Due diligence and access to information – the ways and means!

Philippe de Koster
First Advocate General
Director of CTIF-CFI[1] - Belgian Financial Intelligence Processing Unit

Marc Penna
Advisor at CTIF-CFI – Belgian Financial Intelligence Processing Unit

A. Introduction

The calls for more due diligence measures in the financial sector, for greater access to information, and for better information sharing amongst public and private sectors in the interest of security is the result of the growing threats posed to Western nations by terrorist activities and in particular the recent terrorist attacks in Paris and Brussels, and the growing problem of Foreign Terrorist Fighters (FTFs).

The commitment to combat money laundering (ML) and financial crimes, for instance by introducing due diligence measures in the financial sector, began more than twenty years ago when a group of industrialised countries decided to set up the Financial Action Task Force (FATF)[2]. Since 2001, and the 9/11 attacks in the United States, the FATF has also committed to countering terrorist financing (TF).

The FATF is an intergovernmental body established in 1989 which currently comprises 35 member jurisdictions[3], two regional organisations (the European Commission and the Gulf Co-operation Council) and nine FATF associate members[4] (FATF- Style Regional Bodies or FRSBs). The mandate of the FATF is to set standards (Recommendations) and to promote effective implementation of legal, regulatory and operational measures to fight ML, TF and the financing of proliferation of weapons of mass destruction, and other related threats to the integrity of the international financial system[5]. In 1990, the FATF adopted a series of 40 Recommendations[6], which were revised several times (in 1996, 2001, 2003 and 2012).

The FATF 40 Recommendations set out the essential measures[7] that countries should have in place to: identify the ML/TF risks, and develop policies and domestic coordination; pursue money laundering, terrorist financing 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 (e.g. investigative, law enforcement and supervisory authorities) and other institutional measures; enhance the transparency and availability of

[1] Cellule de Traitement des Informations Financières – Cel voor Financiële Informatieverwerking
[2] See http://www.fatf-gafi.org
[3] See http://www.fatf-gafi.org/pages/aboutus/membersandobservers/
[4] 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
[5] Philippe de Koster and Marc Penna, 'The case of money laundering. Real administrative procedure used in the detection of fraudulent transactions' in F. Galli and A. Weyembergh, Do labels still matter? Blurring boundaries between administrative and criminal law. The influence of the EU (Brussels, IEE, 2014) page 69
[6] See http://www.fatf-gafi.org/topics/fatfrecommendations/documents/fatf-recommendations.html
[7] FATF (2012), 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 of the FATF Recommendations, 112).

beneficial ownership information of legal persons and arrangements, and facilitate international cooperation.

In the European Union, the 40 FATF Recommendations have been transposed into EU Anti Money Laundering/Countering Financing of Terrorism (AML/CFT) Directives (in 1991, 2001 and 2005). The latest (the 4th) European Directive, transposing the revised 40 FATF Recommendations of February 2012, was adopted by the European Parliament and the Council in May 2015[9].

Since the 1990s, and the establishment of the FATF, public and private sector have worked together to protect the integrity of the global financial system and to fight serious crimes. Financial institutions and DNFBPs play an important role in detecting ML/TF suspicious transactions by carrying out due diligence measures and monitoring the financial activities of their customers.

Timely and effective information sharing is a key central requirement of the FATF standards and one of the cornerstones of a well-functioning AML/CFT framework. Because of the growing threats posed by recent terrorist activities, the FATF and many other international organisations, recently called for greater information sharing.

Since the Paris attacks in November 2015, the FATF has held several special meetings with the private sector on information sharing. For the FATF, "the importance of timely and accurate information sharing cannot be overemphasized, especially in the context of the recent terrorist attacks which underscored the importance of having rapid, meaningful and comprehensive sharing of information from a wide variety of sources, across the national, supranational and global scale. Information sharing is equally crucial for combatting transnational and organised criminal networks and syndicates, operating in multiple jurisdictions and legal environments. Multinational money laundering schemes do not respect national boundaries".

The European Commission's action plan to strengthen the fight against terrorist financing[10], adopted in February 2016, also recognises the importance of information sharing in the fight against terrorist financing.

Effective information sharing requires that the right information is shared at the right time, between the right people and in a secure environment. Too much information sharing is counter-productive, while not enough information sharing is also risky, especially in the context of terrorism and terrorist financing activities. We could never know in advance if specific information we hold could be useful to someone else, because we do not know for sure what information they hold. Information which we hold could have added value when added to information of others.

FIUs and law enforcement authorities rely on financial institutions and DNFBPs detecting the right ML/TF suspicious financial transactions at the right time and, conversely, financial institutions and DNFBPs rely on the public sector providing the right and useful information at the right time (trends, analysis of Suspicious Transaction Reports (STRs), lists of targeted suspects or geographical vulnerabilities) to help them to monitor their customer's activities.

Of course, the collection, use or transfer of (financial) data must be protected by privacy and data protection laws, but in cases of national security breaches, the effective implementation of AML/CFT measures should take precedence over privacy and data protection issues.

[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.

[10] http://europa.eu/rapid/press-release_MEMO-16-209_en.htm

The interplay between AML/CFT and data protection frameworks is discussed further on in this paper.

B. Due diligence measures

The private sector collects and processes a lot of personal data that could be useful to monitor a customer's activities and financial flows and to detect suspicious ML/TF financial transactions.

In the banking sector, these data are collected at the time of onboarding of customers or later on in the course of the commercial relationship. To be useful these data must be as accurate as possible and must be updated on a regular basis. In the banking sector, the customer's data are collected and stored locally by the different entities of the financial group.

These data could circulate between the head office, other affiliates or subsidiaries within the same group, or may be exchanged with other financial institutions when these stakeholders are involved with the same customer or the same suspicious transactions, and with the public sector when there are suspicions of ML or TF.

The private sector also holds certain non-financial data about a customer such as their IP addresses, geolocation data when the customer uses the online banking system (sometimes from a foreign country), mobile phone numbers, previous addresses etc. In combination with information from law enforcement and/or intelligence services, these data could be useful for detection and investigation purposes.

Other financial institutions, such as Money Value Transfer Services (MVTS) providers, have other business models and operate through networks of agents all around the world or they use their own distribution channels. As they use a more centralised structure or ledger of wire transfers, they have a global picture of the financial flows of their customers and not just a picture of the local transactions.

The preventive framework mainly includes "know your customer" due diligence measures; measures to identify beneficial owners and beneficial ownership of legal structures; constant due diligence measures of the (financial) transactions of customers; suspicious transactions reporting obligations; AML/CFT supervision of the financial sector and the DNFBPs; vigilance with regard to the NPO sector; etc.

The customer or a third party may not be informed that a STR has been filed with the FIU or that an investigation for ML or TF is ongoing. This obligation results from the confidentiality and tipping-off provisions. It is important to know that STRs are based only on suspicions of ML or TF that only FIUs and law enforcement could confirm using their analysis and investigatory powers.

In certain countries, financial institutions also automatically report transactions above a pre-defined threshold (most of the time USD/EUR 10 000). For instance: Currency Transaction Report (CTRs)[11] and Cross-Border Currency Transactions Reports (CBTRs)[12]. Consequently, FIUs or law enforcement routinely receive thousands of financial transactions (transactions above USD/EUR 10 000, not all are suspicious or ML/TF transactions) that are stored in huge databases. Analytical methods help to extract the right and useful information.

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

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

All types of FIUs receive declarations on the transportation of cash: Cross-Border Cash Transactions Report (CBCTRs)[13] or may have access to the CBCTRs database.

C. Access to information

The personal data collected by financial institutions could be useful to other stakeholders in the private sector and stakeholders in the public sector (FIUs and law enforcement) investigating criminal activities and ML or TF activities.

Today, states accept to restrict fundamental and individual rights in specific situations where access to information could be useful to public safety, national security or to a criminal investigation, including an ML/TF FIU or criminal investigation.

Even if there is no specific FATF requirement or recommendation on information sharing, customer due diligence and information sharing, between private sector stakeholders and between the public and the private sector, are implicit because they are essential to successfully implement the FATF requirements.

Many of the 40 FATF Recommendations (R) and their interpretative notes (INR) impact on issues related to customer due diligence and information sharing[14] mainly (a) between private sector stakeholders and (b) between public and private sector stakeholders: (a) R9 on bank secrecy laws[15], R24 & 25 on transparency and beneficial ownership of legal persons and legal arrangements[16], R13 on correspondent banking[17], R16 on processing wire transfers[18], R17 on CDD measures performed by third parties[19], R18 on implementing group-wide AML/CFT programmes[20].

---

[13] CBCTRs: declaration made by travellers when they travel with more than €10 000 in cash.

[14] Cf. Consolidated FATF Standards on information sharing – June 2016 – http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/Consolidated-FATF-Standards-information-sharing.pdf

[15] Countries should ensure that financial institution secrecy laws do not inhibit implementation of the FATF Recommendations.

[16] Countries should ensure that there is adequate, accurate and timely information on the beneficial ownership and control of legal persons that can be obtained or accessed in a timely fashion by competent authorities [...] Countries should consider measures to facilitate access to beneficial ownership and control information by financial institutions and DNFBPs undertaking the requirements set out in Recommendations 10 and 22. [R24] Countries should ensure that there is adequate, accurate and timely information on express trusts, including information on the settlor, trustee and beneficiaries, that can be obtained or accessed in a timely fashion by competent authorities. Countries should consider measures to facilitate access to beneficial ownership and control information by financial institutions and DNFBPs undertaking the requirements set out in Recommendations 10 and 22. [R25].

[17] With respect to "payable-through account", financial institutions should be required to be satisfied that a respondent bank has conducted CDD on the customers having direct access to accounts of the correspondent bank, and that it is able to provide relevant CDD information upon request to the correspondent bank.

[18] Countries should ensure that financial institutions include required and accurate originator information, and required beneficiary information, on wire transfers and related messages, and that the information remains with the wire transfer or related message throughout the payment chain.

[19] Countries should permit financial institutions to rely on CDD measures performed by third parties if the following conditions are met: (a) the financial institution relying upon a third party should immediately obtain the necessary information concerning elements (a)-(c) of the CDD measures set out in R10. (b) Financial institutions should take adequate steps to satisfy themselves that copies of identification data and other relevant documentation relating to the CDD requirements will be made available from the third party upon request without delay. (c) The financial institution should satisfy itself that the third party is regulated, supervised or monitored for, and has measures in place for compliance with, CDD and record-keeping requirements in line with Recommendations 10 and 11. (d) When determining in which countries the third party that meets the conditions can be based, countries should have regard to information available on the level of country risk.

[20] Financial institutions should be required to implement programmes against money laundering and terrorist financing. Financial groups should be required to implement group-wide programmes against money laundering and terrorist financing, including policies and procedures for sharing information within the group for AML/CFT purposes [...].

(b) INR1 on risk information[21], INR6 on targeted financial sanctions[22], INR8 on protecting NPOs from terrorist abuse[23], INR1 on due diligence and Suspicious Transaction Report (STR), R11 on record keeping and comply with information request from competent authorities, INR19 on dealing with higher risk countries[24], R20 on Suspicious Transaction Report (STR), R21 on tipping-off[25], R34 on feedback, INR26 on supervisors on-site and off-site access to all relevant information on customers, products and services risks and compliance risks, R29/31 on FIU and Law Enforcement Authorities' access to additional information.

The FATF recommendations require competent authorities (FIUs, law enforcement authorities) to have strong legal and operational frameworks or mechanisms to communicate and inform the private sector about potential ML/TF risks and trends. Sharing of information with the private is essential to effective detection of suspicious financial transactions.

Terrorist financing activities are difficult to detect as they often involve legal sources of financing and smaller amounts of money. This is the case in the Foreign Terrorist Fighters (FTFs) files and the Paris and Brussels attacks files handled by the Belgian FIU CTIF-CFI.

In terrorist financing, sharing of information and intelligence, and the sharing of lists of relevant individuals under monitoring or under investigation (the so-called "list-based approach") is crucial to assist the private sector in detecting suspicious TF transactions. But sharing lists of individuals with the private sector is also a highly sensitive issue, especially when law enforcement authorities want to preserve the confidentiality of ongoing investigations.

The nature of transactions makes the linkages by the private sector with a criminal or terrorist activity difficult, unless the financial institution is tipped off by the FIU, the law enforcement or the intelligence services.

[21] Countries should take appropriate steps to identify and assess the money laundering and terrorist financing risks for the country, on an ongoing basis and in order to: [...] (iii) make information available for AML/CFT risk assessments conducted by financial institutions and DNFBPs. Countries should keep the assessments up-to-date, and should have mechanisms to provide appropriate information on the results to all relevant […] self-regulatory bodies (SRBs), financial institutions and DNFBPs. Where countries identify higher risks, they should ensure that their AML/CFT regime addresses these higher risks and [...] either prescribe that financial institutions and DNFBPs take enhanced measures to manage and mitigate the risks, or ensure that this information is incorporated into risk assessments carried out by financial institutions and DNFBPs, in order to manage and mitigate risks appropriately. Financial institutions and DNFBPs should be required to take appropriate steps to identify and assess their money laundering and terrorist financing risks [...] and have appropriate mechanisms to provide risk assessment information to competent authorities and SRBs [...]

[22] The competent authority(ies) should have appropriate legal authorities and procedures or mechanisms to collect or solicit as much information as possible from all relevant sources to identify persons and entities that, based on reasonable grounds, or a reasonable basis to suspect or believe, meet the criteria for designation in the relevant Security Council resolutions. Countries should have mechanisms for communicating designations to the financial sector and the DNFBPs immediately upon taking such action, and providing clear guidance, particularly to financial institutions and other persons or entities, including DNFBPs, that may be holding targeted funds or other assets, on their obligations in taking action under freezing mechanisms.

[23] Countries should use all relevant sources of information in order to identify features and types of NPOs, which, by virtue of their activities or characteristics, are likely to be at risk of terrorist financing abuse. Countries should ensure effective cooperation, coordination and information-sharing to the extent possible among all levels of appropriate authorities or organisations that hold relevant information on NPOs. Countries should ensure that full access to information on the administration and management of a particular NPO (including financial and programmatic information) may be obtained during the course of an investigation.

[24] There should be effective measures in place to ensure that financial institutions are advised of concerns about weaknesses in the AML/CFT systems of other countries.

[25] Reporting entities should be prohibited by law from disclosing ("tipping-off") the fact that a suspicious transaction report (STR) or related information is being filed with the FIU.

The suspects in the recent Paris and Brussels attacks used their bank accounts, their (anonymous) prepaid credit cards and money remittance services to carry out common (not really abnormal or atypical transactions) and small value transactions (including the receipt of social and/or unemployment benefits, small cash deposits and small withdrawals at ATM, money remittance transfers of small amounts, payments of invoices by wire transfers (mainly to two car rental firms), payments of hotel rooms in Paris and payments of multiple small expenditures in shops (for instance to purchase the suitcases or bags used in the Brussels attacks), in airports, in petrol stations and on motorways). The financial transactions that the FIU investigation has directly linked to the preparation and perpetration of the Paris attacks in November amounted to maximum EUR 5 000 to 7 500.

The financial sector may encounter some difficulties to link these apparently usual (not abnormal or atypical) transactions to potential terrorist activities or the potential preparation and perpetration of a terrorist attack, unless the financial sector receives intelligence from the FIU, law enforcement or intelligence services.

However, the information these small financial transactions contain may be useful and highly valuable to the criminal investigation, to localise terrorists and terrorist groups when they withdraw money at an ATM, and to follow their routes and criminal activities when they use their prepaid credit cards or transfer money abroad by wire transfers or money remittance, and to establish linkages and connections between suspects of terrorism.

On its own, such information has no real value. But if shared with the FIU, with law enforcement and intelligence services, they have a great deal of added value and they could contribute greatly to any ongoing criminal investigation.

It is therefore important that the financial sector shares this relevant data with the public sector in a timely fashion.

D. Barriers and challenges to information sharing

In December 2015, the President of the FATF stated in a speech given during a Special Session of the United Nations Security Council meeting of Finance Ministers in New York that: "different data protection laws mean that one of our largest sources of intelligence, the banks, are often prevented from sharing information across borders within their own organisations, let alone with each other or with the authorities"[26].

The FATF Policy Development Group, a subgroup of the FATF, just finished drafting a best practices paper on information sharing. Barriers and challenges to information sharing are also identified in this document, which will be published soon. Some of the identified barriers and challenge are discussed later in this paper.

In July 2016, the Royal United Services Institute for Defence and Security Studies (RUSI) in London also published a study document on information sharing[27]. According to this study there is no apparent conflict between data protection and financial crime regulation under the current AML/CFT and data protection frameworks. But, reporting entities, especially in the financial sector, apparently report a lot of unfocused, poor quality STRs in an effort to protect themselves from further regulatory penalties, and this may create data protection issues. State authorities should, according to RUSI, consequently provide better STR guidance to regulated sectors to avoid over-reporting and

[26] The importance of urgent action to implement FATF's measures to counter terrorist financing and help defeat ISIL – Special Session of the United Nations Security Council meeting of Finance Ministers New York, Thursday 17 December 2015 (www.fatf-gafi.org/publications/fatfgeneral/documents/importance-urgent-action-to-implement-fatf-standards-counter-terrorist-financing.html)

[27] Challenges to information sharing – Perceptions and Realities – Inês Sofia de Oliveira –July 2016 (https://rusi.org/publication/occasional-papers/challenges-information-sharing-perceptions-and-realities)

consequently over-storing of STRs data by FIUs and law enforcement authorities. The issues of data erasure and length of storage of data is also discussed in this study.

Nevertheless, some financial institutions report to RUSI difficulties in implementing existing AML/CFT regulations because of jurisdictional limitations, lack of clarity of existing legislation and the increased demand for information sharing by FATF and national authorities. Legislation should allow for private-to-private and private-to-public sector information sharing whilst taking into account the principles of 'necessity' and 'proportionality'.

These principles of 'necessity' and 'proportionality' and the accuracy of the data exchanged are important because too much information sharing or the sharing of inaccurate personal data may also have an impact on and damage the effectiveness of the preventive AML/CFT framework.

The costs of an effective AML/CFT framework (including the implementation of effective customer due diligence measures) and the importance of the regulatory sanctions (sometimes huge financial penalties) in case of non-compliance are factors that significantly influence the customer acceptance policy of financial institutions. Financial institutions are increasingly reluctant to accept new customers or maintain customer relationships with customers potentially at risk of ML or TF. This is, for instance, the case when a financial institution holds or finds "negative or bad" information on one of its customers, or on specific groups of customers (e.g. on migrants), when the FIU or a law enforcement authority had requested information on one of its customers or when a customer was mentioned in a newspaper article, even if the customer was at that time only suspected of ML/TF or suspected of being involved in criminal or terrorist activities and the suspicions were not subsequently confirmed by the FIU or the criminal investigation.

The FATF has already taken action to tackle de-risking and de-risking will continue to be a priority of the FATF[28].

De-risking creates new AML/CFT challenges. Natural persons, whose access to the financial system is suddenly refused, could use uncontrolled financial service providers, cash or underground financial systems such as "hawala". Such reactions negatively influence the capacity of FIUs and law enforcement to trace and investigate suspicious ML/TF transactions.

In 2016, the European Commission updated the EU data protection and privacy frameworks. A new Regulation ((EU) 2016/679[29]) and a new Directive ((EU) 2016/680[30]) were published on 4 May 2016 and shall be applicable on 25 May 2018. The Directive entered into force on 5 May 2016 and EU Member States have to transpose it into national law by 6 May 2018.

The new Directive (EU) 2016/680 recognizes the importance of the free flow of personal data between competent authorities for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security within the Union and the transfer of such personal data to third countries and organisations. The free flow of personal data must be facilitated while ensuring a high level of protection of personal data.

Regulation (EU) 2016/679 applies in cases where a body or entity collects personal data for other purposes and further processes those personal data in order to comply with a legal obligation to

[28] http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-action-to-tackle-de-risking.html

[29] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

[30] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA

which it is subjected. For example, for the purposes of investigation detection or prosecution of criminal offences, financial institutions retain certain personal data which are processed by them, and provide those personal data only to the competent national authorities in specific cases and in accordance with Member State law.

Any processing of data must be lawful. The collection and processing of the personal data must be a necessary and proportionate measure in a democratic society. The specific purposes for which the personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data. The personal data should be adequate and relevant for the purposes for which they are processed. The collected data should not be excessive and not kept longer than is necessary for the purpose for which they are processed. An appropriate level of security and confidentiality must be ensured when data are collected and processed. The transfer to a third country or international organisation takes place only if necessary for the prevention, investigation and detection or prosecution of criminal offence. The data transferred must be accurate. The transfer may take place in cases where the European Commission has decided that the third country or international organisation ensures an adequate level of protection and safeguards to the provided information.

According to Article 35 of the new Directive, transfer of data may also take place to a third country or international organisation which is not on the European Commission's list of safe countries if and after the Member State competent authorities have assessed the level of personal data protection in the third country or the international organisation and provided a prior authorisation. The transfer of data is also permitted without prior authorisation for the prevention of an immediate and serious threat to public security and if prior authorisation could not be obtained in good time.

The objective of both new pieces of legislation is to have common data protection frameworks in all EU Member States, which reduce the barriers existing between inconsistent legal frameworks of data protection and privacy across different jurisdictions and protect the exchange of data with jurisdictions outside the EU.

According to the FATF, one of these barriers is the inconsistent legal frameworks of data protection and privacy across different jurisdictions, creating AML/CFT implementation challenges for the private sector. Different regional and jurisdictional levels of data protection requirements may influence the fight against ML or TF as they limit the free flow of information within a firm or a group of subsidiaries belonging to the same firm.

In certain countries, the country data protection legislation treats intra-group information sharing as information sharing between third parties. Some data protection legislation considers head offices and subsidiaries/branches as third parties thus creating restrictions in terms of information sharing, preventing efforts to establish a global customer information mechanism and also limiting the ability of a financial group to fully implement group-wide and consolidated AML/CFT compliance policies, procedures and supervision[31]. Because of the above-mentioned limitations a financial institution could file a STR in its home country without informing or instructing its head office or other group subsidiaries. The head office or a foreign subsidiary, not knowing that a STR has been filed, could continue to deal with the same customer, creating a ML/TF risk exposure for the subsidiary and the financial group as a whole.

Some reporting entities from the financial sector also apparently abuse tipping-off provisions to avoid making a consolidated Suspicious Activity Report (SAR) containing all the relevant information across the different jurisdictions. These reporting entities wrongly believe that they are not authorised by the tipping-off provisions to disclose the full picture of a cross-border suspicious financial transaction to two different FIUs simultaneously, without breaching the tipping-off provisions. As a consequence, no single FIU has a complete picture of the transactions, which could

[31] FATF recommendation 18 requires financial institutions to implement group-wide programme against ML/TFD, including policies and procedures for sharing information within the group for AML/CFFT purposes.

connect all the pieces of the puzzle, unless both FIUs exchange the received information with each other using the channel of the international cooperation.

In investigations involving cross-border ML/TF activities or multiple successive cross-border money remittance activities for instance, some financial institutions are known to use the tipping-off provisions as grounds to report to each respective country FIU only a fraction of the available data on a suspicious transaction (the data obtained in the country of each FIU), even though the financial institutions could also have reported the full picture of financial transactions to both FIUs.

The FATF also identified the explicit consent to process personal data as a barrier to information sharing. Processing of personal data requires specific and explicit consent of customers in certain cases. Sometimes data protection legislation also provides that the consent should be a freely given, specific, informed and explicit indication of the individual's wish to agree to the processing of his or her personal data, as expressed by a statement or by a clear affirmative action. The consent requirements may also apply to transfer of data and sometimes a general consent obtained by the financial institutions at the time of onboarding customers is not enough to share information with a subsidiary or an involved third party. In some cases a more specific consent is needed each time the data is processed by financial institutions.

In some countries, for cross-border transfer of data, the domestic or supranational legislative framework requires adequate safeguards to ensure confidentiality of data, an equivalent data protection regime in the recipient country, and in some cases a specific requirement to have a positive determination of such safeguards by the data protection authorities of the host country. The data protection authorities of the host country must first confirm that the information sent to the third country will be subject to an adequate level of data protection.

The new EU data protection legislation will improve the exchange of data with third countries because the European Commission will advise and help EU countries and their financial sector by publishing lists of countries presenting equivalent level of safeguards and data protection as the EU countries.

The FATF also identified challenges in relation to identification of beneficial owners. Beneficial owners may not be customers of the financial institution and financial institutions are not able to obtain the beneficial owner's consent to the collection, processing, or sharing of their personal data. Identities of beneficial owners are obtained by the financial institutions from the representatives of the company without the beneficial owner being present and being aware of this. Obtaining the consent of the beneficial owners is problematic. Finally, the FATF observed that if group-wide financial institutions are not able to share information on beneficial owners they are not able to establish linkage or connections between companies with the same beneficial owners conducting suspicious transactions in other subsidiaries of the group.

The right to be forgotten and to data erasure may inhibit the implementation of the record-keeping requirements according to the FATF best practices paper on information sharing. As per the FATF standards, the customer identification documents and the transaction records are required to be kept for a minimum period of time. Data protection laws may require financial institutions to delete personal data after a certain time and/or some may have maximum retention periods that are shorter than the minimum retention periods provided by the FATF standards. A customer could also terminate the business relationship and ask for deletion of all records on him. The stricter data protection requirements could also be used as an excuse for not (correctly) implementing the FATF requirements and in some countries the bank secrecy legislation may prohibit the release of customer account information, also negatively affecting the investigation. In some countries the FIU is not allowed to request financial information on bank accounts in the country on demand of a foreign FIU, unless the requested FIU already received a SAR on the subject of the foreign request for information.

E. The ways and means

National competent authorities need to share more information, on specific threats or lists of individuals with the private sector, but keeping in mind the high level of sensitivity and confidentiality of the information as well as the need to ensure appropriate safeguards and data protection. Information about particular countries which may pose a greater risk of TF or certain business that may pose a heightened security risk can also be shared with the private sector. Most countries organise a forum or meeting with the private sector at least once a year to discuss emerging threats or risks and trends of ML and TF.

In some countries, specific TF working groups or task forces have been established between public and private sectors. Recently the Belgian authorities adopted a new legal framework to create a central database of all information available on FTFs[32]. The UK's Joint Money Laundering Intelligence Taskforce (JMLIT)[33] is also an innovative model which could be used in other countries. In the Netherlands, ten years ago, the public authorities created a Counter Terrorist (CT) Infobox[34], which is a kind of exchange platform where public partners exchange useful CT information.

The establishment of the Belgian FTF dynamic database will centralize in one place and share all available information on the FTF in relation with Belgium, held by intelligence and police services, as well as other partners. The data can be continually updated according to the evolving situation. The services involved in the fight against terrorism (including the Coordination Unit for Threat Analysis, the Belgian Crisis Centre, the Public Prosecutor's Offices, the federal and local police, the FIU CTIF-CFI, both intelligence services (civil and military), the Belgian Customs and Excises Administration, the Immigration Service, the Belgian jails,…) have been granted a read access and (depending on the competent authority) a direct or indirect write access.

The Joint Money Laundering Intelligence Taskforce (JMLIT) was set up in partnership with the financial sector to combat money laundering. Established in 2015, JMLIT was developed in partnership with the government, the British Bankers' Association, law enforcement and some 20 major UK and international banks. The taskforce uses the available information and its expertise in the public and private sectors to better understand money laundering mechanisms and understand how terrorists use the financial system to finance terrorist attacks. The platform has identified and implemented actions to address these risks. In the future, JMLIT will develop stronger partnerships between governments, regulators, law enforcement, financial intelligence units (FIUs) and business to detect and prevent the flow of illicit funds.

Partners in the CT Infobox bring together information on networks and people involved in one way or another in terrorist activities or radicalization into a central contact point (the CT Infobox). The CT Infobox is a partnership between the intelligence services, tax authorities, the control services of the Ministry of Economic affairs, Immigration and Naturalization Service, the local unit of the National Police, the Royal Military Police, the military intelligence services and the Public Prosecutor's office. It is the task of the CT Infobox to advise on the desirability of providing information within the partnership or to third parties, and also opportunities to take criminal law, immigration law, administrative or intelligence-related measures.

[32] Law of 27 April 2016 on addition measures with regards the fight against terrorism – Loi du 27 avril 2016 relative à des mesures complémentaires en matière de lutte contre le terrorisme (http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&table_name=loi&cn=2016042707)

[33] http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/economic-crime/joint-money-laundering-intelligence-taskforce-jmlit

[34] De CT Infobox tien jaar in werking - Christianne de Poot and Sander Flight - https://www.aivd.nl/actueel/nieuws/2015/03/27/ct-infobox-10-jaar-ruimte-om-te-delen

In Belgium, the FIU CTIF-CFI also holds quarterly informal meetings with the compliance officers of the five major financial institutions in the country. These meetings provide the opportunity to exchange practical experiences and information on trends and emerging TF risks. These meetings are highly valuable in helping reporting entities when monitoring the transactions of their customers. They are greatly appreciated by the private sector. These meetings supplement the information already provided to the reporting entities through the FIU's annual activity reports[35] and via the FIU's website[36].

In certain countries, compliance officers with security clearance are appointed by the private sector to exchange information securely and protect the confidentiality of the shared information. Information is exchanged in meetings gathering stakeholders from the public sector and compliance officers with security clearance appointed by the financial sector.

According to the RUSI study, the amount of data submitted by the financial sector, sometimes defensively or based on very low suspicions of ML/TF and retained by FIUs, law enforcement must be reduced in line with the principles of 'necessity and proportionality'. Two solutions are put forward by RUSI to reduce the over-reporting and increase the quality of information sharing.

Providing financial institutions and DNFBPs with better reporting guidance on ML/TF trends and risks, including implementation of the principles of the list approach and a more effective information or intelligence sharing framework with the private sector on specific TF risks or targets will enable the institutions and DNFBPs to better report suspicious transactions. Better feedback on the quality of the reporting by the financial sector could also be a solution and is essential to reduce the over-reporting and over-storing of inaccurate or unfocused data by FIUs and law enforcement authorities.

Finally, the length of storage of the STRs by FIUs and law enforcement is also identified by RUSI as a major concern in many countries.

In Belgium, the AML/CFT legal framework does not include a provision on the length of time for the storage of data, including STRs, by the FIU. In practice, information or data on STRs older than 10 years are no longer used by the Belgian FIU when a file is forwarded to the Public Prosecutor's Office. These data no longer have any value in prosecution.

F. Conclusions

Timely and spontaneous sharing of relevant, up-to-date, accurate and reasonable (not excessive) amount of data between the private sector stakeholders and between the private and the public sectors with adequate safeguards and protection mechanisms is essential to fight financial crime, protect the integrity of the financial system and prevent abuse by criminals.

The EU clearly understands the importance of the free flow of personal data between competent authorities for the purpose of the prevention, investigation, detection or prosecution of criminal offences (including ML/TF) or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

The 2016 revision of the data protection and privacy EU legislation considers the free but controlled flow of personal data as an important factor for the purpose of the prevention, investigation, detection or prosecution of ML and TF and to disrupt terrorist activities.

Free flow of data involves a two-way relationship between the public and the private sector, the private sector learning from and sharing intelligence with the public sector (new trends, ML/TF

[35] http://www.ctif-cfi.be/website/index.php?option=com_content&view=article&id=206&Itemid=76&lang=en
[36] http://www.ctif-cfi.be/

risks and risk assessments, results of strategic analysis, safeguarded and confidential exchanges of lists of suspects) and vice versa (reporting of suspicious transactions to competent authorities).

Information sharing (public-to-public and public-to-private sector) is particularly important to combat terrorism, prevent terrorist attacks and terrorist financing activities.

The Belgian experience showed that the financial sector has important information and data useful to a criminal investigation, and sometimes not only pure financial data, but also useful intelligence such as terrorists' geolocation data (IP addresses used by terrorists when connecting to online banking system, the country from where the Internet connection was made, geolocation of an ATM used to withdraw cash, pictures of suspect(s) withdrawing cash at an ATM (important because sometimes the one withdrawing the cash is not the holder of the bank account), geolocation of the prepaid credit card used (in specific shops or locations).

But the sharing of information is limited by a number of barriers. The FATF recently identified these barriers and the implementing challenges countries and the public and private sectors encounter when exchanging information and combatting ML and TF.

One of the barriers identified is the inconsistent legal framework of data protection and privacy legislation across different jurisdictions, creating AML/CFT implementation challenges for the private sector.

In May 2016, the EU revised the data protection and privacy frameworks to have the same framework in all EU Member States.

Another barrier is a too strict data protection and privacy framework creating tensions between AML/CFT and data protection frameworks.

The abuse by the private sector of the data protection, privacy and tipping-off legislation to avoid sharing all available (including cross-border) information (STRs or additional financial information) with the FIUs and the law enforcement has also been recognized as a factor negatively impacting on information sharing and on the whole AML/CFT framework.

As a consequence of this practice, no FIU or law enforcement has a full and complete picture of the suspicious financial ML/TF transactions, unless they use the channel of the international cooperation to exchange the data they received from their respective FIUs.

A dialogue between the authorities responsible for data protection and privacy and AML/CFT is, therefore, helpful to adopt compatible and coherent policies and to facilitate financial institutions taking responsibilities in the AML/CFT area.

In certain countries, regulators from the financial sector have regular meetings with the data protection and privacy authorities and provide guidance to the financial sector on how to implement and apply both frameworks (data protection and AML/CFT).

In Belgium, new AML/CFT laws or any revisions of an already existing AML/CFT law is submitted for advice to the data protection and privacy authorities, before the law is adopted by parliament.