
The 'Pre-investigative' Role of Financial Intelligence Units in Recovering Assets

MARC PENNA*

Introduction

The commitment to combat money laundering began more than 20 years ago, when a group of industrial countries, including Belgium and Luxembourg, decided to create the Financial Action Task Force (FATF).¹ The FATF is an inter-governmental body established in 1989 which currently comprises 35 member jurisdictions,² two regional organisations (the European Commission and the Gulf Co-operation Council) and nine FATF associate members³ (FATF-Style Regional Bodies, or FSRBs), representing most major financial centres in all parts of the globe.

The mandate of the FATF is to set standards and to promote effective implementation of legal, regulatory and operational measures for combating money laundering (ML), terrorist financing (TF), financing of the proliferation of weapons of mass destruction⁴ and other related threats to the integrity of the international financial system.⁵

* Belgian Financial Intelligence Processing Unit (CTIF-CFI).

¹ See www.fatf-gafi.org.

² See www.fatf-gafi.org/pages/aboutus/membersandobservers/.

³ Asia Pacific Group, Caribbean Financial Action Task Force, Council of Europe Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (Moneyval), Eurasian Group, Eastern and Southern Africa Anti-Money Laundering Group, Financial Action Task Force of Latin America, Inter Governmental Action Group against Money Laundering in West Africa, Middle East and North Africa Financial Action Task Force and Task Force on Money Laundering in Central Africa.

⁴ This aspect will not be covered in this chapter.

⁵ See P de Koster and M Penna, 'The Case of Money Laundering. Real Administrative Procedure Used in the Detection of Fraudulent Transactions' in F Galli and A Weyembergh (eds), *Do Labels Still Matter? Blurring Boundaries between Administrative and Criminal Law. The Influence of the EU* (Brussels, IEE, 2014) 69.

In 1990, the FATF adopted a series of 40 Recommendations, which were revised several times (in 1996, 2001, 2003 and 2012)⁶ to adapt them to new emerging threats. The FATF 40 Recommendations set out a comprehensive and consistent framework of measures that countries should implement in order to combat ML and TF, as well as financing of the proliferation of weapons of mass destruction. The FATF Recommendations set out the essential measures⁷ that countries should have in place to: identify the risks, and develop policies and domestic co-ordination; pursue ML, TF and the financing of proliferation; apply preventive measures for the financial sector and other designated non-financial businesses and professions (DNFBPs);⁸ establish powers and responsibilities for the competent authorities (eg investigative, law enforcement and supervisory authorities) and other institutional measures; enhance the transparency and availability of beneficial ownership information of legal persons and arrangements; and facilitate international co-operation.

FATF members and FSRB members committed to implementing this framework of measures. In the European Union, the 40 FATF Recommendations have been translated into EU AML/CFT Directives (in 1991, 2001 and 2005). The latest European Directive (the 4th one), translating the revised 40 FATF Recommendations of February 2012, was adopted by the European Parliament and the Council in May 2015 and published in June 2015.⁹ This Directive must be transposed by Member States into national legislation before June 2017 at the latest.

Policy- and lawmakers, the financial sector and the DNFBPs, their supervisory or control authorities, the investigative and law enforcement authorities, and many other services of the state are all involved in some way in the implementation of this framework of measures. The objective of all these measures is to prevent ML and TF activities by increasing the transparency of the financial sector (and the DNFBPs), promoting and ensuring a better and effective detection of the ML/TF financial transactions, and enabling the effective and dissuasive prosecution and sanctioning of ML/TF activities—and, for ML, their related predicate offences.

Amongst the FATF-recommended measures, the ongoing and effective detection by the financial sector and by the DNFBPs of suspicious ML or TF transactions and the co-operation with a central and independent anti-ML and counter-financing of terrorism (AML/CFT) unit, called a Financial Intelligence Unit (FIU), are the cornerstone of the whole AML/CFT regime.

⁶ See www.fatf-gafi.org/topics/fatfrecommendations/documents/fatf-recommendations.html.

⁷ FATF, *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation* (Paris, FATF, 2015) (hereinafter FATF 40 Recommendations).

⁸ DNFBPs include: casinos, real estate agents, dealers in precious stones, lawyers, notaries, other independent legal professionals, external accountants and trust and company service providers (general glossary to the FATF 40 Recommendations (ibid) 112).

⁹ Directive 2015/849/EU of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC [2015] OJ L141/73.

This chapter gives an overview of the pre-investigative role of FIUs in recovering criminal assets, with a particular focus on the Belgian experience.

I. What is a Financial Intelligence Unit?

FATF Recommendation number 29 requires that:

Countries should establish a financial intelligence unit (FIU) that serves as a national centre for the receipt and analysis of: (a) suspicious transaction reports; and (b) other information relevant to ML, associated predicate offences and TF, and for the dissemination of the results of that analysis. The FIU should be able to obtain additional information from reporting entities, and should have access on a timely basis to the financial, administrative and law enforcement information that it requires to undertake its functions properly.¹⁰

Many countries in the world have now set up FIUs and imposed AML/CFT measures to prevent the use of their financial system for ML and TF purposes, and to safeguard the integrity of their financial system.

The main rationale of an FIU is to be a 'buffer' between the financial sector (and, more generally, entities and professionals subject to reporting obligations—DNFBPs) and law enforcement and judicial authorities in charge of financial crime investigations and prosecutions. This national centre could be an administrative one, part of the law enforcement authorities, or of a judicial or prosecutorial type.¹¹

A. Administrative-Type FIUs

An administrative FIU is a central national agency, placed under the supervision of a ministry or administration, such as the Ministry of Finance, the Central Bank or a regulatory agency ('autonomous' FIUs), or not placed under such supervision but, rather, independent from law enforcement or judicial authorities ('independent' FIUs).

Administrative-type FIUs are often preferred by the banking sector and by the other reporting entities. Financial institutions and DNFBPs facing a problematic transaction or atypical customer relationship do not have evidence that such a transaction involves ML or criminal activity, or that the customer involved is part of a criminal operation or organisation. They will therefore be reluctant to disclose their suspicions directly to a law enforcement agency. The role of the FIU is to analyse the suspicion, and to send the case for further criminal investigation and prosecution only if the suspicion is substantiated.

¹⁰ See FATF 40 Recommendations (n 7) 24.

¹¹ See International Monetary Fund and World Bank, *Financial Intelligence Units: An Overview* (Washington DC, 2004).

The powers of administrative-type FIUs are limited to the receipt, analysis and dissemination of information and data related to suspicious ML/TF transactions and other related reports; they do not include investigative or prosecutorial powers.

Employees from administrative-type FIUs are generally civilians, hired by the FIU itself, or officials seconded from various administrative services of the state (customs, tax authorities, etc). Employees from administrative-type FIUs are never in contact with the criminals they investigate regarding ML or TF activities. This means that administrative-type FIUs never intercept, detain or question criminals they suspect of ML or TF activities. Administrative-type FIUs do not have the power to judicially seize criminal money or assets and belongings they suspect to be of criminal origin.

However, countries that have opted for an administrative-type FIU usually also give their FIU the power to postpone the execution of a suspicious financial transaction or the power to block any transactions involving the bank accounts of the criminals or criminal organisation for a short period of time (between two and five days) before the prosecutor's office decides whether to seize the criminal proceeds.

B. Law-Enforcement-Type FIUs

The law-enforcement-type FIU is closer to other law enforcement units, such as a financial crimes unit, and benefits from their expertise and sources of information. In return, information received by the FIU can be accessed more easily by law enforcement agencies and can be used in any investigation. Exchange of information may also be strengthened through the use of existing national and international criminal information exchange networks.¹²

A law-enforcement-type FIU normally has the powers of the law enforcement agency itself (without specific ML/TF legislative authority being required), including the power to freeze transactions and seize assets (with the same degree of judicial supervision applied to other law enforcement powers in the country). This is likely to facilitate the timely exercise of law enforcement powers when this is needed. Therefore, under the control of the prosecutor's office, law-enforcement-type FIUs have the power to seize funds, freeze accounts, conduct interrogations, detain suspects and conduct searches.

C. Judicial or Prosecutorial-Type FIUs

Judicial or prosecutorial-type FIUs are most frequently within the prosecutor's jurisdiction, but, like an administrative FIU, they act independently as a 'buffer'

¹² Such as Europol and Interpol.

between the financial sector, the DNFBPs and the prosecutor in charge of the criminal investigations.

Suspicious financial ML/TF activities are directly reported by the financial sector and the DNFBPs to the designated division of the prosecutor's office.

If the ML or TF suspicions of the financial sector and DNFBPs are confirmed by the first inquiries carried out under its supervision, the prosecutor could immediately decide to start a judicial or criminal investigation, and could request the assistance of an examining magistrate or the law enforcement authorities.

The judicial powers (eg seizing funds, freezing accounts, conducting interrogations, detaining suspects and conducting searches) can then be brought into play without delay. The choice of the prosecutor's office or the law enforcement authorities as the location of an FIU does not exclude the possibility of establishing and positioning the FIU as a department of the prosecutor's office or as a police service with special responsibility for financial investigations.

The principal advantage of this type of arrangement is that disclosed information is passed from the financial sector directly to an agency located in the judiciary.

The circumstances or the context of the country could also justify reporting to an administrative FIU, to the law enforcement authorities or to the prosecutor's office. In countries where the financial sector is reluctant to co-operate directly with the law enforcement or judicial authorities (because of a high bank secrecy, for example), an administrative FIU could be more appropriate.

D. The Belgian Experience

CTIF-CFI¹³ is the Belgian FIU and was established by the Law of 11 January 1993 on preventing the use of the financial system for purposes of money laundering or terrorist financing.¹⁴ CTIF-CFI has been operational since 1 December 1993, and is an autonomous public administrative authority, with its own budget (through contributions from the reporting entities).¹⁵ It is supervised by the Minister of Justice and by the Minister of Finance.

The board of CTIF-CFI is composed of eight financial experts, including three magistrates (fully seconded public prosecutors), appointed by the King of Belgium. One of the three magistrates manages the FIU. CTIF-CFI is operationally autonomous: the eight financial experts decide independently and without any constraint if there is any serious indication that the suspicious transactions analysed are related to a potential ML or TF activity. A secretariat of eight people, a team of 30 financial analysts, three strategic analysts, three advisors and a translator assist

¹³ Cellule de Traitement des Informations Financières (CTIF)—Cel voor Financiële Informatieverwerking (CFI).

¹⁴ See www.ctif-cfi.be/website/images/FR/law_be/loi937042015.pdf.

¹⁵ Royal Decree of 11 June 1993 on the composition, the organisation, the functioning and the autonomy of the Financial Intelligence Processing Unit.

the eight financial experts. CTIF-CFI acts as a 'buffer' between the financial sector and the DNFBPs, on the one hand, and the law enforcement and judicial and prosecutorial authorities, on the other.

II. What are the FIU's Sources of Information?

Due to their central position in the AML/CFT system, FIUs manage huge databases with mainly two types of information: information issued from 'reports' and information called 'intelligence'.

A. Reports

Reports contain one or more individual suspicious ML/TF transactions. Usually, a report is the starting point of an FIU's financial analysis or administrative investigation. Reports include ML/TF financial transactions collected from suspicious transaction reports (STRs),¹⁶ currency transaction reports (CTRs),¹⁷ cross-border transaction reports (CBTRs)¹⁸ and cross-border cash transactions reports (CBCTRs).¹⁹

STRs are the result of a subjective but well-documented prior analysis of suspicious transactions by the compliance officers of financial institutions or DNFBPs. The CTRs and CBTRs result from the occurrence of indicators or the exceeding of a defined threshold: CTRs and CBTRs, therefore, are not the result of an actual and substantial analysis.

Depending on the legal system of a country (common or civil law), the country may receive mainly STRs and incidentally threshold-type reports (eg Belgium, France), or mainly CTRs and CBTRs and incidentally STRs (eg United States, Canada). However, all types of FIUs receive copies of CBCTRs or may have access to the CBCTR database.

The STRs, CTRs and CBTRs mainly come from financial institutions (banks, currency exchange offices and payment institutions) and DNFBPs (notaries, real estate agents and accountants). The customs and excise administration is the authority that usually receives and records the CBCTRs, then makes them available to the FIU. Suspicious ML transactions are mostly classified in three categories, according to the different stages of the ML process: injection, layering

¹⁶ STRs: any kind of suspicious transaction reported to the FIU and based on a subjective analysis of the suspicious transactions with regard to the profile of the customer.

¹⁷ CTRs: transactions in cash automatically reported to the FIU when exceeding a given threshold (in general, €/\$10,000).

¹⁸ CBTRs: international transactions (wire transfers) automatically reported to the FIU when exceeding a given threshold (in general, €/\$10,000).

¹⁹ CBCTRs: declarations made by travellers when they travel with more than €10,000 in cash.

and integration. Each stage corresponds to various types of potential suspicious financial transaction.

In the first stage (injection), the 'criminal' or 'illegal' money is injected in cash into the financial system (eg cash deposit into a bank account, currency exchange in a currency exchange office). It is then wire transferred between multiple bank accounts belonging to the criminal organisation (the layering stage). The objective is to move the funds from one bank account to another (if possible, in different countries) to complicate the paper trail and any criminal investigations. After the first and second stages of ML, the funds can be integrated into high-value goods, such as real estate, securities, gold or diamonds, equity investments in commercial companies. When amounts of cash are injected into the purchase of, for example, real estate, the last stage (integration) is used to classify the suspicious transactions.²⁰

B. Preventive Measures Applying to STRs

The effectiveness of the preventive system and adequate detection of suspicious ML/TF transactions depends on the quality of the preventive measures applied by the reporting entities. The preventive measures applicable to the financial sector and DNFBPs mainly include:

- 'know your customer' due diligence measures; measures to identify beneficial owners and beneficial ownership of legal structures;
- constant due diligence measures regarding the (financial) transactions of customers;
- STRing obligations;
- AML/CFT supervision of the financial sector and DNFBPs; and
- vigilance with regard to the nonprofit organisation sector.

The financial sector and the DNFBPs must identify and verify the identity of their customers when establishing a business relationship with a regular customer, in certain types of transactions with occasional customers, in case of doubts about the veracity or adequacy of the identification data regarding an existing customer, and in case of suspicions of ML or TF.

The financial sector and the DNFBPs also have to observe constant due diligence to ensure that the conducted transactions are consistent with the knowledge they have of their customer and of his professional and/or commercial activities.

In large structures, a compliance officer or a compliance department co-ordinates the internal mechanisms designed by the financial institution or the DNFBP to fight ML and TF. In small structures with a limited number of professionals, the compliance officer is one of the professionals.

²⁰ Since 2014, Art 20 of the Law of 11 January 1993 on preventing the use of the financial system for purposes of money laundering or terrorist financing (Law of 11 January 1993), has prohibited any payment in cash for purchasing real estate, even if the amount paid in cash is small.

Compliance officers must closely review any transaction they consider particularly likely, due to its nature, its unusual character in view of the customer's activities, the circumstantial elements or the capacity of the people involved, to be linked to ML or TF. Whenever a financial institution knows or has reason to suspect that a transaction is related to ML or TF, the compliance officer must inform the FIU.

The nature and extent of investigations conducted by the compliance officers on suspicious ML/TF transactions are limited to collecting information available internally (resulting from the implementation of the 'know your customer' due diligence measures and from the analysis of the customers previous transactions profiles) and consulting some specific public commercial databases. Compliance officers do not have access to police, law enforcement, customs or tax authority databases.

Consequently, it is not up to the reporting entities to prove that the suspicious ML/TF transactions detected are ML or TF activities or to identify a potential ML predicate offence. To notify the FIU, financial institutions and DNFBPs only have to suspect transactions of being related to ML or TF activities.

Compliance officers must in good faith assess if there are enough elements to conclude that the suspicious ML/TF transactions could be related to a ML/TF activity and justify an STR to the country's FIU.

The assessment leading to the decision whether or not to notify the FIU must be well reasoned in an internal written report. The assessment (internal written report) made by the compliance officer (ie the reasons why he decided to report (or not report) the suspicious transactions) must be available for review by the supervisory or control authorities. The reporting entities and their representatives are protected from any civil, criminal or disciplinary proceedings if the reporting to the FIU has been made in good faith. Supervisory or control authorities must verify that the reporting entities' internal control mechanisms are adequate and sufficient to meet their legal obligations (including the AML/CFT legal obligations).

C. Measures Applying to CTRs and CBTRs

CTRs and CBTRs never result from a prior subjective analysis by the compliance officer, but they do result from some predefined rules applied automatically to the transactions of customers. The compilation and reporting of the transactions are therefore easier, but require more sophisticated computer software to automatically detect financial transactions and notify the FIU.

FIUs receiving CTRs and CBTRs also have to invest in strong and expansive hardware storage devices, and must invest in adequate computer software to enable them to store and handle all the data received.

The three types of reports (STRs, CTRs and CBTRs) have advantages and disadvantages. STRs present the advantage of resulting from a prior analysis by the compliance officer of the financial institution or DNFBP. Consequently, the suspicious transactions reported are more likely to be ML or TF related.

When the country obliges financial institutions and DNFBBs to complete CTRs and CBTRs, the FIU will receive a large amount of data to store and to handle or analyse. Many CTRs and CBTRs, however, are justified by perfectly legal backgrounds and professional activities, and FIUs may encounter difficulties when trying to extract the illegal or ML/TF transactions from all of the transactions reported (millions are reported each year).

FIUs receiving and handling CTRs and CBTRs depend more on the intelligence coming from a criminal investigation, and they usually initiate an ML/TF investigation after the law enforcement authorities has asked them if they have information about the subjects under investigation.

D. Intelligence

As mentioned earlier, FIUs also collect intelligence. 'Intelligence' is any kind of information (of an ongoing criminal investigation, on suspicions of tax crimes, etc) transmitted spontaneously by a 'non-reporting entity' that the FIU is not authorised to use in order to start an analysis or investigation, but that it can use to understand potential ML or TF activities. Such intelligence may be provided spontaneously by law enforcement authorities, intelligence services, judicial authorities, tax authorities, etc.

Intelligence is not necessarily used immediately; rather, FIUs normally keep the intelligence in their databases for use at a later date, if a suspicious transaction is reported by a financial institution or DNFBB.

E. The Belgian Experience

CTIF-CFI is an administrative FIU that mainly receives STRs from financial institutions and DNFBBs. The financial institutions and DNFBBs have to notify CTIF-CFI before executing a suspicious transaction,²¹ and must indicate any deadline for completing the transaction.

If unable to inform CTIF-CFI prior to completion of the transaction because of its very nature (eg exchanges of currencies of relatively small value, money remittance of small amounts, casino operations) or because delaying execution of the transaction is likely to prevent prosecution of the beneficiaries of the suspected ML, the compliance officer of the financial institution or DNFBB must notify CTIF-CFI immediately afterwards, stating the reason(s) for so doing.

CTIF-CFI may receive reports from the financial sector (eg banks, exchange offices, the Belgian Post with regard to their financial services, the Central Bank when doing businesses with natural persons, stockbroking firms, portfolio management and investment advice companies, life insurance companies, payments

²¹ Art 23, para 1, of the Law of 11 January 1993.

and electronic money institutions); notaries; real estate agents; external accountants, auditors and external tax advisors; leasing companies; companies issuing or managing credit cards; diamond traders; and lawyers (who address their STRs through the president of their bar association, who verifies their validity).²² Some reporting entities may (also) report to CTIF-CFI according to thresholds or indicators. For example, casinos, notaries and real estate agents apply indicators or thresholds when reporting financial transactions to the FIU.²³

Table 1 gives an overview of the number of reports received in 2014 from the main categories of reporting entities.

Table 1: Number of reports received in 2014 from the main categories of reporting entities

Main contributors	Number of reports received	%
Exchange offices and payment institutions (money remittance)	12,504	47.57
Banks	6,955	26.46
Notaries and real estate agents (most of the reports are related to real estate investments)	1,445	5.50
<i>bpost</i> (financial services)	1,392	5.29
Casinos	1,110	4.22
Central Bank	516	1.96
Foreign FIUs	424	1.61
Accountants, tax advisors and auditors	201	0.76
Life insurance companies	138	0.53
Administrative services of the state ^a	1,440	5.48
Supervisors	16	0.06
Others	146	0.56
Total ^b	26,287	100

^a Includes certificates of tax regularisation received in 2014 for which CTIF-CFI is legally competent to check that the tax regularisation was not used for ML or TF purposes.

^b Not including the 1,480 cash declarations (CBCTRs) received in 2014 by the Customs and Excise Administration.

²² In particular, '(a) when they assist their client in the planning or execution of transactions concerning the: buying and selling of real property or business entities; management of his money, securities or other assets; opening or management of bank, savings or securities accounts; organisation of contributions necessary for the creation, operation or management of companies; creation, operation or management of companies, trusts, fiduciaries or similar legal arrangements; (b) or when they act on behalf of and for their client in any financial or real property transaction'.

²³ When reporting to CTIF-CFI, casinos must use the 11 indicators included in the Royal Decree of 6 May 1999 made under Art 26, para 2 of the Law of 11 January 1993. Pursuant to Art 20, para 2 of

When, in the course of their inspections of institutions or persons under their jurisdiction, they identify facts that may be related to ML or TF,²⁴ the supervisors of the above-mentioned businesses and professions also have to notify CTIF-CFI.

No civil, criminal or disciplinary proceedings can be instituted against and no professional sanction can be imposed upon the institutions or persons referred to above, their employees or representatives, the president of the bar association, or the management or employees of the supervisory authorities, on the grounds of the information they have disclosed in good faith.²⁵

It is worth mentioning that since the Law of 11 January 1993 was amended (in 2010 and 2012), CTIF-CFI may also receive STRs from the Federal Public Prosecutor's Office when it is investigating a TF case,²⁶ and from officials of the state (tax authorities, intelligence services) when they have ML or TF²⁷ suspicions. Furthermore, according to the Belgian anti-ML law, any request from a counterpart FIU has the same status as an STR, which enables CTIF-CFI to use its investigative powers upon receipt of such foreign request.

In addition to the reports, CTIF-CFI also receives spontaneous intelligence from various administrative services of the state. All this intelligence is maintained in the central database for further use.

III. What is an FIU Investigation (Analysis)?

A. In General

Financial information—including information gathered from STRs, CTRs and CBTRs, as well as from reports on cross-border transportations of cash—has a central role in identifying ML and TF funds, as well as predicate offences.

The recently revised FATF standards now recognise financial investigation and financial intelligence as core elements of the FATF's operational and law enforcement recommendations.²⁸ In June 2012, the FATF adopted a guidance note, which highlights the importance of financial investigations. This guidance note was intended to help policy makers, public prosecutors and law enforcement

the Law of 11 January 1993, when notaries and real estate agents discover that the provision of Art 20, para 1 has not been respected and that the sales price of a real estate has been paid in cash (even partially) they shall immediately inform the CTIF-CFI in writing or by electronic means.

²⁴ Art 31 of the Law of 11 January 1993.

²⁵ Art 32 of the Law of 11 January 1993.

²⁶ Art 33, para 5 of the Law of 11 January 1993.

²⁷ Art 33, para 3 of the Law of 11 January 1993.

²⁸ FATF Recommendation No 30: 'At least in all cases related to major proceeds-generating offences, the designated law enforcement authorities should develop a pro-active parallel financial investigation

authorities to better understand their role²⁹ in the larger AML/CFT context, specifically addressing the role of financial investigation.

A financial investigation³⁰ is an enquiry into the financial affairs related to criminal conduct. Its primary goal is to identify and document the movement of money during the course of a criminal activity. The link between the origins of the money, its beneficiaries, when the money is received and where it is stored or deposited can provide information about and proof of criminal activity. Identifying the extent of criminal networks and the scale of crime (and gathering evidence that can be used in criminal proceedings), as well as tracing the proceeds of crime, terrorist funds and other proceeds subject to confiscation, are all part of an overall effective AML/CFT regime. The following can be considered the main objectives of FIU financial investigations:

- identification of all the people and corporate structures involved in ML and criminal activities;
- identification of the beneficial owners of the corporate structures and legal constructions involved;
- tracing of the origin and destination of funds;
- collection of law enforcement information on all the people, corporate structures and legal constructions involved;
- identification of links to people and criminal activities;
- identification of potential predicate offences to the ML transactions;
- identification and disruption of activities of criminals and ML organisations; and
- support of judicial and law enforcement authorities to seize proceeds of crimes.

The FIUs in some countries mainly collect STRs, CTRs, CBTRs, CBCTRs and other relevant data, and make them available on request or on demand of the law enforcement authorities. Other FIUs proactively analyse the STRs, CTRs, CBTRs and CBCTRs to detect potential unknown ML and predicate offence activities.

when pursuing money laundering, associated predicate offences and terrorist financing. This should include cases where the associated predicate offence occurs outside their jurisdictions. Countries should ensure that competent authorities have responsibility for expeditiously identifying, tracing and initiating actions to freeze and seize property that is, or may become, subject to confiscation, or is suspected of being proceeds of crime. Countries should also make use, when necessary, of permanent or temporary multi-disciplinary groups specialized in financial or asset investigations. Countries should ensure that, when necessary, co-operative investigations with appropriate competent authorities in other countries take place.

²⁹ The guidance note also applies to those competent authorities which are not law enforcement authorities per se, but which have the responsibility of pursuing financial investigations of predicate offences, to the extent that these competent authorities are exercising functions covered under Recommendation No 30 (anti-corruption enforcement authorities and tax authorities with enforcement powers).

³⁰ See FATF, 'Operational Issues. Financial Investigations Guidance', available at www.fatf-gafi.org.

To investigate the STRs, most FIUs have the legal power to request (additional) information from various authorities (eg the reporting entity itself, other reporting entities covered by the AML/CFT regime, the law enforcement authorities, the prosecutor's office, the intelligence services, the tax authorities, the social security services).

B. The Belgian Experience

Upon receipt of an STR from one of the above-mentioned reporting entities and/or from a competent authority (federal prosecutor, administrative services of the state), CTIF-CFI is empowered to request and receive any information it deems useful in order to analyse the suspected ML/TF transactions³¹ from different authorities, such as the reporting entity itself; all other financial institutions and persons subject to the AML/CFT law; the law enforcement authorities (all police agencies via two liaison officers from the Federal Police); the public prosecutor's office; all administrative services of the state (tax authorities, intelligence services, customs); the supervisory, regulatory or disciplinary authorities of the reporting entities; and the European Commission's Anti-fraud Co-ordination Unit, OLAF. As mentioned above, CTIF-CFI may also receive spontaneous information from these authorities.

The worldwide spread of ML mechanisms, the complexity of arrangements set up by criminal organisations and the extreme mobility of financial transactions make the exchange of information between countries an absolute necessity to combat ML and TF efficiently. CTIF-CFI therefore co-operates with its counterpart FIUs abroad, and actively participates in the work of the Egmont Group of FIUs.³² CTIF-CFI has signed memoranda of understanding with around 100 other FIUs across the world, but international co-operation may also take place on a case-by-case basis and under conditions of reciprocity. Information is exchanged between FIUs securely through the Egmont Secure Web (a worldwide system) or through the FIU.NET system (between the 28 Member States of the European Union), sponsored by the European Commission.

When identifying serious indications of ML, restricted, however, to one or more of the predicate offences enumerated in the Law of 11 January 1993,³³ or of TF, CTIF-CFI must report the results of its analysis and investigations to the public prosecutor for further investigation and prosecution. CTIF-CFI reports between 1,000 and 1,300 new cases to the public prosecutor's office each year, involving

³¹ Art 33, para 1 of the Law of 11 January 1993.

³² The Egmont Group of Financial Intelligence Units, created in 1995 on the initiative of the Belgian FIU (CTIF-CFI) and the American FIU (FinCEN), currently consists of 151 member FIUs. The main objective of the Egmont Group is to increase and improve international co-operation between FIUs around the world (www.egmontgroup.org/).

³³ Art 5 of the Law of 11 January 1993.

a total amount of between €600 million and €1 billion. CTIF-CFI does not have discretionary power, like magistrates or the public prosecutor's office, to assess whether to prosecute or not. Rather, as soon as CTIF-CFI identifies serious indications of ML or TF, it is obliged to forward the file to the judicial authorities. Most of the time, CTIF-CFI has only 'serious indications' of ML or TF, but no real evidence. Collecting evidence that could be used in court is the task of the judicial and law enforcement authorities.

CTIF-CFI's involvement as a buffer between the reporting entities (and other competent authorities) and the judicial and law enforcement authorities prevents the judicial authorities and police services in charge of criminal investigations from becoming needlessly inundated with irrelevant disclosures and information. At the same time, it allows them to benefit from CTIF-CFI's specific expertise and central role.

It is worth mentioning that the FIU experts, employees, the liaison officers seconded to the FIU and the reporting entities and their representatives may not, under any circumstances, inform the client concerned or third parties that information has been transmitted to the FIU or that an investigation into ML or TF is being carried out. This measure is essential to ensure the efficiency of the preventive system.

IV. FIUs and Asset Recovery

A. In General

Tracing the origin and destination of funds helps the location of criminal proceeds and their seizure. Because law enforcement and judicial or prosecutorial-type FIUs remain in direct contact with the financial sector and DNFBPs (the reporting entities) and receive the STRs directly, they are in a better position to judicially seize the funds before they disappear. However, all types of FIUs (including administrative-type FIUs) can play a significant and important role in asset recovery.

In administrative-type FIUs, reporting entities (financial institutions and DNFBPs) must notify the FIU prior to carrying out a suspicious transaction (especially when the financial transaction involves a large amount of money). The FIU then has the right to request and enforce the postponement of the suspicious transaction within a certain time-frame; such a postponement gives the judicial authorities enough time to judicially seize the funds, in this way counterbalancing the disadvantages of having an intermediary (an administrative-type FIU) between the reporting entities and law enforcement authorities in charge of the criminal investigation.

Administrative-type FIUs now have extensive experience in financial investigations. Furthermore, the legal system and the good relationships between FIUs and financial institutions' and DNFBPs' compliance officers facilitate the

access of the FIUs to the financial information held by the financial institutions and DNFBPs.

Most administrative-type FIUs are empowered to obtain from reporting entities all the (financial) information they need within the time-frame they have set. Furthermore, administrative-type FIUs usually obtain this financial information free of charge.

Consequently, the FIU's financial investigation (regardless of the FIU type) is a fundamental resource for the detection of criminal money and criminal assets.

B. The Belgian Experience

When a financial institution reports a suspicious transaction prior to carrying out that transaction, CTIF-CFI will consider the case to be an urgent case requiring immediate attention. The financial institutions generally allow CTIF-CFI a short period (one or two days) to analyse and investigate the reported suspicious transaction.

In order to safeguard the integrity of the related money or property for seizure by the judicial authorities, CTIF-CFI has the power (without having to refer to, or obtain the authorisation of, a court or tribunal) to request the postponement of the reported transaction before the deadline indicated by the reporting institution. This request freezes the transaction for a maximum period of two to five working days. The reporting entity is allowed to inform the customer of CTIF-CFI's postponement only after the first two working days.³⁴

In order not to compromise the safety of the financial institutions' and DNFBPs' employees (customers whose money is retained by the bank following a postponement order could become violent), the power to postpone the transaction (for up to five working days) is used with caution and only in a limited number of cases, where there are strong indications of ML or TF, or in cases involving huge amounts of money and highly suspicious financial transactions.

When CTIF-CFI finds, in the course of an investigation, that there are serious indications of ML or TF, the power to postpone the suspicious financial transactions for five days is also used to give judicial and law enforcement authorities more time to examine the ML/TF case and take the most appropriate actions (eg seize the funds, release the funds to avoid disrupting the criminal investigation, request further law enforcement investigation, appoint an examining magistrate). The figures below give an overview of the number of postponements carried out by CTIF-CFI since 2011:

2011 33 postponements, concerning a total amount of €183.59 million

2012 36 postponements, concerning a total amount of €11.81 million

³⁴ Art 23, para 2 of the Law of 11 January 1993.

2013 25 postponements, concerning a total amount of €12.34 million

2014 19 postponements, concerning a total amount of €8.71 million

It is worth highlighting that the number of STRs received prior to the execution of the suspicious transactions remains small (less than 1 per cent). Furthermore, in many ML/TF cases, CTIF-CFI is not in a position to postpone the (suspicious) transactions because further investigations are required to identify serious indications of ML or TF.

However, even though CTIF-CFI has not postponed the financial transactions in many cases, it has been able to trace huge amounts of criminal assets and belongings, and has informed the prosecutor's office that huge amounts of criminal money could be seized in Belgium or abroad. Consequently, one may suggest that there is no relation between the number of postponement actions (and the amounts involved) and the amounts of the seizures and confiscations at the end of the criminal investigations. Indeed, if, during the course of a financial investigation, CTIF-CFI notes—in case of serious indications of ML or TF—that large amounts of money or high-value assets could be seized, the Law of 11 January 1993 obliges CTIF-CFI to notify the public prosecutor's office and also the Central Office for Seizure and Confiscations (COSC).

Each year, CTIF-CFI notifies COSC of about 200 cases in which large amounts of money or high-value assets could be seized. COSC then works together with the public prosecutor's office to seize and manage the criminal proceeds. For example, following notification by CTIF-CFI, €120 million was seized in one case in 2011 and €60 million was seized in three cases in 2014.

Conclusion

The repeatedly revised FATF 40 Recommendations, now implemented in most Western countries, have been very useful in improving the transparency of the financial system and preventing the use of the financial system for ML and TF. The customer due diligence measures imposed on the financial sector and on DNFBPs (identification and verification of the identity of their customers, 'know your customer' measures, ongoing due diligence with respect to the transactions of their customers) have certainly contributed to the improved stability of the financial system.

However, important challenges remain, since the ML/TF techniques and mechanisms evolve constantly and criminals are always finding new channels and new processes to launder the proceeds of their criminal activities. Two of the 40 FATF Recommendations of February 2012 contain important challenges for FATF members. In particular, they recommend that members analyse and evaluate (on a regular basis) the potential ML/TF risks that could affect the country as a whole, the sectors and the individual reporting entities covered by the AML/CFT regime.

Furthermore, they recommend that FATF members take measures to increase the transparency of the legal structures created or established in their country. These include measures to identify the beneficial owners of corporate structures and legal constructions available in the country, and measures to make this information available to the reporting entities, FIUs, law enforcement and the public.

The recently adopted fourth EU AML/CFT Directive³⁵ requires each Member State to store in a central database information on the beneficial owners of corporate structures and legal constructions created in the country and to keep this database up to date. This is a crucial challenge.

Finally, the use of financial intelligence is an important tool for detecting, tracing and disrupting criminal activities, and confiscating funds and assets from a criminal origin or committed to finance terrorist activities. The recently revised FATF standards now recognise financial investigation and financial intelligence as core elements of the FATF's operational and law enforcement recommendations.

FIUs now have extensive experience in financial investigations. This experience has been used to prevent and prosecute ML (and also TF), but also to trace and ultimately seize and confiscate criminal proceeds. Even if postponement mechanisms are not extensively used, the pre-investigate role of FIUs is becoming more and more important and useful. In Belgium, for example, between 1993 and 2013, in those cases transmitted by CTIF-CFI to the prosecutors, courts and tribunals imposed penalties and confiscations to a total amount of €1.152 billion, representing 5 per cent of the suspicious ML/TF transactions forwarded to the judicial authorities (€22.5 billion) in the same period of time.

It is evident, however, that the effectiveness of the ML/TF investigation and prosecution still needs to be enhanced. The abnormal length of criminal investigations and the exceeding of the acceptable or reasonable time for prosecution are two factors that are increasingly taken into account by courts and tribunals to drop charges. Even if the real percentage of confiscation is probably higher than the United Nations estimate of the proceeds of crime seized worldwide (ie only 1 per cent of the proceeds of crime),³⁶ one may still conclude that increasing the effectiveness of the fight against ML and TF remains a huge challenge for all policy makers.

³⁵ Art 30 of Directive 2015/849/EU.

³⁶ UNODC, 'Estimating Illicit Financial Flows Resulting from Drug Trafficking and Other Transnational Organized Crime', Research Report (Vienna, 2011), available at www.unodc.org.

