with the private sector, similar to the one in United Kingdom, for instance.

In 2016, there was another sharp rise in the number of new files processed by CTIF-CFI (+12,38 %), despite the small decrease in the number of disclosures (-3,5 % compared to 2015 and -1,8 % compared to 2014), following the considerable increase between 2012 and 2014 (+35%).

This increase in the number of new files is the result of awareness-raising campaigns of professional bodies, supervisory authorities of the professionals subject to the anti-money laundering and terrorist financing framework (financial sector, notaries, accounting professions, lawyers,…).

Enhanced cooperated was initiated in this respect in 2016 between CTIF-CFI and the *Ordre des barreaux francophones et germanophone de Belgique* [French-speaking and German-speaking Bar Association of Belgium] (OBFG). This demonstrates the awareness that money laundering and terrorist financing prevention is essential, in compliance with the bars' code of conduct.

Page 11 of this report includes a detailed overview of the key figures of 2016.

Yet figures should be interpreted correctly. The figures regarding the files reported to the judicial authorities (page 11 and 55-65) relate to potential money laundering or terrorist financing that, based on the elements and information held by CTIF-CFI, it decided to forward to the judicial authorities, in accordance with the provisions of Article 34, second subparagraph of the Law of 11 January 1993. The judicial authorities may conduct additional enquiries, where appropriate, and subsequently entirely independently decide whether prosecution is useful and appropriate.

To safeguard ongoing criminal investigations the most confidential elements were removed from the section on terrorist financing.

The terrorist threat must not distract us, however, from the new challenges society currently faces.

We should first and foremost adjust to the digital revolution (new digital payments, FinTech, virtual currencies) and measure the impact of this revolution on the approach of tackling money laundering, terrorism and (financial) crime in general.

CTIF-CFI and the Financial Services and Markets Authority (FSMA) have laid the foundations of a strategic partnership to correctly assess the consequences of this digital revolution.

This digital revolution involves a large-scale decentralisation of the economy and finance.

This points to a revolution in our behaviour and new uses, especially so in the financial sector (banking, insurance and money remittance). These applications have already become a reality in our daily lives. We are able to carry out secure financial transactions almost instantly, in currencies that are not always legal tender, for minimal (transfer) fees and without the supervision of a central supervisory authority (bank or central bank). Moreover, some applications were developed and are provided by other intermediaries (technology companies), which are not the usual financial intermediaries.

A radical social transformation is taking place in the financial sector. This change will undoubtedly have a significant impact and repercussions on our approach of money laundering and terrorist financing.

We should be aware of this and tackle tomorrow’s challenges.

20 July 2017

Philippe de KOSTER
Director

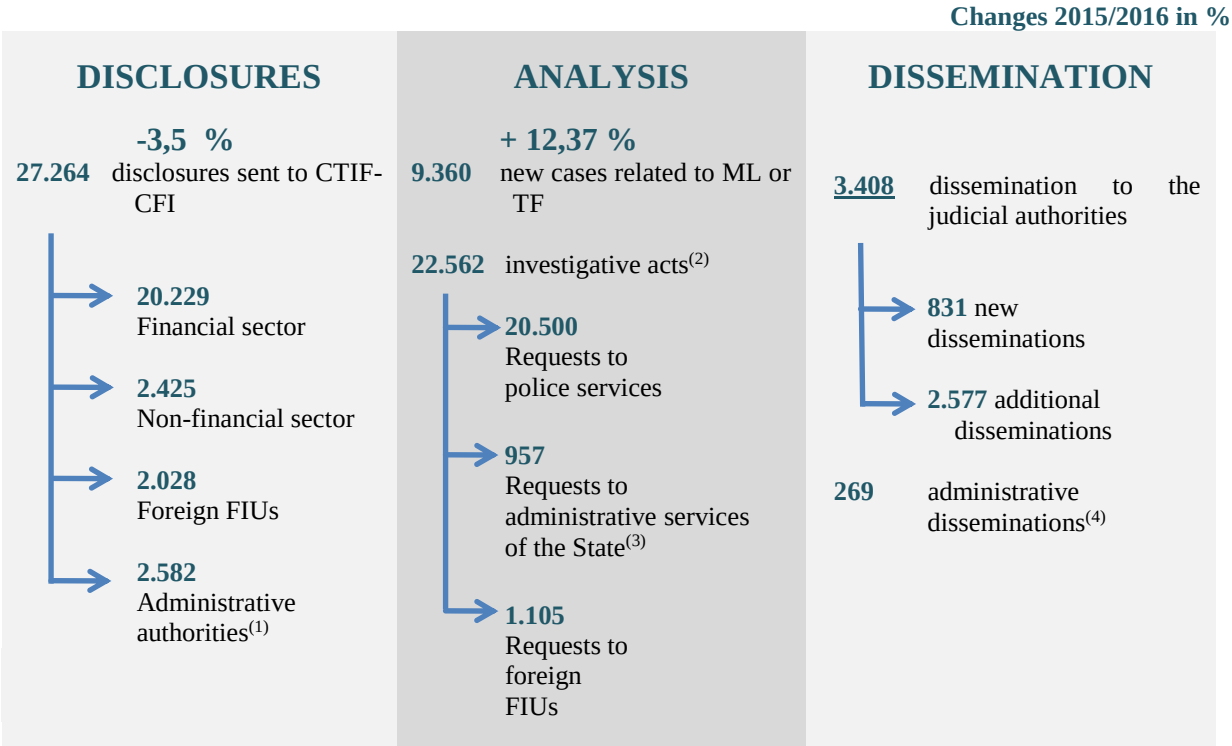
II. COMPOSITION OF CTIF-CFI[1]

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

[1] Situation on 31 December 2016.

III. KEY FIGURES 2016

CTIF-CFI's mission is to receive disclosures of suspicious transactions from institutions and persons mentioned in the law (referred to as disclosing entities), from foreign FIUs as part of international cooperation and from other services of the State, as referred to in the law. CTIF-CFI analyses and enhances 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. For a few years now, CTIF-CFI has been required to notify the unit "Anti-fraud Coordination (CAF)" of Federal Public Service Finance when the information reported to the Public Prosecutor relates to laundering the proceeds of an office related to serious fiscal fraud, whether organised or not, or an offence for which the customs authorities are competent, and the *Service d'Information et de Recherche Social/Sociale Inlichtingen- en Opsporingsdienst* [Social Information and Investigation Department] when the information reported to the Public Prosecutor concerns laundering the proceeds of offences that may have repercussions in terms of social fraud, and the Prosecutor at a labour tribunal when the information reported to the Public Prosecutor concerns laundering the proceeds of an offence related to trafficking in illegal labour or in human beings. To tackle the security threat, it has been legally possible for CTIF-CFI since 2016 to cooperate more closely with the intelligence services and the Coordinating Unit for Threat Analysis (OCAM-OCAD). CTIF-CFI can now contextualise requests for information it sends to these three services. As part of mutual cooperation (cf. Article 35 of the Law), CTIF-CFI can also send useful information to the intelligence services and OCAM-OCAD.



(1) Disclosures of cross-border transportation of currency, fiscal regularisations (DLU-EBA*ter*), disclosures by officials of the administrative services of the State pursuant to Article 33 of the AML/CFT Law.

(2) These figures do not include (additional) requests for information that CTIF-CFI's analysts send to disclosing entities and persons pursuant to Article 33, nor the checking of commercial databases.

(3) Tax authorities, social inspectorate, State Security Department (VSSE), General Intelligence and Security Service of the Armed Forces (SGRS-ADIV), pursuant to Article 33 of the AML/CFT Law.

(4) Information sent to the unit "Anti-fraud Coordination (CAF)" of the Federal Public Service Finance, the Labour Prosecutor's Offices, Social Information and Investigation Department (SIRS-SIOD) pursuant to Article 35 of the AML/CFT Law.

The number of disclosures sent to CTIF-CFI rose sharply in recent years, a 35% increase since 2012. The number of new files opened as a result of these disclosures has more than doubled since 2012.

- **27.264** disclosures sent to CTIF-CFI
- **9.360** cases. CTIF-CFI groups the information received that relates to the same case into one case. CTIF-CFI's analytical department always processes all information received.
- **22.562** investigative acts (police requests, administrative requests or requests to foreign FIUs) to enhance disclosures.
- **831** files and **2.577** additional reports sent to Public Prosecutor's Offices and the Federal Public Prosecutor's Office, for a total amount of **EUR 1.285,68 million**
- **269** information notes were sent to the unit "Anti-fraud Coordination (CAF)" of the Federal Public Service Finance, the Prosecutors at a labour tribunal, Social Information and Investigation Department (SIRS-SIOD), the Central Office for Seizure and Confiscation (OCSC-COIV), the intelligence services and the Coordination Unit for Threat Analysis (OCAM-OCAD) pursuant to Article 35 of the AML/CFT Law.

The rise in the number of opened files is a result of the increase in the number of disclosures from credit institutions (+12 % compared to 2015 and + 24 % compared to 2014), and from foreign FIUs (twice as many as in 2015 and four times as many as in 2014).

Part IV contains an overview of money laundering and terrorist financing trends in 2016. A detailed overview of the statistics of 2016 is included in the annex.

IV. MONEY LAUNDERING AND TERRORIST FINANCING TRENDS

The first part of this report illustrates the threats that CTIF-CFI identified on the basis of files reported to the judicial authorities in 2016. With respect to money laundering, these are criminal threats linked to organised crime groups, drug trafficking networks, human trafficking and smuggling networks. These threats also refer to various types of financial crime and corruption. The terror threat and terrorist financing are also discussed.

The second part relates to sectors that are particularly vulnerable with regard to money laundering: the building industry, the art and antiques trade, precious stones and precious metals, the hotel and catering industry, retail trade and second-hand cars.

The third part is dedicated to emerging risks related to financial technological innovations (FinTech). Although FinTech has many advantages, there are also great challenges in respect of combating money laundering and terrorist financing. FinTech facilitates greater anonymity and can hamper the traceability of transactions, and these risks need to be addressed.

The money laundering and terrorist financing trends identified by CTIF-CFI in the files reported to the judicial authorities in 2016 are illustrated below using concrete elements from the files' operational analysis. In order to distinguish the operational analysis elements, these are printed in blue.

1. Threats

The FATF defines a "threat" as a person, a group of people or activity, that due to its inherent nature, could endanger or cause harm to society[2].

To identify these threats it is essential to have a current understanding of the environment in which predicate money laundering offences are committed and terrorist financing activities evolve. Based on the files reported to the judicial authorities in 2016, CTIF-CFI identified several threat categories, for money laundering as well as for terrorist financing.

1.1. Money laundering threats

1.1.1. Organised crime groups

Financial flows from multiple criminal activities

One of the main elements of organised crime is the fact that criminal organisations are involved in various forms of criminal activities. Organised crime is a multifaceted problem and multiple criminal activities are committed. Globalisation, new technologies and the economic crisis have contributed to the increase and diversification of activities linked to organised crime. Many criminal groups have become increasingly opportunistic and switch from one offence to the next because of operational advantages or higher profits. According to the SOCTA 2017 report published by Europol, the number of groups involved in multiple criminal activities rose sharply in recent years: currently 45% (compared to 33% in 2013)[3].

---

2 FATF Guidance for Countries on assessing money laundering and terrorist financing risk – October 2012 (www.fatf-gafi.org)

3 EUROPOL SOCTA 2017, Crime in the age of technology.

Analysis of the files that CTIF-CFI reported to the judicial authorities because of organised crime shows that the laundered funds are the proceeds of multiple criminal activities. In a number of files, dozens of individuals changed British pounds into euros, for a total amount of several million euros. These individuals came from the same regions in Eastern Europe, without any link with Belgium. Despite there not being a link with Belgium, they repeatedly travelled to Belgium to carry out numerous currency exchange transactions, without ever explaining why they chose to come here. Over a period of a few months, these individuals changed in excess of one million euros. Even considered individually, these were large transactions. The document numbers revealed that they intentionally structured their transactions and that these people were couriers. They carried out the currency exchange transactions in succession. Several individuals were known to the Belgian and foreign judicial authorities and police for serious offences related to organised crime (drug trafficking, human trafficking, exploitation of prostitution,…), making it difficult to link this to a specific offence.

Financial flows enable us to get to the top of the criminal or terrorist organisation, where the money is accumulated. The Framework Policy Document Comprehensive Security [*Note-cadre de Sécurité intégrale / Kadernota Integrale Veiligheid*] 2016-2019 states that the chance of dismantling such groups, or at least seriously disrupting their illegal activities, is sometimes greater when cutting off criminal financial flows rather than solely tackling the predicate offence[4].

Money laundering activities are becoming increasingly professional

The second element of organised crime is the way in which criminals organise themselves, i.e. the organised aspect of their activities. According to Europol, more than 5000 international organised crime groups, involving more than 180 nationalities, are currently being monitored in the European Union[5].

These structures, which used to be very hierarchically structured and centralised, have increasingly been replaced by groups that are part of a network, which are more flexible, mobile and prefer to use electronic means of telecommunication. They work together to take advantage of new opportunities. These structures can operate internationally, using partners, in many fields and countries, in order to reduce costs and maximise profits. Some of CTIF-CFI's cases reported to the judicial authorities feature managers of shops selling luxury goods who use their private accounts to pay invoices using various national and international counterparties. These payments were only partially explained or not at all. Even though it could initially be considered to be a commercial transaction that was not fully declared to the tax authorities, CTIF-CFI repeatedly identified indications of money laundering organised by multi-criminal organisations. Further analysis of the counterparties showed that nearly all of them could be linked to criminal activities, ranging from drug trafficking, CEO fraud, serious tax fraud or organised crime. These managers are key players of international criminal networks that launder funds under the pretext of purchasing goods. Traceability of funds is often hampered by using online betting services or foreign payment services. Criminals are becoming increasingly competent and efficient in using technology, so this is probably the greatest challenge for law enforcement authorities, including in the European Union[6].

---

4 Federal Police, Framework Policy Document Comprehensive Security [*Note-cadre de Sécurité intégrale / Kadernota Integrale Veiligheid*]

5 EUROPOL SOCTA 2017, Crime in the age of technology.

6 EUROPOL SOCTA 2017, Crime in the age of technology.

For laundering they can be assisted by white-collar criminals who, while not actually belonging to criminal organisations, have mutually lucrative business relations with them[7]. CTIF-CFI's files reported to the judicial authorities frequently indicate that self-laundering is gradually replaced by increasingly professional money laundering, which has become an activity in itself. Professional money laundering networks are providers of money laundering services to launder the proceeds of a wide range of offences, to which they cannot be directly linked.

1.1.2. Drug trafficking networks

Illegal drugs, still a thriving market

The illegal drug market still yields large sums of money that can be laundered. In terms of the estimated turnover, cannabis still takes the bulk of the illegal drug market in Europe, followed by heroin, cocaine, amphetamines and MDMA[8]. A new trend is that the supply of substance is on the rise and psychoactive substances are now also manufactured in Europe, near consumer markets.

As to the current situation of the Belgian market, the professional manufacturing of cannabis (cannabis factory) and synthetic drugs is a common problem[9]. Apart from the Iberian Peninsula, Belgium is also one of the main points of entry of cocaine and heroin in Europe, hidden in containers shipped to the port of Antwerp[10].

Taking into account the revival of the drug market, the large quantities of drugs seized and the large amounts of money these drug networks yield, it is important to recognise that the number of disclosures and files CTIF-CFI reports to the judicial authorities still remains low.

7 European Parliament, Report on organised crime, corruption and money laundering: recommendations on action and initiatives to be taken (final report) (2013/2107(INI)), 2013

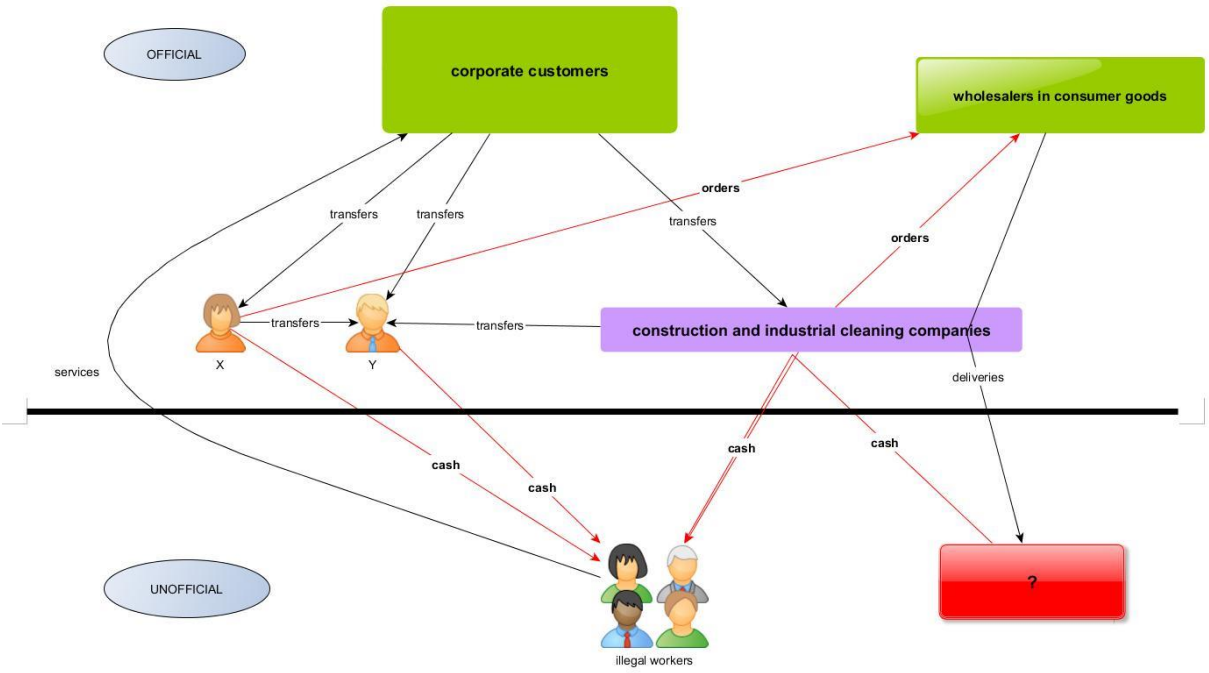
8 European Monitoring Centre for Drugs and Drug Addiction, EU Drug Markets Report, 2016

9 European Monitoring Centre for Drugs and Drug Addiction, EU Drug Markets Report, 2016

10 European Monitoring Centre for Drugs and Drug Addiction – EUROPOL, EU Drug Markets Report: In-depth Analysis, 2016

Part of the explanation could be the increasing use of strategies to bypass the banking system, in order to avoid banking transactions that financial institutions could find suspicious.

CTIF-CFI has repeatedly identified and illustrated the "offsetting technique" (also referred to as "compensation technique") in its annual reports, for the first time in 2014. This technique mainly takes place outside of the conventional banking system, making it difficult for disclosing entities to detect such schemes. The funds, proceeds of drug trafficking for instance, are laundered without the use of the conventional banking system, which are therefore not detected by banks' normal monitoring systems. In several of CTIF-CFI's files, a number of corporate customers transferred funds, with reference to the payment of invoices, to the accounts of construction and industrial cleaning companies. Debit transactions from the accounts included large cash withdrawals and transfers to companies trading in consumer goods (tobacco, drinks, sweets).



Many of the companies who carried out the transactions featured in files that CTIF-CFI had reported to the judicial authorities, mainly related to trafficking in illegal workers. Most of the withdrawn cash was undoubtedly meant to pay illegal workers. No explanation was provided for the financial transactions between these companies, the company objects were also unrelated. In reality, these transactions could have been carried out as part of an "offsetting scheme". The construction and industrial cleaning companies would pay the orders of goods to wholesalers of consumer goods on behalf of third parties, who would give them cash in exchange for these transactions or transfers. This way the construction and industrial cleaning companies did not have to use the financial system to withdraw cash from their accounts. The cash could be used to pay illegal workers. These third parties were presumably individuals / companies from industries generating large amounts of cash. The cash could have been generated through illegal (retail) trade and/or criminal activities.

In some cases the indication of laundering the proceeds of drug trafficking was strengthened by police information revealing links between the companies' managers in the construction and industrial cleaning industries and the individuals behind international drug trafficking to Europe. The "offsetting technique" was probably used to launder the proceeds of international drug trafficking. In this case, cash proceeds of drug trafficking were handed over and used to pay illegal workers in the construction and cleaning industries. These funds were ultimately invested in the legal economy (via transfers) by purchasing consumer goods.

Changing trafficking methods: the online drug market

Illegal drug trafficking used to take place on physical locations, yet new technologies have led to the development of online markets. These markets either use the visible Internet or invisible websites on the darknet.

Darknet[11]

The world wide web consists of the surface web (some 10% of the world wide web), whose contents is indexed by conventional search engines. The remaining 90% is the deep web, whose content is not indexed by conventional search engines. This deep web contains the darknet, a stacked layer of the network structure that can only be accessed with specific software and configurations or authorisation, often via non-standard ports and communication protocols. The darknet contains online market places trading in various types of illegal goods: drugs, weapons, explosives, fake identity cards, in exchange for virtual currencies. Identifying and locating criminals that operate on the darknet is very complicated and requires resources and enhanced international cooperation.

As to the substances purchased online, the majority of the drugs are shipped in parcels. To avoid parcels being detected no sender is mentioned on the parcels or a fake delivery address is used. Moreover, the drugs are packaged to ensure the contents are concealed as much as possible. The parcels are delivered to post boxes, at the buyer's home, to a third party or a regular postal address. Several credit transactions were carried out, transfers from electronic money institutions under British law with an account in a different country to personal accounts in Belgium. The involvement of an electronic money institution made it difficult, or even impossible, to identify and check the origin of the funds. For these transactions reference was made to a bitcoin exchange platform. Virtually all funds were subsequently withdrawn in cash. In several cases police information enabled us to link account holders to trafficking in synthetic drugs, sold on the darknet, delivered in parcels and paid in bitcoins. The money was laundered by changing bitcoins into EUR.

[11] Yves Charpenel, *Le DARKWEB, la face cachée d'internet,* Dalloz IP/IT, February 2017, page 71 to 96.

Various strategies were used to conceal transactions, such as the use of anonymisation services to conceal a computer's IP address or the use of virtual currencies to carry out payments (see part 3 of this report)[12].

1.1.3. Human trafficking and human smuggling networks

Sexual exploitation networks

Human trafficking takes place in many sectors, but the largest number of victims is recorded in cases of sexual and economic exploitation[13].

In Belgium, the policy for combating human trafficking and smuggling is mentioned in various strategic documents, some of which were recently updated. This includes the action plan 2015-2019 of the Interdepartmental Unit of Coordination for Human Trafficking Prevention. This unit is a national coordination body for this policy area, chaired by the Minister of Justice. CTIF-CFI has been a member since 2014.

The action plan highlights the importance of financial investigations with regard to human trafficking and stresses CTIF-CFI's role in this regard. Detecting and tracing financial flows is essential to identify networks, destabilise criminal organisations and deprive them of their assets. As part of this action plan, CTIF-CFI committed to contribute to awareness-raising of financial, legal and accounting professions in order to increase the quality and quantity of disclosures to CTIF-CFI[14].

One of the aspects of human trafficking is the exploitation of people in the world of prostitution. In Belgium, prostitution generated an estimated turnover of EUR 870 million in 2015[15]. Sexual exploitation can involve various aspects and differ according to the circumstances. There has been a shift from visible forms of sexual exploitation to more hidden forms. Especially Nigerian networks and networks from Eastern Europe (Romania, Bulgaria and Albania) are the most active ones in Belgium.

---

[12] EUROPOL SOCTA 2017, Crime in the age of technology ; European Monitoring Centre for Drugs and Drug Addiction, The Internet and the drug markets – Insights, 2016.

[13] Trafficking in human beings is a criminal offence (Article 433*quinquies* of the Penal Code et seq) consisting of recruiting, transporting, lodging, sheltering a person, taking or transferring control over this person for exploitation purposes. The Law mentions five types of exploitation: sexual exploitation, exploitation by carrying out work inconsistent with human dignity, exploitation of begging, trafficking in organs and the fact of compelling a person to commit a crime or a serious offence.

[14] The information note for the disclosing entities will be published by the end of 2017.

[15] Adriaenssens Stef, Hendrickx Jef, Heylen Wim, Machiels Thomas, *A direct measure of output in prostitution in Belgium, KU Leuven, Faculty of Economics and Business*, September 2015. According to this study by the National Bank and KU Leuven more than half of the turnover of prostitution consists of escort services and private services. Window prostitution represents EUR 149 million, followed by massage parlours (119 million), clubs (90 million) and street prostitution (5,5 million).

Asian massage parlours

The number of massage parlours is on the rise in Belgium. The city of Antwerp, for example, noticed an increase by 43 % of the number of new massage salons. There is a shift from Chinese restaurants, which are subject to increasing inspections, to Asian massage parlours. The files reported to the judicial authorities indicated the following elements with regard to the individuals involved: the use of bogus self-employed people and/or front men, dormant companies that suddenly become active, multiple companies are set up simultaneously, multiple companies in name of the same owner, and managers often change and operate the same massage parlours, the registered office is also frequently moved. With respect to the transactions, these files often feature many cash deposits, as well as exchange transactions where small-denomination banknotes are changed into large-denomination banknotes, or transfers to Asia or to individuals of Asian origin. Other offences are also identified in connection with massage parlours, such as forged accounting, arrears in social security, successive bankruptcies, tax evasion, etc.

Another aspect of human trafficking involves economic exploitation. Few sectors are spared from this issue. The building, cleaning, transport and the hotel and catering industry are hardest hit, although there were also victims among domestic staff and seasonal workers.

Operators set up complex structures to avoid detection or to conceal their responsibility ("bogus self-employed", subcontractors,…). Front companies are also used, whose articles of association are often changed, including a succession of new managers, changes to the company name, broadening the company objects or moving the registered office. Ultimately, these companies are cleared out and declared bankrupt. Sometimes front men or forged documents are also used, as well as the organisation of insolvency. These files have following characteristics: frequent use of cash (deposits and withdrawals), domestic transfers in sensitive industries (building industry, industrial cleaning,…), followed by cash withdrawals or money remittance to countries known to provide illegal workers.

In more complex files, CTIF-CFI has found that criminals are becoming increasingly professional. This is particularly the case when the "offsetting technique" is used, with Asia for example. In several files unusual financial transactions were carried out on personal accounts, even though account holders did not carry out any professional or commercial activities in their own names. These transactions were mainly payments of invoices by order of building or industrial cleaning companies, followed by cash withdrawals (mainly prior to 2016) and international transfers to companies with accounts in China and in Hong Kong (after 2016). The international transfers were carried out in exchange for cash. These criminal groups, who have large amounts of cash at their disposal, make this cash available to companies employing illegal workers. This cash is used to pay illegal workers employed by these companies. In exchange, these companies carry out international payments, with fake invoices as supporting documents.

Migrant smuggling

Smuggling of human beings is where smugglers, in exchange for large amounts of cash, organise the illegal transport of migrants. This only refers to foreigners from countries outside of the European Union. This is commonly known as migrant smuggling. Smuggling of human beings is the fastest growing offence in Europe in 2015[16].

According to a joint report by Europol and Interpol, travel by 90% of the migrants to the European Union is predominantly facilitated by members of a criminal network, in exchange for large amounts of money. Europol estimates that these criminal networks generated a turnover between EUR 3 and 6 billion in 2015 alone, and that this amount could double or treble in 2016[17]. Europol and Interpol expect a rise in sexual or economic exploitation of migrants in the coming years, especially in the country of destination, as they need to repay their debt to smugglers[18].

CTIF-CFI's experience shows that human trafficking networks range from fairly simple (with a few people involved) to quite complex (which are so complex and organised they can be regarded as a genuine criminal organisation). CTIF-CFI found that, in the files related to migrant smuggling reported to the judicial authorities, cash was deposited on accounts of legal persons (in particular night shops). Police information showed that individuals use their illegal activities to conceal a network of illegal immigration. Although the commercial activities of these companies could provide an explanation for these cash deposits, given the police information, it is probable that, at least part of these deposits, could be linked to the proceeds generated by smugglers.

1.1.4. Financial crime

An increasing number of files related to serious fiscal fraud

The files analysed by CTIF-CFI and reported to the judicial authorities because of fiscal fraud cover various areas: fiscal regularisation, inheritance taxes, life insurance, VAT and legal arrangements aimed at avoiding tax abroad.

Various measures have facilitated the exchange of tax information and improved fiscal transparency, thanks to various obligations such as disclosing accounts abroad, disclosing to the Central Point of Contact at the National Bank of Belgium, disclosing any life insurance policies and legal arrangements.

The Law establishing a permanent system for fiscal and social regularisation (also referred to as "DLU-EBA *quater*") came into force on 1 August 2016. Belgian tax payers have another chance to regularise professional income, income from moveable and immoveable assets and various income that they did not disclose to the tax authorities.

---

[16] *Joint Europol-Interpol Report*, *Migrant smuggling networks*, *Executive summary*, May 2016; https://www.europol.europa.eu/content/europol-and-interpol-issue-comprehensive-review-migrant-smuggling-networks

[17] Europol, *Migrant Smuggling in the EU*, February 2016. Available at: https://www.europol.europa.eu/

[18] *Joint Europol-Interpol Report*, *Migrant smuggling networks*, *Executive summary*, May 2016,: https://www.europol.europa.eu/content/europol-and-interpol-issue-comprehensive-review-migrant-smuggling-networks.

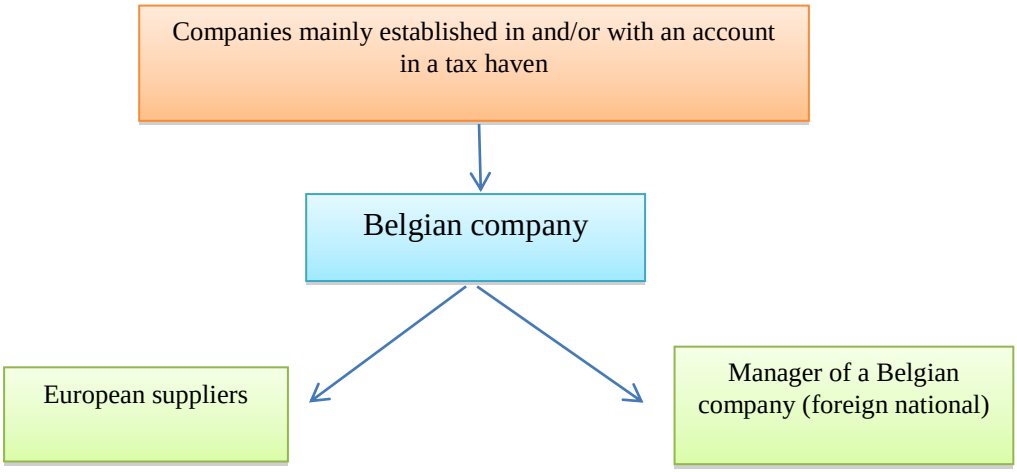
As with the previous regularisation scheme it will be void if the income, sums, VAT transactions or capital are the proceeds of illicit activities or if the regularisation is used for money laundering purposes. CTIF-CFI's role consists of checking whether the fiscal regularisation is not used for money laundering purposes and that the funds derive from regularised fiscal fraud. In some files reported to the judicial authorities, CTIF-CFI found that the accounts of Belgian customers often received international transfers from insurance companies in a neighbouring country. The explanation provided was that several life insurance policies were liquidated. Before moving these funds these people carried out a fiscal regularisation (DLU-EBA*ter*), for the moveable assets generated by investing funds on foreign accounts. Nothing was done, though, to regularise any fiscal fraud prior to the investments. Yet these files showed that fiscal fraud had been committed. Not disclosing assets abroad to the tax authorities was aimed at concealing this fiscal fraud. Moving these funds and their subsequent use can be considered to be the laundering of proceeds of serious fiscal fraud.

With respect to life insurance, the due diligence mainly consists of detecting atypical transactions prior to and after taking out the policy. The reporting entities in this industry must therefore be constantly vigilant, life insurance companies, as well as non-exclusive insurance intermediaries. Close cooperation between CTIF-CFI and the FSMA will increase the industry's awareness. In this regard CTIF-CFI and the FSMA recently published a joint statement for non-exclusive insurance intermediaries dealing in life insurance policies[19].

Files related to VAT carrousel fraud indicate that Belgium is still used by fraudsters to launder proceeds of this crime. Another trend is that Belgium is used to set up fraudulent legal arrangements for tax avoidance abroad or to launder the proceeds of this fraud in Belgium. In these files CTIF-CFI informs its foreign counterparts to whom this fraud is of concern, to share information as part of effective and enhanced international cooperation.

[19] Statement on combating money laundering and terrorist financing: summary of the main obligations of non-exclusive insurance intermediaries, FSMA_2016_16 dated 20 September 2016.

In several files, CTIF-CFI identified financial flows carried out by a Belgian company set up by foreign nationals. These flows can be illustrated as follows:



Various elements indicate that setting up a company in Belgium and the transactions on the account were part of a plan exclusively aimed at avoiding taxes owed by foreign nationals in a country where they carried out their commercial activities, and at laundering the proceeds of this fiscal fraud. To this end, they set up a complex network of Limited companies in a tax haven, to which the proceeds of their commercial activities were sent. The European suppliers were reluctant to be paid by Limited companies in sensitive countries. To safeguard their commercial activities with their European suppliers they therefore set up a second layer of the arrangement, a company under Belgian law, as an intermediary between the Limited companies and the European companies. This Belgian company's account (which received transfers from the Limited companies) was used to pay suppliers, in order to avoid any direct links with Limited companies. Although the Belgian company complied with the fiscal and social requirements, it enabled the laundering of the proceeds of fiscal fraud to the detriment of foreign tax authorities.

Operation Russian Laundromat[20]

According to the *Organized Crime and Corruption Reporting Project* (OCCRP) at least 20 billion dollars of Russian funds were laundered during an operation dubbed "Russian laundromat". It led investigators to a vast network of offshore companies, enabling their owners to remain anonymous. The funds were the proceeds of embezzlement of the Russian Treasury because of fraud, forged State contracts or tax evasion using more than 732 banks in 96 countries. Over 500 people are said to be involved. Investigations are ongoing in several countries.

[20] https://www.occrp.org/en/laundromat/

It should be noted that Belgian courts are also competent with regard to proceeds of crimes committed abroad, laundered in Belgium. Prosecution of laundering sums illegally obtained abroad does not require the identification of the crime or serious offence through which the assets were obtained, nor that the prosecution of that crime is part of the Belgian judge's jurisdiction[21].

Fraud: one goals, several variations

Fraud has been the most common predicate offence for a number of years now in the files reported to the judicial authorities. The laundered funds are the proceeds of various types of fraud.

Nigerian fraud and its variations (fake lottery, fake inheritance, romance scam,…) consists of victims being asked to advance certain costs that are never paid back.

In fraud cases involving "fraudulent transfers" fraudsters obtain a company's customer list and send an e-mail requesting to pay the next invoices by transferring the money to a new bank account number, this account is managed by the fraudsters.

In cases of CEO fraud, fraudsters pretending to be a manager (usually the CEO or CFO) approach an employee or a senior member of staff of this company in an attempt to convince this person to transfer money to an account held by the fraudsters, contrary to internal procedures.

Prevention remains the best way to combat these various types of fraud, by informing the public of the fraudsters' modus operandi[22]. Thanks to awareness-raising campaigns and more effective case management of such fraud cases, CTIF-CFI has found that the number of cases reported to the judicial authorities has fallen in recent years, even though this number is still high.

In recent months, CTIF-CFI found that fraud related to the trade in binary options is being committed. Many investors are approached to enter into contracts with binary options. They have to put money on a prediction of the short-term (ranging from a few minutes to a few days) evolution of the price of assets (share index, foreign currency or commodity). If the prediction proves correct, the investors get their money back and gain a profit. If they are wrong, they lose all of the invested money.

[21] Cass., 20 November 2013, P.13.1105.F

[22] Please refer to the information and awareness-raising brochure of the Federation of Enterprises in Belgium, the economic professions (company auditors, accountants and tax consultants) that Febelfin, UNIZO, UCM and the judicial police of Brussels (National and International Fraud Office) published in 2015, https://www.ibr-ire.be/nl/DocumetsMailings/Brochure-betalingsfraude-FR-DEF.pdf

Apart from the fact that binary options are highly speculative and entail great risks[23], some providers of binary options do not have the required license to operate as an investment company or credit institution, and they may not provide banking and/or investment services in or from Belgium. Nor do they publish a prospectus approved by the Financial Services and Markets Authority (FSMA), as required for each public offering of investment vehicles in Belgium.

Despite their sound appearance, several platforms that trade in binary options are operated by unlicensed companies led by fraudsters that operate without a license, forge the results of the platforms or embezzle the invested funds. In such cases investors never get their money back given that these illegal service providers are generally located abroad. In the files reported to the judicial authorities in this regard CTIF-CFI found that the Belgian accounts of a Limited company received funds from victims and that the money was always transferred to another (second) Limited company abroad. The funds were subsequently transferred to a third Limited company in another country. The third Limited company was an electronic money company that processes Internet transactions, and after deducting their fees, transfers these funds to the merchants.

The use of several Limited companies and bank accounts in Belgium and abroad for the transactions is intended to hamper further investigation into the final destination of the embezzled funds. In the files reported to the judicial authorities, the individuals featured in fraud investigations using fictitious Forex trade platforms. The victims were approached online and by phone to speculate on the foreign exchange market (FOREX). Call centres are used to attract potential victims, promising a return between 20 and 30% or more. In reality these were fictitious exchange platforms. The *Enforcement* unit of the FSMA received several complaints from victims that had transferred money to fraudsters, each time with the same payment reference. As a result, there was a strong suspicion that the fraudsters used the payment system of the latter Limited company (electronic money company).

[23] See the FSMA's warning on this topic (https://www.fsma.be/en/news/fsma-issues-warning-about-binary-options)

1.1.5. Corruption

A widespread problem

Corruption is a global issue and affects industries as well as public services. No single country is spared from corruption and the costs are enormous. An estimate by the IMF puts the annual cost of bribery between 1.500 and 2.000 billion dollars, roughly 2% of the global GDP[24].

The amounts in the files related to corruption that CTIF-CFI reported to judicial authorities reveal the scope of the problem, with amounts ranging between some thousand EUR and some hundred million EUR.

Analysis of the files related to corruption that CTIF-CFI reported to judicial authorities shows it mainly concerns corruption of government officials, as well as private corruption to a lesser extent. The individuals concerned are generally politically exposed persons (PEPs), mainly foreign nationals and/or individuals residing abroad; or government officials or individuals working in the private sector, primarily Belgians and/or Belgian residents.

The money laundering transactions are usually carried out through the banking system. It is not uncommon that bank accounts are opened solely to conduct money laundering transactions. In the files reported to the judicial authorities CTIF-CFI found that there were significant financial flows related to assets left to heirs by people known for corruption. Assets held with several banks in a neighbouring country were brought back to Belgium. The assets were transferred to accounts held by the heirs that had been opened specifically for this operation with banks in Belgium. The assets, securities worth several million EUR, were sold and the proceeds of the sale were transferred to other accounts with several other banks in Belgium.

The most common transactions are mainly cash deposits, followed by transfers abroad, or transfers from abroad followed by cash withdrawals. Although in most files money laundering transactions are carried out by corrupt persons, some files reveal that money laundering transactions are carried out by third parties, especially when politically exposed persons are involved. The third parties include family members, partners or non-financial professionals. In some cases more complex money laundering techniques are used, such as private banking abroad, transit accounts, front companies and offshore centres. Belgian nationals as well as foreign nationals invest in assets, property or insurance.

[24] IMF, *Corruption: Costs and Mitigating Strategies*, 2016.

1.2. Terror threat and terrorist financing

1.2.1. Terrorist attacks in Brussels

On the morning of 22 March 2016, the largest terrorist attack in the country's history was committed. More than thirty people lost their lives and hundreds were injured in two separate attacks, one at Brussels Airport and one at the metro station Maelbeek in Brussels. These attacks were prepared and carried out by individuals linked to the terrorist group Islamic State (IS). There was also a clear link with the attacks in Paris in November 2015 and the terrorist cell of Verviers dismantled in January 2015.

The attacks in Brussels obviously had a great impact on CTIF-CFI's work in connection with terrorist financing in 2016. From 2014 onwards it became clear that the Belgian authorities fighting terrorism had to face a new reality because of the increasing power of IS and the growing number of Foreign Terrorist Fighters, who left Belgium for war zones. In 2016, this reality became critical and the issue evolved from fighters joining IS to returnees and lone wolves committing attacks in their home country.

CTIF-CFI is competent for dealing with terrorist financing on a domestic level. CTIF-CFI analyses disclosures of suspicious transactions it receives from several categories of disclosing entities, as well as information from the Federal Public Prosecutor's Office, the police or the intelligence services. In addition, it conducts strategic analyses to identify typologies and assess terrorist financing risks. Moreover, CTIF-CFI is a member of an international network of FIUs and takes part in activities and projects of global organisations such as the FATF or the Egmont Group.

1.2.2. Evolution in figures and trends

Overview of the files related to terrorism reported to the judicial authorities

In 2016, 112 files were reported to the judicial authorities because of serious indications of terrorist financing or laundering the proceeds of terrorism. This is a sharp rise compared to the 75 files in 2015 and more than three times the number of files in 2014. The total amount of the files reported to the judicial authorities remains stable and is, in absolute figures, a relatively limited amount of EUR 6,66 million in 2016.

Contrary to the number of files, the total amount of files reported to the judicial authorities related to terrorist financing is fairly limited compared to the total amount of all files reported to the judicial authorities. These absolute figures are a good indicator of the importance CTIF-CFI attached to terrorist financing in recent years. In the context of terrorist financing the absolute amounts are not very relevant. Often a transaction in itself can be sufficient to locate people or link them to each other, regardless of the amount of the transaction.

CTIF-CFI reacted to the increasing number of disclosures by setting up an internal "terrorism" unit at the start of 2015 combining specific operational and strategic knowledge related to terrorist financing, allowing to quickly analyse all information related to the issue.

Recent evolution of the identified typologies

- From FTFs to returnees and lone wolves

In 2015, CTIF-CFI reported several files to the judicial authorities regarding individuals leaving for war zones who emptied their account or took out loans. These files that CTIF-CFI reported to the judicial authorities also showed that Belgian fighters often financed their departure with their salary, social benefits or cash deposits were potential proceeds of petty crime, given their police records.

This form of direct financing of IS by foreign fighters was no longer identified in files reported to the judicial authorities in 2016. Information from the Coordination Unit for Threat Analysis (OCAM-OCAD) confirms that the phenomenon of those leaving Belgium in 2016 virtually disappeared.

Instead, in 2016 the fears of an attack in Belgium unfortunately became reality in March. The issue of so-called returnees remained very topical after these events. An international arrest warrant was issued for those whom it was certain that they had been in Syria, yet the risk is real that those who have returned or wish to return are at the very least radicalized and could be used to commit attacks.

Apart from the returnees, who have at least in the area of conflict for a short period of time, recent attacks have also been committed by individuals who had never travelled to Syria or Iraq and can be considered to be 'Homegrown Terrorist Fighters' - 'HTFs' or 'lone actors'. These individuals were radicalized in a short period of time and are only inspired by IS, but do not get any direct operational or financial support. As IS's situation in Iraq and Syria becomes more precarious, it is to be expected that the organisation will further advocate this type of attacks. Social media is used, asking supporters to no longer travel to Syria but to continue the battle in their country of residence. IS recommends using easy and easily accessible weapons and low-level "soft" targets to result in as many casualties as possible.

The threat of attacks by returnees or HTFs results in new challenges for the departments competent for combating terrorism. This is particularly the case for CTIF-CFI, as financial transactions associated with these new forms of terrorism are very limited and particularly difficult to detect. Money laundering is analysed based on a suspicious transaction, whereas the starting point of terrorist financing investigation is often an entity that can potentially be linked to terrorism, whose financial transactions are then investigated. CTIF-CFI has access to OCAM-OCAD's dynamic database, in order to be informed of known FTFs and radicalised individuals.

A financial investigation can also confirm whether or not a person in a war zone receives money from family and acquaintances and is therefore still alive. This information is valuable as, in the past, various FTFs staged their death to be able to travel and operate more freely. In 2016, CTIF-CFI reported several files to the Public Prosecutor's Office related to indirect money remittance to fighters in a war zone.

- The attacks in Brussels and Paris

Following the attacks in Brussels, CTIF-CFI analysed the financial aspects of the attacks and more widely looked into the financing of the structure responsible for setting up the terrorist cell that was dismantled in Verviers in January 2015, the attacks in Paris in November 2015 and the attacks on the metro at Maelbeek and at Brussels Airport on 22 March 2016.

Although the organisation behind Verviers and the attacks in Paris and Brussels was part of one single structure, this does not mean the operational cells operate under a strict hierarchy or had a clear structure. Analysis shows these cells operate fairly autonomously, loosely grouped, with approval and limited instructions from IS leaders in Syria and Iraq. As long as IS had great military power in the war zone and could train and use FTFs the organisation's interest in Western Europe as a target was rather limited.

The change in strategy by IS on actions outside the "caliphate" is also visible in the financing of the attacks. The organisation sometimes supports the cells financially to a certain extent, but not every need.

Several successes of the investigation into the attacks in Paris and Brussels can be attributed to the fact that the individuals collect or transfer funds in a fairly improvised manner and independently.

Due to the immense impact and the serious consequences of the attacks one would be inclined to think that the perpetrators, and by extension IS, use a great degree of professionalism when organising these attacks.

Yet the organisation seems to have improvised in many respects. Several perpetrators hesitated or changed their minds, only part of the explosives were brought to the place of destination and the perpetrators on the run seemingly contacted random acquaintances for help.

Analysis into the financing and the financial elements of the attacks reveals a similar pattern. Part of the funds for the attacks clearly came from IS in Syria, although the different cells also seem to have collected and transferred funds independently in a variety of ways. The individuals used various financing sources and techniques, seemingly without any clear strategy and sometimes without worrying about possible detection. The fact that an organisation with little structure as to its financing can carry out attacks with such devastating consequences is not only very worrying but also leads to certain conclusions on how to combat terrorist financing.

The various sources and mechanisms of financing are discussed below that were identified with regard to the terrorist cell of Verviers and the attacks in Paris and Brussels, or that IS potentially used in Syria and Iraq.

1.2.3. Identified sources and mechanisms of financing

Sources of financing

- ***Macrofinancing***

With regard to financing, the terrorist group IS represents a completely new phenomenon. Where "conventional" terrorist organisations previously used to have great difficulty raising the necessary funds to ensure their long-term operations, IS had access to significant funds access to significant resources from the outset. The physical and administrative control over an area covering large parts of Syria and Iraq gave IS an unprecedented source of income from illegal activities. During a large-scale offensive in 2014 IS was also able to gain control over a far greater area in Syria and Iraq.

The most important forms of illegal macro financing in the area under IS control are bank robberies, extortion, human trafficking, smuggling of oil and kidnapping.

As part of its operational activities CTIF-CFI only dealt with these forms of microfinancing indirectly and to a limited extent, as they are very much geographically linked to the area of conflict and Iraq and Syria's neighbouring countries. At a strategic level two possible forms of macrofinancing were studied, given their potential repercussions for Belgium. These are illegal trade in cultural antiquities and trade in Captagon.

By gaining control over archaeological sites in Syria and Iraq IS potentially generated income from trade in antiquities. Reports from UNESCO show that the trade in ancient cultural artefacts from sites in Iraq and Syria became increasingly important from 2015 onwards. The issue of illegal trade in antiquities is very relevant to Belgium. Brussels, an important centre for the antiques trade, could also be used as a hub for this trade in cultural objects, the proceeds of which could return to IS. Apart from physically countering the smuggling of cultural artefacts, the detection of the underlying financial flows is also an important aspect of tackling this illegal trade.

The importance of the trade in antiquities in the entire financing capacities of IS should nevertheless probably be put into perspective. According to local archaeologists IS showed little interest in the trade. Because of losing further ground in 2016, IS lost control over important sites such as Palmyra, so this specific form of macrofinancing is no longer very relevant.

The increasing number of bombings by the coalition against IS and a series of military defeats decreased IS's financial capacity from 2015 onwards. IS typically relied heavily on occasional sources of financing, not on sources that would generate a steady long-term income.

There are indications that from mid-2015 onwards IS focussed on drug trafficking, Captagon in particular, to counter the decrease in revenue.

Captagon is the brand name for an amphetamine derivative; it is a very popular "party drug" in the Middle East that is also used by fighters in Syria and Iraq as a stimulant. For years hashish and Captagon were produced in the Bekaa Valley in eastern Lebanon. Since the start of the war in Syria producers of Captagon have taken advantage of the chaotic situation to move production to Syria to further reduce the risk of being detected.

The war is Syria is also said to be one of main causes of the fast-growing worldwide trade in illegal amphetamines. The number of seizures of these products has quadrupled in the last five years. Given that Captagon is very popular among IS fighters and other fighting parties, as well as traumatized and fleeing civilians, it is not unlikely that IS would have taken over part of this trade. With a potential income worth hundreds of millions of dollars a year the trade in Captagon would be a substantial and steady source of income.

Not all of IS's sources of financing are illegal though. Thanks to an ingenious marketing and communication strategy using modern technological tools the organisation is able to receive substantial donations from individuals and organisations in the Persian Gulf Region. Foreign fighters also paid an "entry fee" before joining IS. These funds were often obtained by emptying their bank accounts or by taking out short-term loans just before leaving.

Financial intelligence units such as CTIF-CFI in Belgium are generally fairly powerless against IS's macrofinancing as military action on the ground is much more effective to reduce the area controlled by ISIL and to deplete its sources of financing.

Now that these sources have decreased and fewer foreign terrorist fighters travel to the war zone, the financial focus has shifted. IS will increasingly tend to move funds collected through macrofinancing to cells in Europe to carry out attacks.

Moreover, individuals or cells in Europe will increasingly finance themselves or ensure their own logistical needs.

- ***Micro financing***

- **Licit origin**

Analysis of the financial profile of the individuals involved in the attacks in Paris and Brussels in the months prior to the attacks revealed that a large part of the incoming funds on these accounts were salaries, unemployment benefits or other social benefits.

- **Illicit origin**

Many of them have numerous police convictions and are known to the authorities for (petty) drug trafficking and drug use, theft, handling stolen goods and other crimes.

The occasional cash deposits on these accounts are presumably funds generated by these illicit activities. It is also likely that most of the cash is also spent in cash, by renting expensive cars, or buying drugs and luxury goods for example.

When preparing a terrorist attack it is probable that this cash is also used for logistical arrangements. The individuals tend to generate additional cash by committing criminal offences, available information shows that IS sometimes provides financial support but that most of the financing is done by cells independently.

In addition to petty crime as a source of financing for terrorism it also became apparent in 2015 and 2016 that the boundaries between serious organised crime and terrorism became increasingly blurred.

This fusion of the world of crime and terrorism enables potential perpetrators of terrorist attacks to build networks that give them access to heavy weapons and forged documents as well as potential additional sources of financing.

Mechanisms of financing

- ***Cash***

The main finding of a financial investigation and one of the main reasons why it is so difficult get an insight into the financing of terrorist attacks and organisations is the widespread and universal use of cash. When investigating the attacks the account history of the individuals involved in the attacks does not provide an explanation for the money spent on buying weapons and explosives, renting cars and safe houses and other expenses related to setting up a terrorist cell. Police investigation and questioning of the suspects revealed that virtually all purchases were paid in cash.

In case the use of cash would be too suspicious prepaid cards or an account were used, after the money had been deposited in cash.

Petty crime, one of the potential sources of financing for the attacks, yielded cash.

- ***New communication and payment systems***

Despite IS's Salafist view of society IS has always used the latest communication and information tools to spread its message.

Those involved in the attacks in 2015 and 2016 also frequently used recent apps and payment systems. Financial information shows frequent online purchases paid with PayPal or other online payment systems.

These transactions cannot be directly linked to the preparation of the attacks but do indicate that these "new" ICT applications are used with ease.

- ***Prepaid debit cards***

Investigation into the attacks in Paris and Brussels revealed that several individuals used prepaid debit cards. These cards can be used like credit cards but the amount should be transferred to the account linked to the card in advance.

The reason for terrorists to use this type of card is not anonymity, although some prepaid debit cards can be used anonymously (loading cash does not require identification), but the amounts that can be loaded onto the cards are quite low. The card used when preparing the attacks in Paris was of a different type and was linked to an account whose account holder had been identified. This was not an anonymous card, the card was not personalised, i.e. the name of the card holder was not printed on the card itself. This type of card was used as it did not require a brief credit check of the customer, which often is required for a conventional credit card. For some transactions, such as renting cars, card payments stand out less than large cash payments.

- Virtual currencies

There is a real risk that virtual payment systems such as Bitcoin can be misused for money laundering and terrorist financing purposes. This risk is mainly linked to the second money laundering stage, layering. Although the blockchain in the Bitcoin system is essentially public, in practice it can be very difficult to trace the funds due to the use of specific software.

Moreover, virtual currencies are frequently used for payments on illegal trade platforms hidden in the "darknet", the part of the Internet that is not publicly accessible.

Virtual currencies also entail a risk in respect of terrorist financing. In 2014, IS called upon its sponsors to transfer funds using Bitcoin, as this makes the funds more difficult to trace.

2. Vulnerabilities of specific sectors

In relation to combating money laundering the FATF defines vulnerabilities as the whole of structural and institutional factors making the commission of a crime and/or carrying out a money laundering transaction more attractive[25].

Vulnerabilities are related to the legal system, practical measures and instruments used in a specific sector. The probability of a risk appearing is also important.

Based on various criteria (organisation, supervision, structure, traded product/service), several sectors particularly sensitive with regard to money laundering were identified as part of the national money laundering risk assessment[26] (threats and vulnerabilities).

2.1. Building industry

Several factors make the building industry a vulnerable sector with regard to money laundering. One of the main elements is the use of subcontractors. The subcontractors may conceal various other companies and the managers with legal responsibility are front men. Moreover, often new managers are appointed, thus complicating investigation and prosecution, especially when these managers are front men, are insolvent or disappear when these fraudulent transactions come to light.

A large number of shell or dormant companies are also used in this sector. Fake document are also produced, especially with regard to social fraud. By using vague and broad company objects it becomes easier to set up arrangements with numerous companies (group structures that fit together like Russian dolls) and conduct illegal activities.

In brief, the sector conducts unofficial activities that generate large amounts of cash.

CTIF-CFI's experience confirms these vulnerabilities. The number of files reported to the judicial authorities shows that fraudulent subcontractors are often used, complicating the analysis of financial flows: companies outsource the work to various companies, who in turn use subcontractors. Fake invoices are drawn up to account for the financial flow, necessary for the unofficial payment. This multi-tiered system is able to continue given that companies are declared bankrupt after the first inspection and immediately replaced by another company set up with that specific aim. Several files also reveal that unofficial workers are used, as part of so-called "Brazilian networks". The secondment procedure is improperly used. Foreign workers are employed as bogus self-employed workers because this is cheaper.

---

[25] *FATF Guidance for Countries on assessing money laundering and terrorist financing risk* – October 2012 (www.fatf-gafi.org)

[26] The national risk assessment money laundering was conducted by the Board of Partners (*Assemblée des partenaires*) of the Board for Coordinating the fight against laundering money of illicit origin (*Collège de coordination de la lutte contre le blanchiment de capitaux d'origine illicite*). The vulnerability assessment was conducted with contributions provided by CTIF-CFI, the Federal Public Service Economy, the National Bank of Belgium, the Financial Services and Markets Authority, the Federal Public Service Finance and the Customs and Excise Administration.

The files reported to the judicial authorities also indicate that building companies used for fraudulent and money laundering purposes are predominantly shell companies with a short life span, which sometimes remain dormant and are potentially vulnerable. CTIF-CFI also found that building companies are increasingly involved in money laundering transactions by using the compensation technique.

It should also be noted that CTIF-CFI identified similar practices in files reported to the judicial authorities involving the industrial cleaning industry and road transport.

2.2. Art and antiques trade

The art and antiques trade is diverse and includes auctions as well as purchases at art galleries, museums, antique dealers and collectors, and of course the growing online trade.

Several features make the arts and antiques trade vulnerable with regard to investments of money of criminal origin. Supervision of the sector is difficult, dealings are discrete and the market is opaque. Gallery owners, antique dealers and auctions are easy to inspect, the distribution channels on the other hand are more difficult to supervise in case of direct sales transactions between private individuals, especially online, which is an increasingly popular distribution channel.

High-value products in an opaque sector will make the industry more vulnerable in connection with money laundering. In the arts and antique trade the value of the product is often unclear or cannot be objectively determined. Large amounts of money are sometimes involved, so these goods could be used for money laundering purposes.

There are other elements making this sector vulnerable: these are high-value goods that can easily be transported and fake documents can be produced. In this sector goods can change owners easily and quickly and anonymous operations are possible, especially on the Internet. The sector's vulnerability in terms of anonymous use is further increased by the expansion of new financial technology, in particular anonymous means of payment such as virtual currencies (*see part 3 of this report*).

In the files that CTIF-CFI reported to the judicial authorities CTIF-CFI found that the art and antiques trade can be involved in a variety of ways. As a channel to carry out criminal activities, for instance. Several files are linked to the illicit trade in antiques, and cash transactions are used (cash deposits, followed by cash withdrawals) and international transfers (linked to China in particular). In other files the sector is involved in theft, counterfeiting, forgery or fraud with art or antiques.

This sector is also used as a channel to launder criminal proceeds. The files reported to the judicial authorities show that investments in the art world are used to launder proceeds of corruption, drug trafficking and trafficking in illegal workers. The techniques used include fake invoices (when the merchant draws up a fake invoice for a customer), fake auctions (the money launderer sells artwork by auction, an accomplice buys with dirty money) or fake online auctions.

2.3. Precious stones and precious metals

Dealers in precious stones and precious metals are vulnerable with regard to money laundering. Due to the large number of parties in these sectors and the possibility that fake documents or fake invoices could be used supervision is not straightforward. Furthermore, the activities are closely linked to import and export and there are links with countries where AML/CFT measures are not as strict.

With regard to vulnerability, sectors trading or handling goods that can easily be changed or altered are to be considered vulnerable. The same goes for the gold trade as gold can easily be taken out of jewellery and made into bars. Unprocessed gold can be changed into cash or sold on.

Goods that are easy to transport also make it easier to carry out money laundering transactions. Jewellery and precious stones can therefore facilitate money laundering transactions, making the sector in which these goods are traded more vulnerable with reference to money laundering.

The diamond trade is vulnerable because of the commercial practices in this sector. The international nature of the diamond trade (the majority of the counterparties, clients or suppliers are located abroad) may make it difficult to identify clients and suppliers. In recent years, a number of foreign locations, apart from Antwerp, such as Dubai, South Africa, Israel and India, have become increasingly important, resulting in an increase of the diamond trade but also the financial flows. Finally, the use of cash is also common in this sector.

The vulnerabilities of the sector dealing in precious stones and precious metals may increase even further because of the development of products as a result of technological innovations, such as changing virtual currencies in precious metals (gold, silver) or the use of payment cards linked to the supply of diamonds, gold and silver (see part 3 of this report).

2.4. Hotel and catering industry

The hotel and catering industry is vulnerable to money laundering at different levels. Large amounts of cash are used and by maintaining control over the accounts of a business the regular influx of cash can be explained. Money of illicit origin can easily be combined with licit income for a business or used to pay non-declared workers. A sudden upsurge in turnover is another common technique, facilitated by the increased turnover.

Front men, allowing fraudsters to remain anonymous, and fake documents (fake invoices, fake VAT receipts, fake letters of resignation) are also used.

A sector such as the hotel and catering industry, in which companies have a short life span, are more vulnerable with regard to fraud and money laundering. Companies in this industry are “ephemeral” and schemes are set up to draw up invoices for fake services, to allow outgoing cash to be recorded in the accounts. The fraud and money laundering schemes often reveal the following signs: the company is declared bankrupt, dissolved, given up or one corporate structure is replaced by another in a short space of time (often when tax or VAT inspections are carried out) or new managers are appointed.

Given the size of the market, the large number of players has an impact on the supervisory authorities' capacity to correctly supervise the sector.

CTIF-CFI's experience confirms this sector's vulnerabilities, the sector is used to conceal illegal activities such as drug trafficking, exploitation of prostitution or human trafficking.

2.5. Retail trade

This group mainly includes night shops, tobacconists and shops selling phone cards. The only preventive provisions with regard to these traders is the general ban on any cash payment for goods or services worth over EUR 3000.

This sector is also vulnerable to money laundering in various ways. Like the hotel and catering industry, retail trade offers the advantage of a large cash flow. Money that needs to be laundered can easily be combined with the business's takings before being injected into the financial system as supposed business income (see the box on migrant smuggling).

Furthermore, several businesses use bogus self-employed people or front men as their managers. Other common features include: vague and broad company objects, non-transparent accounting, undeclared workers and an unusually high turnover compared to the economic reality. Because of the availability of cash informal money transfer systems (underground banking such as hawala).

Checks in several shops showed that companies in this sector have a fairly short life span (12 to 18 months), making the sector even more vulnerable. Often a company is declared bankrupt after a first VAT inspections by FPS Finance or FPS Work, and a new company is automatically set up with new people or the company shares are transferred to other people. It is therefore difficult to identify the people who are actually responsible.

Given the difference in price of tobacco in Belgium and some neighbouring countries retail traders in tobacco carry out many cross-border movements of cash and tobacco, especially some retailers in border regions (France and the United Kingdom). Private individuals also buy tobacco in Belgium to avoid paying excise duties and VAT in their country of origin. Tobacco is easily transportable and it is quite easy to draw up fake documents given that illegally purchased tobacco can be transported with transport documents for legally purchased products.

2.6. Second-hand cars

Cash remains an important means to launder money, so sectors that accept cash are more vulnerable in terms of money laundering. The second-hand car trade generates significant financial flows. The EUR 3000 threshold actually makes it possible to sell many cars using cash (about half of all available second-hand cars cost less than EUR 3000). Furthermore, there are no restrictions on the use of cash when selling to private individuals. As a result, large amounts of cash can be used when selling second-hand cars. When reselling vehicles dirty money can be added to the profit margin.

Fake documents can also be used in this sector: by paying the difference unofficially it is possible to register a lower amount for a sales transactions between the second-hand car dealer and the buyer. Conversely, a higher amount can be recorded for a purchase between the

company and the seller. The accounts can also be forged, given that prices vary for transactions between private individuals.

Import and export activities can be used to conceal Trade-Based Money Laundering (TBML) activities. Some large export channels use various intermediaries in Belgium and abroad. In case of some export channels, particularly to West Africa, these intermediaries are part of the same group of companies, thus increasing their vulnerability. The fact that customers do no live in Belgium is also a vulnerability factor.

Although the vast majority of companies has a good reputation and is listed in the Crossroads Bank for Enterprises, supervision of the export channels is rather difficult.

CTIF-CFI's experience confirms the sector's vulnerabilities, especially at international level. Several drug trafficking networks were dismantled in the past years. Open sources reveal that the proceeds of cocaine trafficking in Europe is no longer sent to Africa using money remittance, but used to buy second-hand cars that are subsequently shipped to West Africa.

3. Emerging risks related to financial innovations (FinTech)

As in other sectors, profound changes are taking place in financial services linked to the technological revolution. FinTech companies are either new or existing players, who use and/or provide innovative processes, products or services.

The risk that they are used to launder money or finance terrorism can be high or very high, especially when misusing a combination of FinTech instruments (such as the use of virtual currencies combined with the use of an electronic wallet, the use of an e-money institution linked to crowdfunding…). In these cases the number of layers increasing the level of anonymity, transactions become more difficult to trace and future investigations into the ordering party, recipient and the origin and the destination of the funds.

3.1. Virtual currencies risks

Virtual currencies are a digital representation of value, not issued by a central bank or a government authority but are accepted by natural or legal persons as a means of payment and can be transferred, stored or exchanged electronically[27].

These completely virtual units of account, which are digitally stored, enable a community of users to mutually exchange goods and services without using legal tender and without having to use the conventional financial system. These virtual currencies are opaque and not regulated[28].

Currently more than 700 virtual currencies use the distributed ledger technology (blockchain), facilitating currency exchange between people, with bitcoin being the most well-known example. Bitcoin currently has a market share of over 90% in the virtual currency market. Nevertheless, new types of virtual currencies do emerge, such as Ether or Monero.

[27] European Banking Authority, Virtual currency schemes - a further analysis, February 2015, (only available in English).

[28] Blundell-Wignall, A. (2014), "The Bitcoin Question: Currency versus Trust-less Transfer Technology", OECD Working Papers on Finance, Insurance and Private Pensions, No. 37, OECD Publishing; Sofie ROYER, *BITCOINS in het Belgische strafrecht en strafprocesrecht* [BITCOINS in Belgian criminal law and criminal procedure law], *Rechtskundig Weekblad* nr. 13, 26 November 2016, pages 483 -501.

Blockchain[29]

Blockchain is a technology for storing and transferring information, transparent and without any central supervisory authority. By extension, a blockchain is a database containing the history of all exchanges between its users since it was set up. This database is secure and distributed, it is shared among users, without any intermediaries, so everyone can check the validity of the chain. This technology is comparable to a ledger in which every new transaction (date, sender's account, recipient's account, amount of the transaction) is recorded and it is not possible to delete any of the transactions.

Although blockchain and bitcoin were developed together there are currently many players (companies, governments, etc.) wishing to use the blockchain technology for other purposes than for electronic money. The areas in which it can be used are vast: banks[30], insurance[31], real estate[32], health[33], energy[34], transport[35], online voting[36]. In general blockchain could replace most of the centralized "trusted third party" by distributed computer systems. For banks this would mean streamlining some back-office tasks. As the "trusted third party" system that checks the transactions becomes superseded blockchain could significantly reduce transaction costs and processing time.

Blockchain could bring about a great technological revolution, yet the general use will need time as the processing possibilities are currently still limited and the legal and policy issues have not yet been solved.

Following the rise of virtual currencies new companies were set up: exchange platforms, price comparison companies, wallet providers. Cash machines were developed where bitcoins could be changed. Using a bitcoin wallet, euro notes can be withdrawn from these machines. Conversely, by inserting euro notes into the machine your bitcoins will be put onto your wallet.

Because of their features and the way they work virtual currencies carry intrinsic risks. They enable the financing of criminal activities and facilitate laundering the proceeds of these activities. Criminals and terrorists use these technological developments and increasingly use new electronic instruments to launder proceeds of illegal activities or to finance their terrorist activities[37].

[29] ECB, Virtual currency schemes – a further analysis, February 2015; European Securities and Markets Authority (ESMA), Call for evidence: Investment using virtual currency or distributed ledger technology, April 2015.

[30] https://blockchainfrance.net/2016/08/17/quels-impacts-de-la-blockchain-sur-les-banques/

[31] https://blockchainfrance.net/2016/02/17/assurances-et-blockchain/

[32] https://blockchainfrance.net/2016/03/03/des-cadastres-sur-la-blockchain/

[33] https://blockchainfrance.net/2016/03/02/la-blockchain-et-la-sante/

[34] https://blockchainfrance.net/2016/07/07/la-blockchain-pour-lenergie/

[35] https://blockchainfrance.net/2016/03/19/arcade-city-le-uber-killer-de-la-blockchain/

[36] https://blockchainfrance.net/2016/02/12/democratie-et-blockchain-le-cas-du-vote/

[37] EUROPOL SOCTA 2017, Crime in the age of technology; Financial Action Task Force (FATF), Virtual Currencies, June 2014 (only available in English); European Parliament, Report on virtual currencies (2016/2007(INI)), Committee on Economic and Monetary Affairs, A8-0168/2016.

At the moment there is no regulation in Belgium to licence exchange platforms for virtual currencies and there is no supervisory authority for these platforms. The National Bank and the Financial Services and Markets Authority warned that virtual currencies are not legal tender and are not a form of digital money. There is no financial supervision on virtual money[38]. There are no exchange platforms in Belgium, although foreign ones (including in the European Union) are accessible from Belgium.

To counter anonymity and increase the transparency of financial flows the European Commission developed an action plan to strengthen the fight against terrorist financing. A proposal[39] for a Directive amending the fourth Directive was published on 5 July 2016 in order to bring virtual currency exchange platforms and custodial wallet providers under the scope of the Directive[40]. Licensing virtual currency exchange platforms in Belgium (with the appropriate legislation) would improve supervision of the use of virtual currencies and sanctioning of their use for criminal and terrorist purposes.

Money laundering risks

CTIF-CFI's experience shows that the use of virtual currencies hampers further investigation. Their anonymity makes virtual currencies attractive for criminal purposes. Although transactions can be traced in the blockchain, the ordering party and the beneficial owner cannot be identified based on the financial flows. CTIF-CFI reported files to the judicial authorities featuring individuals who used fake names to open accounts with banks in Belgium. Shortly after they were opened, these accounts received transfers from accounts held by people whose accounts were misused as a result of computer fraud. A large part of the funds was transferred to several virtual currency exchange platforms to purchase bitcoins. This enabled the proceeds of crime to be laundered and it hampered further investigation into the beneficial owners.

Some applications allow transactions to be combined, without being able to determine whom sent what to whom. The issues surrounding virtual currencies also relate to their extraterritorial nature. Completely dematerialized international flows are common, in particular when servers or exchange platforms are located in countries that show little cooperation.

One of the risks of the use of virtual currencies for money laundering purposes relates to the second money laundering stage, layering. Virtual currencies enable users to anonymously transfer value, making it very difficult to trace transactions, especially when programmes such as TOR are used to conceal IP addresses.

[38] See the warnings of the National Bank of Belgium and the Financial Services and Markets Authority for the risks in connection with virtual currencies (statement of 14 January 2014 and 16 April 2015).

[39] http://ec.europa.eu/justice/criminal/document/files/aml-directive_en.pdf

[40] Communication from the Commission to the European Parliament and the Council on an Action Plan for strengthening the fight against terrorist financing, COM(2016) 50 final.

Another way of laundering virtual money is to change it into cash. This is possible through online exchange platforms or physical trade counters. Professional launderers on the darknet also change virtual currencies into cash. Certain trade platforms or physical traders in precious metals also provide the service of changing virtual currencies into precious metals (gold, silver).

Terrorist financing risks

With regard to terrorist financing, and as was identified with prepaid card virtual currencies, virtual currencies can be used to maintain networks: fake documents, airline tickets or material (weapons) are purchased aimed at committing attacks. Moreover, e-wallets linked to accounts of individuals who are not monitored by the authorities can be used to collect and transfer amounts to various groups around the world without raising suspicions with the authorities.

One of the possible terrorist financing techniques is to use accomplices who receive small amounts in bitcoin, change these and then deliver these to a contact in the country in question.

3.2. E-money risks

This past year CTIF-CFI noticed a change in way in which individuals in CTIF-CFI's files paid online. They less frequently use conventional methods of payment and increasingly turn to electronic money institutions. In several files accounts received numerous transfers with accounts in various European countries. These accounts were then used to transfer money to an electronic money institution to purchase bitcoins. The number of transfers and amounts involved were not consistent with the account holder's profile. CTIF-CFI's analysis revealed that the individuals involved were known for drug trafficking. At least part of the transactions from these various European countries, followed by the purchase of bitcoin, could be part of a money laundering operation related to drug trafficking.

CTIF-CFI found that the transactions carried out on these platforms are not subject to supervision by financial institutions. Financial institutions are not able to determine the details of the transactions carried out on these platforms. Companies issuing credit cards face the same issue. Only the amounts and the time (date and sometimes the time) of the transactions are known.

Let us consider the following example: a company for electronic payments established in country A, with an account in country B and a website hosted in country C: identifying the financial flows related to payments conducted via this company is complex and requires international cooperation with the countries involved. Of course CTIF-CFI can request information from foreign counterparts but the detection of suspicious financial transactions and the identification of the ordering party and the beneficial owner remains a particularly delicate issue.

As regards investigation it is possible to detect part of the financial flows on the account on the basis of the IP address used to send the funds and obtain the necessary information for the analysis. It can be complex for a financial intelligence unit to obtain an IP address (especially when programmes to hide IP addresses are used) and this may be an issue with regard to data protection.

Technological developments requires developing a new approach of combating money laundering and terrorist financing. Credit institutions could be required, for instance, to include the IP address as part of the customer due diligence procedures.

Electronic money institutions are not only used to send money to beneficiaries but also to receive money in cash through a network of money remittance operators. It is therefore essential to be able to detect incoming and outgoing financial flows on accounts with these institutions.

The interpretative note to FATF Recommendation 16 (wire transfers) states: "countries may adopt a *de minimis* threshold for cross-border wire transfers (no higher than USD/EUR 1 000), below which the following requirements should apply: (a) Countries should ensure that financial institutions include with such transfers: (i) the name of the originator; (ii) the name of the beneficiary; and (iii) an account number for each, or a unique transaction reference number. Such information need not be verified for accuracy, unless there is a suspicion of money laundering or terrorist financing, in which case, the financial institution should verify the information pertaining to its customer."

The EUR 1000 threshold does not imply a higher risk in terms of money laundering. There is a significant risk with regard to terrorist financing though, as the amounts are usually much smaller in these cases. In this respect there would be no identification for cross-border wire transfers of less than EUR 1000.

3.3. Crowdfunding risks

The general term crowdfunding refers to a method for raising funds from private individuals to finance a project. This can take place in various ways but always involves three parties: the person managing the project, i.e. the person(s) looking for funds to finance their project, the persons financing the project and the social platform joining the parties.

There are three type of crowdfunding. A popular type of crowdfunding, i.e. crowddonating, enables donations to be used to finance non-profit projects. Crowdlending involves a loan instead of donations, usually with interest calculated on the basis of the project's risk. Crowdinvesting is a type of crowdfunding in which company shares can be purchased.

A new law on licencing and defining crowdfunding was adopted in Belgium in December 2016[41]. The law only relates to platforms on which the public can invest in a company in order to get a potential profit (crowdlending and crowdinvesting). These platforms must now be licensed by the FSMA and have to comply with certain rules of conduct.

[41] Belgian Official Gazette, 20 December 2016, Ed. 3, page 87668.

The law also introduces a new exemption for publishing a prospectus for licensed crowdfunding platforms. This new exemption implies that for public tendering there is no need to publish a prospectus, as long as the total amount of the tender does not exceed EUR 300 000 and the total amount of the individual tender per investor does not exceed EUR 5 000.

As crowdfunding platforms that do not offer financial investments are not subject to these provisions and are not supervised by the FSMA there is a significant risk that the platforms are misused for illegal purposes. In several files reported to the judicial authorities CTIF-CFI found that crowdfunding websites were used to create a fundraising website and to raise funds. The aim of the fundraising campaign, presented as a charity or humanitarian cause, could easily be misused for illegal purposes, including terrorist financing. Donors are not always aware of the final destination of funds raised through crowdfunding.

Not only can crowdfunding be used to raise money for terrorist financing purposes, but also to send money abroad without having to use the regulated financial system.

RegTech[42]

Within FinTech, technological innovations are developed to externally manage compliance and risk management: RegTech (regulation and technology). The different solutions put forward are all based on innovative technology (artificial intelligence, big data). The main services include managing large amounts of data (aggregation, analysis and predictions), real-time monitoring of transactions, tools to enhance customer knowledge.

RegTech offers possibilities for combatting money laundering and terrorist financing, i.e. the fundamentals of AML/CFT: know you customer, identification of the origin and the destination of funds and detection of suspicious transactions. CTIF-CFI closely monitors development in the field of RegTech as well as FinTech.

[42] Stacey English and Susannah Hammond, FINTECH, REGTECH and the Role of Compliance: A regulatory opportunity or challenge ? Thomson Reuters, 2016, 24 pages.

V. ANNEX: Statistics 2016

Table of contents

1. KEY FIGURES

1.1. Disclosures sent to CTIF-CFI

In 2016, CTIF-CFI received 27.264 disclosures from the financial sector and the designated non-financial businesses and professions. From 2013 to 2015, the number of disclosures to CTIF-CFI rose sharply and remained stable in 2016.

	2014	2015	2016
Number of disclosures	27.767	28.272	27.264
	+20,90 %	+1,82 %	-3,5 %

13.355 disclosures were new money laundering or terrorist financing cases. 13.919 disclosures were additional reports related to existing files.

Section 2 below provides a detailed overview of these 27.264 disclosures.

The 13.355 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.

"Objective" disclosures include disclosures from the Customs and Excise Administration (cross-border transportation of currency), casinos[43], notaries[44] and real estate agents[45]. These disclosing entities are required to inform CTIF-CFI of objective 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. New 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 2016 were grouped into 9.360 files.

	2014	2015	2016
Number of new files opened because of ML or TF suspicions	6.978	8.329	9.360

[43] In accordance with the indicators of the Royal Decree of 6 May 1999 implementing Article 26, § 2, second subparagraph, of the Law of 11 January 1993.
[44] In accordance with Article 20 of the Law of 11 January 1993.
[45] In accordance with Article 20 of the Law of 11 January 1993.

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.

1.3. Files reported to the judicial authorities

In 2016, 831 new files or cases, for a total amount of EUR 1.146,82 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 2016 as well as in previous years.

In 2016, data or information from 2.577 disclosures, received in 2016 or in previous years, were reported to the judicial authorities following analysis. These 2.577 disclosures related to money laundering or terrorist financing transactions for a total amount of EUR 1.285,68 million.

	2014	2015	2016
Number of files reported to the judicial authorities	1.131	992	831
Amounts in the files reported to the judicial authorities(1)	786,05	639,36	1.146,82
Number of disclosures reported to the judicial authorities(2)	5.183	3.646	2.577
Amounts(1) in disclosures reported to the judicial authorities(2)	1.687,23	1.064,13	1.285,68

(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 2016, CTIF-CFI used its power to oppose execution of a transaction on 17 occasions. CTIF-CFI temporarily froze assets worth EUR 2,69 million.

	2014	2015	2016
Number of freezing orders	19	13	17
Total amount of freezing orders(1)	8,71	3,75	2,69

(1) Amounts in million EUR.

2. SOURCES OF DISCLOSURES SENT TO CTIF-CFI

2.1. Disclosures

	2014	2015	2016	% 2016
Currency exchange offices and agents acting as payment institutions (money remittance)	12.504	10.533	9.392	38,55
Credit institutions	6.955	7.747	8.662	31,77
Postal Service – *bpost*	1.392	1.295	1.118	4,10
Notaries	1.373	1.143	1.094	4,01
Casinos	1.110	1.044	930	3,42
National Bank of Belgium	516	665	603	2,21
External accountants, external tax advisors, external licensed accountants, external licensed tax specialists-accountants	133	162	178	0,66
Life insurance companies	129	902	320	1,17
Real estate agents	72	67	35	0,13
Companies for consumer credit	71	33	42	0,15
Company auditors	68	58	68	0,25
Bailiffs	27	48	81	0,30
Stock broking firms	19	43	63	0,23
Insurance intermediaries	9	3	6	0,02
Mortgage companies	7	5	13	0,05
Lawyers	7	2	4	0,01
Management companies of collective investment undertakings	6	0	0	-
Payment institutions managing credit cards	4	0	0	-
Dealers in diamonds	2	34	35	0,13
Branch offices of management companies of collective investment undertakings in the EEA	1	2	2	0,01
Branch offices of investment companies in the EEA	1	2	1	-
Intermediaries in banking and investment services	0	0	1	-
Security firms	0	1	0	-
Clearing institutions	0	0	2	0,01
Lease-financing companies	0	0	3	0,01
Portfolio management and investment advice companies	0	0	0	-
Branch offices of management companies of collective investment undertakings outside the EEA	0	0	0	-

	2014	2015	2016	% 2016
Collective investment undertakings	0	0	0	-
Public Trustee Office	0	0	1	-
Branch offices of investment companies outside the EEA	0	0	0	-
Market operators	0	0	0	-

2.2. Requests for information received from FIU counterparts

	2014	2015	2016	% 2016
FIU counterparts(1)	424	1.007	2.028	7,44

(1) In accordance with Article 22 §2 of the Law of 11 January 1993.

2.3. Notifications received from the Customs and Excise Administration, trustees in a bankruptcy, the Federal Public Prosecutor's Office and the European Anti-Fraud Office of the European Commission (OLAF)

	2014	2015	2016	% 2016
Customs and Excise(1)	1.480	1.505	1.387	5,10
Federal Public Service Finance	1.420	1.941	1.163	4,26
Federal Public Service Economy	8	9	5	-
Federal Public Service Interior	-	-	1	-
Trustees in a bankruptcy	7	1	8	-
Social inspectorate	-	1	-	-
Other administrative services	2	-	-	-
Coordinating Unit for Threat Analysis (OCAM-OCAD)	2	4	2	-
Federal Public Service Health	1	-	-	-
State Security Department (VSSE)	-	2	12	-
General Intelligence and Security Service of the Armed Forces (SGRS-ADIV)	-	-	2	-
Federal Public Prosecutor's Office	-	-	1	-
European Anti-Fraud Office of the European Commission (OLAF)	-	-	-	-

(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

	2014	2015	2016	% 2016
Supervisory authorities	16	12	1	-
GRAND TOTAL (2.1 – 2.4)	**22.966**	**27.767**	**27.264**	**100**

2.5. Institutions and persons having submitted disclosures / total number of disclosing entities

Financial professions	2014	2015	2016	discl. pers. / inst.
Credit institutions	66	67	66	91
Currency exchange offices, payment institutions and institutions for electronic money	18	28	32	64
Life insurance companies	16	14	16	45
Stock broking firms	8	8	8	32
Companies for consumer credit	6	2	5	85
Mortgage companies	3	4	5	108
Payment institutions issuing or managing credit cards	3	0	0	18
Insurance intermediaries	2	2	6	8.882
Management companies of collective investment undertakings	2	2	0	59
Postal Service – *bpost*	1	1	0	1
National Bank of Belgium	1	1	1	1
Branch offices of investment companies in the EEA	1	2	1	12
Branch offices of management companies of collective investment undertakings in the EEA	1	0	1	8
Intermediaries in banking and investment services	0	0	1	15
Clearing institutions	0	0	1	1
Lease-financing companies	0	0	2	93
Portfolio management and investment advice companies	0	0	0	18
Public Trustee Office	0	0	1	1
Branch offices of investment companies outside the EEA	0	0	0	0
Market operators	0	0	0	1
Branch offices of management companies of collective investment undertakings outside the EEA	0	0	0	3
Collective investment undertakings	0	0	0	53
Total	**126**	**128**	**146**	

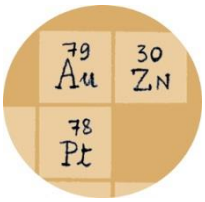
Non-financial professions	2014	2015	2016	discl. pers. / inst.
Notaries	376	311	320	1.500
Accounting and tax professions	82	77	93	9.339
Real estate agents	40	34	18	9.539
Company auditors	22	19	22	1.067
Bailiffs	11	12	12	550
Casinos	9	9	9	9
Lawyers	4	3	4	16.344
Dealers in diamonds	1	3	4	1.600
Security companies	0	1	0	8
Total	**545**	**469**	**482**	

2.6. Breakdown of files by type of main transaction

Transactions[1]	**2014**	**2015**	**2016**	**% 2016**
Deposits into account	884	1.416	2.045	26,05
International transfers	1.304	1.413	1.602	20,41
Withdrawals	966	1.034	1.027	13,08
Fiscal regularisation	1.390	1.918	849	10,82
Domestic transfers	637	755	737	9,39
Securities	79	104	135	1,72
Credits	127	71	81	1,03
Life insurance	73	622	67	0,85
Money remittance	265	288	60	0,76
Real estate	90	77	50	0,64
Use of cheques	56	53	36	0,46
Casino transactions	1	5	8	0,10
Physical cross-border transportation of currency[2]	6	6	3	0,05
Other	786	577	1.149	14,64
Total	**6.664**	**8.329**	**7.849**	**100**

(1) This table does not include requests from FIU counterparts.

(2) In accordance with Regulation (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.



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 2016, CTIF-CFI reported 831 new files to the judicial authorities for a total amount of EUR 1.146,82 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 2016, CTIF-CFI reported a total of 2.577 disclosures (new files and additional reported files) to the judicial authorities for a total amount of EUR 1.285,68 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

	2014	**2015**	**2016**	**% 2016**
Credit institutions	760	584	557	67,03
Currency exchange offices and agents of payment institutions	145	139	95	11,43
Postal Service – *bpost*	144	188	89	10,71
FIU counterparts	19	29	39	4,69
Accounting and tax professions	5	10	11	1,32
Casinos	5	4	8	0,96
Notaries	11	4	6	0,72
Federal Public Service Finance	1	4	4	0,48
Customs	4	16	3	0,36
Life insurance companies	5	6	1	0,12
Company auditors	2	2	-	-
Other	30	6	18	2,18
Total	**1.131**	**992**	**831**	**100**

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

	2014	**2015**	**2016**	**% 2016**
Credit institutions	657,39	461,85	1.035,67	90,31
FIU counterparts	9,72	25,52	48,90	4,26
Currency exchange offices and agents of payment institutions	17,06	27,36	27,57	2,40
Customs	3,62	39,97	10,29	0,90
Accounting and tax professions	2,85	17,76	7,06	0,62
Notaries	22,55	0,14	4,06	0,35
Postal Service – *bpost*	10,35	9,88	3,33	0,29
Federal Public Service Finance	15,17	4,35	3,08	0,27
Life insurance companies	5,68	3,09	0,98	0,09
Casinos	0,32	0,49	0,76	0,07
Company auditors	35,16	44,75	-	-
Other	6,18	4,21	5,12	0,44
Total	**786,05**	**639,36**	**1.146,82**	**100**

(1) Amounts in million EUR.

Breakdown per category of disclosing institution for disclosures reported to the judicial authorities in 2014, 2015 and 2016

	2014		2015		2016	
	Number	**Amount**[(1)]	**Number**	**Amount**[(1)]	**Number**	**Amount**[(1)]
Credit institutions	1.895	1.422,62	1.666	828,40	1.278	1.148,89
Currency exchange offices and agents of payment institutions	2.679	139,05	1.292	42,62	713	29,36
Postal Service – *bpost*	266	12,78	340	15,00	167	3,72
FIU counterparts	82	32,80	106	44,47	120	51,11
Casinos	74	3,46	62	1,36	85	1,81
Customs	39	4,01	34	40,08	78	11,44
National Bank of Belgium	7	0,20	33	1,36	30	0,90
Life insurance companies	14	6,69	30	4,62	23	1,42
Accounting and tax professions	21	3,54	30	18,36	19	8,01
Notaries	34	23,74	27	4,81	23	8,24
Federal Public Service Finance	12	0,43	7	8,43	8	3,08
Company auditors	4	35,19	5	44,75	3	-
Other	56	2,72	14	9,87	30	17,70
Total	**5.183**	**1.687,23**	**3.646**	**1.064,13**	**2.577**	**1.285,68**

(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. Files reported to the judicial authorities by type of transaction

Main transactions in files reported to the judicial authorities – Evolution in the past 3 years[1]

Type of transactions	2014	2015	2016	% 2016
Withdrawals	269	217	183	23,11
Money remittance	243	288	147	18,56
Deposits into account	146	110	134	16,92
Domestic transfers	138	124	114	14,39
International transfers	164	100	96	12,12
Casino transactions	5	5	8	1,01
Securities, precious metals	5	5	8	1,01
Cheques	15	11	6	1,00
Credits	21	8	3	0,30
Real estate	11	4	3	0,30
Physical cross-border transportation of currency[2]	4	6	3	0,30
Other	91	85	87	10,98
Total	**1.112**	**963**	**792**	**100**

(1) This table does not include requests from FIU counterparts.
(2) In accordance with Regulation (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.

Amounts – Evolution in the past 3 years[1]

Type of transactions	2014	2015	2016	% 2016
International transfers	384,26	226,18	788,80	71,84
Domestic transfers	69,55	64,03	104,62	9,53
Withdrawals	153,35	106,44	96,64	8,80
Deposits into account	54,89	45,99	32,54	2,96
Securities, precious metals	3,96	4,71	14,95	1,36
Physical cross-border transportation of currency[2]	3,62	0,85	10,29	0,94
Money remittance	16,13	17,19	8,15	0,74
Cheques	13,08	4,46	3,45	0,31
Credits	5,36	1,25	2,08	0,19
Real estate	3,98	31,72	0,78	0,08
Casino transactions	0,32	0,51	0,76	0,07
Other	67,83	110,52	34,86	3,18
Total	**776,33**	**613,85**	**1.097,92**	**100**

(1) This table does not include requests from FIU counterparts.
(2) In accordance with Regulation (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.

Breakdown of disclosures in files reported to the judicial authorities in 2014, 2015 and 2016 by type of transaction[1]

	2014		2015		2016	
Type of transactions	**Number**	**Amount**[2]	**Number**	**Amount**[2]	**Number**	**Amount**[2]
International transfers	411	561,89	323	463,44	256	815,79
Withdrawals	633	223,50	628	141,79	397	121,00
Domestic transfers	360	115,91	348	109,73	285	123,17
Deposits into account	305	79,36	240	75,48	239	60,84
Money remittance	2.724	26,70	1.443	26,09	678	9,89
Securities	18	18,94	16	5,23	10	14,84
Use of cheques	34	18,81	19	4,84	14	3,59
Credits	48	7,22	32	13,86	16	2,68
Real estate	28	5,13	27	35,40	19	4,85
Physical cross-border transportation of currency[3]	39	4,01	23	0,96	77	11,41
Casino transactions	74	3,46	63	1,38	85	1,81
Sale of precious metals	7	0,99	11	1,53	5	1,03
Other	420	588,51	367	139,94	376	63,67
Total	**5.101**	**1.654,43**	**3.540**	**1.019,67**	**2.457**	**1.234,57**

(1) This table does not include requests from FIU counterparts.
(2) Amounts in million EUR.
(3) In accordance with Regulation (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.

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

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

Predicate offence	2014	2015	2016	% 2016
Fraud	278	314	186	22,38
Terrorism and terrorist financing, including proliferation financing	37	75	112	13,48
Misappropriation of corporate assets	227	139	80	9,63
Illicit trafficking in narcotics	80	80	76	9,15
Fraudulent bankruptcy	105	95	74	8,90
Trafficking in illegal labour	78	80	71	8,54
Serious (and organised) fiscal fraud, whether organised or not(1)	84	52	54	6,50
Illicit trafficking in arms, goods and merchandise	61	38	48	5,78
Organised crime	44	40	36	4,33
Exploitation of prostitution	54	24	35	4,21
Trafficking in human beings	29	17	20	2,41
Breach of trust	22	13	15	1,81
Theft or extortion	12	12	12	1,44
Embezzlement and corruption	12	8	6	0,72
Other	8	5	6	0,72
Total	**1.131**	**992**	**831**	**100**

(1) Since the Law of 15 July 2013 amending the Law of 11 January 1993 came into force.

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

Predicate offence	**2014**	**2015**	**2016**	**% 2016**
Embezzlement and corruption	8,90	23,30	658,99	57,46
Serious (and organised) fiscal fraud, whether organised or not[2]	344,61	235,29	150,37	13,11
Organised crime	42,40	87,24	63,14	5,51
Trafficking in illegal labour	48,35	97,84	57,49	5,01
Misappropriation of corporate assets	77,03	39,58	56,12	4,89
Fraud	107,71	34,54	34,92	3,04
Fraudulent bankruptcy	46,52	31,91	28,70	2,50
Illicit trafficking in arms, goods and merchandise	52,30	34,21	23,04	2,01
Breach of trust	8,90	14,50	22,22	1,94
Trafficking in human beings	17,69	13,22	14,63	1,28
Illicit trafficking in narcotics	11,23	13,68	14,22	1,24
Exploitation of prostitution	8,19	5,52	9,12	0,80
Terrorism and terrorist financing, including proliferation financing	6,82	6,50	6,66	0,58
Exploitation of prostitution	1,48	1,40	1,71	0,15
Other	3,92	0,63	5,49	0,48
Total	**786,05**	**639,36**	**1.146,82**	**100**

(1) Amounts in million EUR.
(2) Since the Law of 15 July 2013 amending the Law of 11 January 1993 came into force.

Disclosures in the files reported to the judicial authorities in 2014, 2015 and 2016 by predicate offence

	2014		2015		2016	
Predicate offence	**Number**	**Amount[(1)]**	**Number**	**Amount[(1)]**	**Number**	**Amount[(1)]**
Embezzlement and corruption	38	17,84	36	69,55	22	676,42[(2)]
Serious (and organised) fiscal fraud, whether organised or not	371	562,67	193	322,22	188	193,06
Organised crime	442	550,75	414	225,34	316	81,87
Trafficking in illegal labour	487	90,11	374	133,04	286	74,19
Breach of trust	55	14,40	33	18,14	61	58,09
Illicit trafficking in arms, goods and merchandise	404	90,28	172	55,82	162	45,55
Fraud	965	125,33	761	47,67	428	38,03
Fraudulent bankruptcy	285	70,28	230	40,65	138	32,72
Misappropriation of corporate assets	456	86,00	370	61,33	160	25,73
Illicit trafficking in narcotics	422	25,11	334	43,56	155	16,49
Trafficking in human beings	290	23,60	108	19,13	100	15,06
Terrorism and terrorist financing, including proliferation financing	154	9,21	406	16,07	350	10,55
Exploitation of prostitution	569	10,43	114	6,90	126	9,62
Provision of investment, currency exchange or fund transfer services without authorisation	13	5,23	2	0,36	46	4,47
Theft or extortion	108	1,53	63	1,19	31	1,84
Fraud detrimental to the financial interests of the European Union	4	3,11	3	0,13	2	-
Serious environmental crime	3	1,05	-	-	-	-
Other	117	0,30	33	3,03	6	2,01
Total	**5.183**	**1.687,23**	**3.646**	**1.064,13**	**2.577**	**1.285,7**

(1) Amounts in million EUR.

(2) In 2016, CTIF-CFI reported two significant files to the judicial authorities involving large amounts.

3.4. Files reported to the judicial authorities by nationality of the main person involved

The table below provides the breakdown by nationality of the main person involved in the files reported to the judicial authorities in 2014, 2015 and 2016.

Nationality	2014	2015	2016	% 2016
Belgian	607	479	498	59,93
Dutch	47	56	30	3,61
French	59	52	30	3,61
Moroccan	17	20	23	2,77
Portuguese	22	17	18	2,17
Turkish	16	19	17	2,05
Brazilian	21	26	14	1,68
Italian	12	11	13	1,57
Romanian	39	19	12	1,45
Ivorian	-	33	10	1,20
Bulgarian	23	7	10	1,20
Russian	4	6	10	1,20
Nigerian	6	12	9	1,08
Congolese (DRC)	12	5	7	0,84
Cameroonian	10	5	4	0,48
Ghanaian	-	10	3	0,36
British	11	9	3	0,36
Polish	10	6	3	0,36
Hungarian	4	6	1	0,12
Albanian	14	6	0	0
Beninese	-	5	0	0
Other	197	77	116	13,96
Total	**1.131**	**992**	**831**	**100**

3.5. 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 2016[46]. These tables are intended to help disclosing entities apply the statutory compliance measures.

3.5.1. Residence in Belgium

The table below provides the breakdown for the 694 files reported to the judicial authorities in which the main person involved resided in Belgium.

	Number of files	%
Brussels	284	40,92
Antwerpen	103	14,84
Hainaut	67	9,65
Oost-Vlaanderen	61	8,79
Vlaams-Brabant	12	1,73
West-Vlaanderen	39	5,62
Liège	54	7,78
Limburg	33	4,76
Namur	18	2,59
Brabant Wallon	19	2,74
Luxembourg	4	0,58
Total	**694**	**100**

[46] These tables do not include requests from FIU counterparts or Internet transactions.

3.5.2. Residence abroad

The table below presents the breakdown for the 136 files reported to the judicial authorities in 2016 in which the main individual involved resided abroad.

Country of residence	from 1 January until 31 December 2016	%
Côte d'Ivoire	23	16,91
France	18	13,24
Nigeria	12	8,82
Netherlands	8	5,88
Luxembourg	8	5,88
Tunisia	6	4,41
Romania	5	3,68
Spain	5	3,68
Ghana	4	2,94
Mali	4	2,94
Burkina Faso	3	2,21
Morocco	3	2,21
Portugal	3	2,21
Turkey	3	2,21
United Kingdom	3	2,21
Unknown	3	2,21
Benin	2	1,47
Bulgaria	2	1,47
Democratic Republic of the Congo	2	1,47
India	2	1,47
Poland	2	1,47
United Arab Emirates	2	1,47
Other	13	9,54
Total	**136**	**100**

4. INTERNATIONAL COOPERATION

As the statistics below indicate, in 2016, CTIF-CFI also regularly sent 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. 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 places 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[47] for specific fraud schemes. CTIF-CFI also considers this exchange of information to be spontaneous information exchange.

In 2016, CTIF received and processed 2.028 requests for assistance from counterpart FIUs.

	Date MOU	**Number**
United States	8 July 1994	1.022
Luxembourg	22 April 1999	413
Netherlands	29 June 1995	138
Australia	23 June 1997	120
France	1 February 1994	83
Russia	12 December 2002	18
United Kingdom	24 May 1996	18
Switzerland	16 July 1999	15
Jersey	14 July 2000	13
Spain	16 December 1996	12
Guernsey	21 September 2000	10
Czech Republic	17 November 1997	9
Italy	15 May 1998	9
Germany	19 December 2000	7
Poland	21 March 2002	7
Bulgaria	2 March 1999	6
Canada	2 January 2003	6
Cyprus	9 October 1998	6

[47] Warnings or information on money laundering techniques are published on CTIF-CFI's website or in its annual report.

Democratic Republic of the Congo	27 September 2011	6
Hungary	18 January 2000	6
Nepal	-	5
Singapore	7 September 2001	5
Gibraltar	17 October 2000	4
Malta	23 January 2003	4
Mauritius	14 November 2005	4
Seychelles	26 September 2016	4
Ukraine	19 September 2003	4
Bangladesh	3 June 2014	3
Cameroon	-	3
Israel	21 July 2002	3
Mali	12 August 2010	3
Portugal	5 March 1999	3
Romania	27 November 2000	3
Anguilla	-	2
Argentina	24 June 2004	2
Ghana	8 September 2015	2
Latvia	27 July 1999	2
Madagascar	2 October 2012	2
Monaco	20 October 2000	2
Philippines	2 February 2012	2
Senegal	21 November 2005	2
Tunisia	5 May 2011	2
Turkey	16 May 2003	2
United Arab Emirates	26 May 2009	2
Albania	-	1
Andorra	10 July 2002	1
Aruba	14 June 2004	1
Austria	17 October 2000	1
Chad	-	1
Costa Rica	-	1
Denmark	30 March 1998	1
Finland	29 October 1998	1
Georgia	8 August 2005	1
Greece	8 October 1999	1
Guatemala	3 February 2003	1
Iceland	-	1
Ireland	17 October 2000	1

Isle of Man	-	1
Japan	27 June 2003	1
Kazakhstan	-	1
Kyrgyzstan	2 February 2016	1
Lebanon	10 September 2002	1
Lithuania	18 October 1999	1
Macedonia	21 October 2008	1
Malaysia	-	1
Moldova	7 December 2007	1
Montenegro	-	1
Niger	24 October 2012	1
Nigeria	-	1
Panama	3 May 2001	1
Samoa	-	1
Saudi Arabia	-	1
Slovakia	6 June 2000	1
Slovenia	23 June 1997	1
South Africa	29 July 2003	1
Tanzania	-	1
Thailand	24 April 2002	1
Trinidad and Tobago	-	1
Total		**2.028**

In 2016, CTIF-CFI sent 1.083 requests for information to counterpart FIUs.

	Date MOU	**Number**
France	1 February 1994	223
Netherlands	29 June 1995	165
Luxembourg	22 April 1999	71
Germany	19 December 2000	70
United Kingdom	24 May 1996	61
Spain	16 December 1996	38
Italy	15 May 1998	27
Hong Kong	21 December 1998	25
United States	8 July 1994	21
Switzerland	16 July 1999	19
Romania	27 November 2000	17
Bulgaria	2 March 1999	16
United Arab Emirates	26 May 2009	16
Poland	21 March 2002	15
China	5 November 2008	14

Panama	3 May 2001	14
Morocco	26 August 2010	13
British Virgin Islands	13 December 2000	12
Israel	21 July 2002	12
Russia	12 December 2002	11
Greece	8 October 1999	10
Turkey	16 May 2003	10
Hungary	18 January 2000	9
Democratic Republic of the Congo	27 September 2011	7
Lebanon	10 September 2002	7
Monaco	20 October 2010	7
Portugal	5 March 1999	7
Slovakia	6 June 2000	7
Ukraine	19 September 2003	7
Croatia	25 January 1999	6
Cyprus	9 October 1998	6
Ireland	17 October 2000	5
Kazakhstan	-	5
Sweden	22 March 1996	5
Albania	-	4
Canada	2 January 2003	4
Denmark	30 March 1998	4
India	-	4
Liechtenstein	15 March 2002	4
Singapore	7 September 2001	4
Thailand	24 April 2002	4
Algeria	27 April 2010	3
Australia	23 June 1997	3
Brazil	23 July 1999	3
Cayman Islands	-	3
Czech Republic	17 November 1997	3
Finland	29 October 1998	3
Latvia	27 July 1999	3
Lithuania	18 October 1999	3
Norway	7 June 1995	3
Serbia	20 February 2004	3
South Africa	29 July 2003	3
South Korea	11 March 2002	3
Andorra	10 July 2002	2

Bahamas	30 November 2001	2
Cameroon	-	2
Colombia	6 June 2002	2
Estonia	20 November 2000	2
Georgia	8 August 2005	2
Gibraltar	17 October 2000	2
Isle of Man	-	2
Jordan	15 June 2014	2
Macedonia	21 October 2008	2
Malta	23 January 2003	2
Philippines	2 February 2012	2
Qatar	-	2
Seychelles	26 September 2016	2
Slovenia	23 June 1997	2
Tunisia	5 May 2011	2
Argentina	24 June 2004	1
Austria	17 October 2000	1
Bahrain	-	1
Belarus	-	1
Belize	-	1
Benin	15 October 2010	1
Bermuda	30 June 2005	1
Curacao	7 June 2002	1
Dominica	-	1
Egypt	-	1
Gabon	-	1
Guernsey	21 September 2000	1
Iceland	-	1
Indonesia	1 February 2005	1
Kenya	-	1
Madagascar	2 October 2012	1
Malaysia	-	1
Marshall Islands	-	1
Mauritius	14 November 2005	1
Mexico	27 January 2000	1
Moldova	7 December 2007	1
Namibia	-	1
New Zealand	-	1
Peru	7 October 2005	1
Saint Kitts and Nevis	-	1

Saudi Arabia	-	1
Uruguay	-	1
Vanuatu	-	1
Venezuela	6 August 2003	1
TOTAL		**1.083**

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. At present, EU FIUs, including CTIF-CFI, use the FIU.NET as a tool for exchanging operational data.

5. JUDICIAL FOLLOW-UP

5.1. Breakdown by Public Prosecutor's Office of files reported to the Public Prosecutor between 1 January 2012 and 31 December 2016 and follow-up action by the judicial authorities[48]

	Total	%	Conv.	Acq.	VCR	Inv.	Dis.	FJA	Clos.	Enq.
Brussel	**2.290**	**32,75**	**82**	**-**	**15**	**55**	**1**	**19**	**1.191**	**927**
Antwerpen	**1.129**	**16,15**	**106**	**1**	**10**	**32**	**1**	**2**	**408**	**569**
Antwerpen	870	12,44	97	-	6	26	1	1	328	411
Mechelen	111	1,59	2	1	-	3	-	-	6	99
Turnhout	148	2,12	7	-	4	3	-	1	74	59
Hainaut	**674**	**9,64**	**14**	**-**	**3**	**15**	**-**	**5**	**71**	**566**
Charleroi	307	4,39	6	-	-	4	-	2	25	270
Mons	217	3,10	4	-	-	8	-	-	25	180
Tournai	150	2,15	4	-	3	3	-	3	21	116
Oost-Vlaanderen	**657**	**9,40**	**28**	**-**	**7**	**11**	**1**	**1**	**205**	**404**
Dendermonde	233	3,33	5	-	2	6	-	-	45	175
Gent	358	5,12	22	-	5	4	1	1	139	186
Oudenaarde	66	0,94	1	-	-	1	-	-	21	43
West-Vlaanderen	**410**	**5,86**	**9**	**-**	**12**	**13**	**-**	**4**	**107**	**265**
Brugge	200	2,86	3	-	8	7	-	-	38	144
Ieper	29	0,41	3	-	1	-	-	-	2	23
Kortrijk	144	2,06	2	-	2	4	-	3	59	74
Veurne	37	0,53	1	-	1	2	-	1	8	24
Liège	**426**	**6,09**	**26**	**-**	**1**	**21**	**-**	**2**	**139**	**237**
Huy	29	0,41	3	-	-	1	-	-	10	15
Liège	337	4,82	23	-	1	17	-	2	106	188
Verviers	60	0,86	-	-	-	3	-	-	23	34
Limburg	**343**	**4,91**	**7**	**-**	**6**	**10**	**-**	**-**	**124**	**196**
Hasselt	189	2,70	6	-	3	3	-	-	94	83
Tongeren	154	2,20	1	-	3	7	-	-	30	113
Federal Public Prosecutor's Office	**333**	**4,76**	**8**	**-**	**2**	**7**	**-**	**2**	**47**	**267**
Namur	**176**	**2,52**	**1**	**1**	**1**	**9**	**-**	**-**	**25**	**139**
Dinant	35	0,50	-	-	-	4	-	-	9	22
Namur	141	2,02	1	1	1	5	-	-	16	117
Brabant Wallon	**153**	**2,19**	**-**	**-**	**1**	**1**	**-**	**-**	**18**	**133**
Leuven	**143**	**2,05**	**2**	**-**	**1**	**1**	**1**	**1**	**16**	**121**
Luxembourg	**122**	**1,74**	**1**	**-**	**-**	**-**	**1**	**-**	**44**	**76**
Arlon	**105**	**1,50**	**1**	**-**	**1**	**6**	**-**	**1**	**13**	**83**
Marche-en-Famenne	55	0,79	-	-	-	-	-	1	9	45
Neufchâteau	24	0,34	-	-	1	5	-	-	-	18
Brabant Wallon	26	0,37	1	-	-	1	-	-	4	20
Eupen	**31**	**0,44**	**-**	**-**	**1**	**-**	**-**	**5**	**9**	**16**
	6.992	**100**	**285**	**2**	**61**	**181**	**5**	**42**	**2.417**	**3.999**

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

[48] This table was drawn up based on the information and the copies of judgments held by CTIF-CFI on 15 January 2016 and that were spontaneously sent to CTIF-CFI in accordance with Article 33 § 6.

5.2. Judicial follow-up – fines and confiscations

The table[49] below provided an overview of the fines and confiscations imposed by courts and tribunals, by Public Prosecutor's Office in files reported to the judicial authorities in the past five years (2012 to 2016) 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 2011 to 2016	**Confiscations 2011 to 2016**	**Total**
Brussels	**€ 5.032.307**	**€ 68.371.198**	**€ 73.403.505**
Antwerpen	**€ 1.620.461**	**€ 91.856.320**	**€ 93.476.781**
Antwerpen	€ 1.439.261	€ 78.651.005	€ 80.090.266
Turnhout	€ 146.875	€ 13.205.315	€ 13.352.190
Mechelen	€ 34.325		€ 34.325
Hainaut	**€ 408.852**	**€ 31.947.812**	**€ 32.356.664**
Mons	€ 156.302	€ 30.573.232	€ 30.729.534
Tournai	€ 124.750	€ 1.152.870	€ 1.277.620
Charleroi	€ 127.800	€ 221.710	€ 349.510
Oost-Vlaanderen	**€ 1.749.081**	**€ 21.059.954**	**€ 22.809.035**
Gent	€ 1.609.681	€ 18.511.069	€ 20.120.750
Dendermonde	€ 139.400	€ 2.541.235	€ 2.680.635
Oudenaarde	-	€ 7.650	€ 7.650
West-Vlaanderen	**€ 148.550**	**€ 12.496.383**	**€ 12.644.933**
Brugge	€ 143.050	€ 11.966.964	€ 12.110.014
Veurne	€ 5.500	€ 529.419	€ 534.919
Limburg	**€ 482.245**	**€ 6.573.774**	**€ 7.056.019**
Hasselt	€ 195.250	€ 3.853.644	€ 4.048.894
Tongeren	€ 286.995	€ 2.720.130	€ 3.007.125
Liège	**€ 118.800**	**€ 1.668.483**	**€ 1.787.283**
Liège	€ 102.800	€ 1.668.483	€ 1.771.283
Huy	€ 16.000	-	€ 16.000
Verviers	-	-	€ 0
Namur	**€ 18.750**	**€ 756.600**	**€ 775.350**
Namur	€ 7.250	€ 723.900	€ 731.150
Dinant	€ 11.500	€ 32.700	€ 44.200
Waals-Brabant	**€ 52.575**	**€ 502.900**	**€ 555.475**
Leuven	**€ 145.840**	**€ 174.650**	**€ 320.490**

[49] This table was drawn up based on the information and the copies of judgments held by CTIF-CFI on 15 January 2016 and that were spontaneously sent to CTIF-CFI in accordance with Article 33 § 6.

Luxembourg	**€ 22.000**	**-**	**€ 22.000**
Marche-en-Famenne	€ 22.000	-	€ 22.000
Total	**€ 9.799.461**	**€ 235.408.074**	**€ 245.207.535**

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.