Public Consultation on the

Draft Guidance for Private Sector Information Sharing

Table of Contents

[INTRODUCTION 3](#_Toc486335650)

[OBSTACLES TO INFORMATION-SHARING 5](#_Toc486335651)

[INFORMATION-SHARING UNDER FATF RECOMMENDATIONS 10](#_Toc486335652)

[I. INFORMATION-SHARING WITHIN FINANCIAL GROUPS (RECOMMENDATION 18) 10](#_Toc486335653)

[a) What does ‘financial group’ or ‘group-wide’ mean in the context of information-sharing? 10](#_Toc486335654)

[b) What information is required to be shared for group-wide programmes? 11](#_Toc486335655)

[c) Why is sharing of this information important for group-wide programmes? 13](#_Toc486335656)

[d) Sharing of information on suspicions that funds are the proceeds of crime or related to terrorist financing within the financial group in a cross-border environment 15](#_Toc486335657)

[e) Confidentiality of STR and tipping-off (Recommendation 21) and how it interacts with group-wide sharing 17](#_Toc486335658)

[II. INFORMATION-SHARING BETWEEN FINANCIAL INSTITUTIONS WHICH ARE NOT PART OF THE SAME GROUP 20](#_Toc486335659)

[INFORMATION-SHARING IN THE CONTEXT OF SUSPICIOUS ACCOUNTS AND TRANSACTIONS 21](#_Toc486335660)

[CONCLUSIONS 22](#_Toc486335661)

[ANNEX I – SELECTED EXAMPLES AND PRACTICES 23](#_Toc486335662)

PRIVATE SECTOR INFORMATION-SHARING – DRAFT GUIDANCE

|  |
| --- |
| This paper should be read in conjunction with *FATF Recommendations*, in particular Recommendations 9, 18, 20 and 21, their Interpretive Notes and the FATF Glossary.  This should also be read in conjunction with the following:  (a) FATF Guidance on Correspondent Banking Services (October 2016)  (b) Consolidated FATF Standards on Information-sharing (June 2016)  (c) BCBS Guidelines on Sound management of risks related to money laundering and financing of terrorism (February 2016)  (d) FATF Guidance for a risk-based approach for the banking sector (October 2014) |

# 

# INTRODUCTION

Effective information-sharing is one of the cornerstones of a well-functioning AML/CFT framework. Constructive and timely exchange of information is a key requirement of the FATF standards and cuts across a number of Recommendations and Immediate Outcomes.

Information-sharing for AML/CFT purposes in financial institutions such as banks can occur at different levels within the same group. Other financial institutions such as money and value transfer service providers (which operate mostly through agents or other distribution channels) may have different business models and structures. The underlying objective of effective information-sharing applies to all such institutions operating through various structures.

Information-sharing also takes place between different entities and sectors for example between financial institutions not part of the same group and public sectors, and vice versa. Such information flow can take place within the domestic context or it can be across borders. Public-to-public sharing of information is equally critical and is an important element for the efficacy of the domestic co-ordination and co-operation regime. However public-to-public information-sharing is outside the scope of this Paper, as is operational information-sharing relating to specific alerts or risks.

Information-sharing is critical for combatting money laundering, terrorist financing and financing of proliferation. Multinational money laundering schemes do not respect national boundaries. Barriers to information-sharing may negatively impact the supervisory and law enforcement efforts, but do not impact (and can therefore inadvertently facilitate) operations of such networks. This underscores the importance of having rapid, meaningful and comprehensive sharing of information from a wide variety of sources, across the national and global scale.

Sharing information is key to promoting financial transparency and protecting the integrity of the financial system by providing relevant competent authorities the intelligence, analysis and data necessary to combat ML/TF. Similarly, financial institutions depend upon the public sector to share information on trend analysis, patterns of behaviour, targeted suspects or geographical vulnerabilities in order to better manage their risk exposure, monitor their transaction flows and provide a more useful input to law enforcement. The use of data in this manner highlights the importance of a continuous dialogue between the public and private sectors. The reliance on shared information also underlines the increased focus of international efforts towards identifying potential barriers to information-sharing which might impinge on the effectiveness of the system and exploring possible policy and operational solutions to overcome them.

While the Guidance is non-binding and does not overrule the purview of national authorities, the intent of this guidance is to:

1. Identify key challenges that inhibit sharing of information group-wide and between financial institutions not part of the same group;
2. Articulate the FATF Standards on information-sharing regarding: a) group-wide AML/CFT programmes and within its context, sharing of information on suspicious transactions within the group, and how STR confidentiality and tipping-off provisions interact with such sharing; and b) between financial institutions not part of the same group;
3. Highlight country examples of collaboration between data protection and privacy and AML/CFT authorities to serve mutually inclusive objectives;
4. Provide country examples to facilitate sharing of information within group, between financial institutions not part of the same group; and of constructive engagement between the public and the private sectors;
5. Support the effective implementation of the AML/CFT regime, through sharing of information, both in the national and international context.

This guidance applies to:

1. Countries and their national competent authorities with responsibility for AML/CFT;
2. Practitioners in the private sector, including financial institutions that have group-wide AML/CFT programme obligations to fulfil; and
3. National and supra-national data protection and privacy authorities.

The paper sets out the obstacles to information-sharing, including legal constraints and operational challenges. Annex-1 to the paper contains examples of how countries address these obstacles, including of national data protection and AML authorities working together to meet their respective objective. It also sets out practices adopted by countries to promote group-wide information-sharing and between financial institutions which are not part of the same group. The section also contains examples of established mechanisms and processes to ensure guidance and feedback for the private sector, which helps facilitate better information-sharing among all stakeholders.

# OBSTACLES TO INFORMATION-SHARING

Legal Constraints

Legal constraints emanate from different legal frameworks that may inhibit availability, access, sharing and processing of information for AML/CFT purposes. This may be on account of different policy objectives, customer confidentiality concerns and record retention requirements. In this respect, it should be stated that under recommendation 9, *“countries should ensure that financial institution secrecy laws do not inhibit implementation of the FATF recommendations”.* Countries should therefore overcome the challenges to an effective information-sharing regime concerning application of different legal provisions. Quite often, lack of a clear understanding of what is allowed to be shared and what is not also leads to caution from financial institutions about the scope of information that they can share, creating challenges for an effective information-sharing regime. These challenges may manifest themselves as follows:

*Different legal frameworks of Data Protection and Privacy (DPP) and their implementation*

AML/CFT laws and regulations of a jurisdiction are designed to prevent, detect, disrupt, investigate and prosecute ML/TF. Individuals have the right to privacy and to protect their personal data[[1]](#footnote-1) from abuse. This is a fundamental right in many jurisdictions. This right represents an important policy objective in accordance with the fundamental principles of domestic law. AML/CFT goals also serve significant national security and public interest objectives and should be pursued vigorously, in a way that is mindful of an individual’s right to privacy. AML and DPP public policy goals are not mutually exclusive and should recognise, support and complement each other rather than remain in conflict.

The patchwork legal framework of data protection and privacy laws across jurisdictions, including lack of compliance with FATF Recommendation 18, creates implementation challenges, particularly for the private sector in sharing information. The issue seems further compounded when there is a lack of regulatory guidance, or an inconsistent approach towards AML/CFT requirements and DPP obligations. General data protection requirements, particularly those without exceptions for financial crime affecting national security or the public, may impede the effective implementation of AML/CFT requirements. The complexity of different DPP regimes and the fear of penalties and risk avoidance may also affect availability, access, processing or sharing of information by the private sector, even when such sharing is permitted.

Some such examples where it is stated that difference in DPP regimes and/or their application can affect the information flow include:

1. **Barriers to group-wide sharing of information.** Some jurisdictions treat group-wide sharing of information the same as information-sharing with third parties. This is because some data protection legislation considers other subsidiaries or branches as third parties resulting in sharing restrictions. This may also apply to group-wide offices across jurisdictions where such transfer is also made subject to sharing restrictions. This impacts group-level information-sharing for AML/CFT risk mitigation purposes among subsidiaries and their head office and parent companies. For global firms, different regional and jurisdictional levels of data protection requirements are often cited as being significant as they limit the free flow of information within the firm. Principle of data minimisation under DPP framework (which requires that an organisation should only process the personal data that it actually needs to process in order to achieve its processing purposes) often leads to ambiguity, more particularly due to lack of regulatory guidance on the purposes for which such data can be collected, processed and shared. This issue is compounded in instances where such information-sharing is necessary to comply, or would greatly facilitate compliance with, domestic AML/CFT law. National data authorities in some instances are currently working on developing a compliance framework that will take into account the issue of group-wide data sharing.
2. **Processing of personal data** occurs at all financial institutions at account opening for customer due diligence purposes and thereafter as customers engage in transactions for business accounting and risk mitigation purposes, including AML/CFT. In certain jurisdictions, the processing of personal data requires specific and explicit consent of customers, depending on the type of information concerned. In such cases, it is required that consent should be 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 either by a statement or by a clear affirmative action. Consent, where required, also applies to transfer of data. It leads to uncertainty, whether there can be a general consent obtained by the financial institutions at the time of on boarding customers or a more specific consent is needed each time the data is processed by the financial institutions. There may also be a variation among national jurisdictions as to what portions of customer information is considered personal data for data privacy and/or customer privacy law. Furthermore, there may also be an absolute prohibition in certain jurisdictions on transfer of personal data even in situations where the customer consents. It can be challenging for financial institutions to rely upon general consents or public interest exemptions to transfer customer data for the purposes of combatting financial crime. Express legislative provisions or guidance defining the circumstances in which customer data can be transferred for such purposes can help facilitate information-sharing.
3. **In some cases, transfer of personal data to third countries is prohibited** unless the data protection authorities of the home country confirms that information sent to the third country will be subject to satisfactory levels of data protection, using some safeguards (for instance, for transfers of data within the group, the use of Binding Corporate Rules may be approved by such authority). The absence of such a determination may affect the information exchange. While such legislation provides the derogations on grounds of public interest, often these grounds are stated to be available only for case-by-case data transfer and not for systematic transfers of information, which may require a specific legal framework. The timely flow of information in a seamless manner may be impeded by requirements to give prior notification to national data protection authorities and obtain multiple authorisations, which has an impact on information-sharing.
4. **When beneficial owners are included in the business relationship of financial institutions, the access to information concerning beneficial owners may be hindered when the financial institution or affiliates may be located in jurisdictions subject to privacy restrictions or when the beneficial owner of the customer is located in a foreign jurisdiction, which is subject to privacy restrictions.** Therefore, in such cases, the financial institution may be unable to obtain the beneficial owner’s consent, where required, to the collection, processing, or sharing of their personal information. This may lead to conflicts between DPP and AML/CFT requirements, and in practice means financial institutions face additional problems sharing beneficial ownership information. At a group -wide level, this may impede the ability of financial institutions to detect any abnormal patterns by establishing linkages and connections (e.g. transactions between two or more companies with the same beneficial owner), and hinder identification of suspicious patterns of activity. This may pose additional problems in many cases as the beneficial owner’s identity is generally disclosed by a third party (representative of a legal entity), or is obtained and held by the financial institution itself, without the beneficial owner coming into the picture. Obtaining specific consent in these cases is often stated to be challenging.
5. **Implementation of the requirement to apply additional measures to family members and close associates of PEPs** in a way that is compatible with data protection principles may prove challenging. Gathering identification details from various data sources, including information on known relationships between customers (such as family members, close associates etc.) may be considered challenging due to privacy concerns. For instance, the fact of the PEP being an important official of a certain political party, or a same-sex partner of PEP, would reveal political opinions or sexual orientation. Both are considered sensitive data, and as such the processing of those personal data for one or more specified purposes may be prohibited unless the data subject has given explicit consent to it or for reasons of substantial public interest. This, however, does not prevent financial institutions to obtain such information directly from customers or through public sources. In some cases, data protection principles have been cited as preventing appropriate risk profiling of customers for CDD purposes. This may be considered to inhibit consolidating and sharing of such information at the financial group level. In this respect, it should be recalled that financial institutions should have appropriate risk management systems and take reasonable measures to determine whether the customer or the beneficial owner is a politically exposed person. This requirement should apply to family members or close associated of PEPs.
6. **The right of anonymity and to data deletion may inhibit implementation of record-keeping requirements and may jeopardize ML/TF investigations.** Customer and transaction records are required to be kept for a minimum period of five years as per the FATF Standards. Data protection laws may have maximum retention periods that are shorter than the minimum retention periods provided under the FATF standards. In some jurisdictions, there remains uncertainty as to how data retention requirements interact with data protection laws and the “right to be forgotten/right of anonymity” that exists as a corollary of data privacy rights. Furthermore, where consent is required, customers may withdraw such consent, when exiting the business relationship and ask for deletion of all records. This may bring in incompatibility in record maintenance policies.

The objectives of AML/CFT framework (security and protecting financial integrity) and DPP legislation (protecting the fundamental right of individuals to data protection and privacy) are not mutually exclusive. Generally these objectives complement rather than compete with each other. The apparent conflict between them in some cases is due to lack of engagement between different authorities at the rule-making stage, or due to lack of further coordinated guidance or feedback by relevant supervisors. Lack of guidance, or lack of clarity about regulatory expectations, can lead financial institutions to interpret such provisions in a defensive or overly conservative manner, which leads to further tension between the two frameworks.

In some cases, more clarity from national regulators and public authorities on how to effectively manage differing regulatory requirements would be helpful in this regard. For example, global financial institutions operating in multiple jurisdictions would benefit from clarity on the scope of the public interest derogation contained in different data protection regulations (*i.e.* the extent to which transfers of data made for the purpose of complying with anti-money laundering regulations is permissible under this derogation). National competent authorities and financial institutions should consider adopting a proactive approach in this regard to find the right balance between the legislation on both issues. A dialogue between the national authorities responsible for privacy and AML/CFT is, therefore, helpful and indeed needed, to adopt compatible and coherent policies to facilitate financial institutions taking responsibility in this area.

Operational Challenges

IT capability of the financial institutions and their record-maintenance procedures may hinder effective sharing of information in a timely manner. For example, some customer information that might be useful for CDD purposes may not be integrated into financial institutions’ AML/CFT systems because it was collected for a different purpose. Inadequate IT tools, different data formats, lack of policies and procedures on how to deal with the information available and a general lack of appreciation of the value of information available both on the part of the public and private sector may act as barriers to information-sharing, even when it is available. Issues of IT capability and IT integration may also arise when financial institutions grow their global footprint through acquisition, necessitating the integration of different IT systems into those of the acquiring institutions.

With regards to information-sharing between the public and private sectors, operational challenges emerge due to lack of adequate systems, policies and procedures and the overall capacity of the competent authorities to obtain and process information available with the private sector. Quite often, the public sector is also unaware of the types of information on customers, their transactions and activities which is available with the private sector and which may be useful for them. This calls for frequent engagement and dialogue between the public and the private sector. Lack of guidance and feedback on information shared by the private sector may also lead to ambiguity on the objective of the exercise and processes put in place.

Lack of guidance and feedback by public sector authorities can also impede or discourage information-sharing between different private sector entities, or between private and public sectors, and vice versa, e.g. because regulatory expectations are unclear or because there is insufficient information available about risks. The public sector should clearly communicate via guidance and feedback the mechanisms that should be put in place to share information in this context, including detailed guidance on operational aspects, such as the features IT capabilities should meet to efficiently support information sharing practices. Authorities should also consider establishing forums or partnerships to facilitate the exchange of information between all the relevant actors involved in countering ML and TF.

# INFORMATION-SHARING UNDER FATF RECOMMENDATIONS

In June 2016, FATF issued Consolidated Standards on Information-sharing[[2]](#footnote-2) containing relevant excerpts from the *FATF Recommendations* and Interpretive Notes which relate to information‑sharing. The consolidation of existing Standards without any amendments was done in order to add value and to help to clarify the requirements with respect to information-sharing, which are spread across 25 of the *FATF Recommendations*, and which impact 7 Immediate Outcomes in the FATF Methodology for assessing effectiveness. These are a starting point for the issues considered in this paper.

Information-sharing impacts a number of FATF Recommendations. This covers strategic information-sharing (sharing of risk information, latest trends, methods, techniques and typologies). This also involves tactical and operational information-sharing to fill the intelligence gaps and help promote more comprehensive analysis of available data elements with numerous financial institutions as well public authorities. In both the scenarios, public and private sector institutions can be both source and target of information flow.

This section sets out key FATF Recommendations (R.18, R.20, R.21) and their expectations in the context of a) information-sharing within financial group and b) information-sharing between financial institutions not belonging to the same group.

## I. INFORMATION-SHARING WITHIN FINANCIAL GROUPS (RECOMMENDATION 18)

|  |
| --- |
| **Recommendation 18- Internal controls and foreign branches and subsidiaries**  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.  Financial institutions should be required to ensure that their foreign branches and majority-owned subsidiaries apply AML/CFT measures consistent with the home country requirements implementing the FATF Recommendations through the financial groups’ programmes against money laundering and terrorist financing. |

### What does ‘financial group’ or ‘group-wide’ mean in the context of information-sharing?

As per the FATF Glossary, Financial group means a group that consists of a parent company or of any other type of legal person exercising control and coordinating functions over the rest of the group for the application of group supervision under the Core Principles, together with branches and/or subsidiaries that are subject to AML/CFT policies and procedures at the group level.

For the purpose of effective banking supervision, the Basel Core Principles define the term “banking group” to include, on a consolidated basis, the holding company, the bank and its offices, subsidiaries, affiliates and joint ventures, both domestic and foreign. Risks from other entities in the wider group (whether financial or non-financial) are also relevant. This group-wide approach to supervision goes beyond accounting consolidation. In supervising an individual bank which is part of a corporate group, it is thus essential that supervisors consider the bank and its risk profile from a number of perspectives: on a solo basis; on a consolidated basis (in the sense of supervising the bank as a unit together with the other entities within the “banking group”) and on a group-wide basis (taking into account the potential risks to the bank posed by other group entities outside of the banking group).[[3]](#footnote-3)

The term “Group wide” (or “enterprise-wide”) used in the context of AML/CFT Programme requirements for the financial group under FATF Recommendation 18 include all the entities comprised by the definition of financial group laid down in paragraph 21 above. This is in line with the principle that a financial group as a whole may be exposed to ML/TF risk due to activities of its group entities, which are covered under *FATF Recommendations*, and hence such risk should be identified, managed and mitigated at the group level.

FATF Recommendation 18 requires financial institutions to implement group-wide programme against ML/TF, including policies and procedures for sharing information within the group (as defined in FATF glossary) for AML/CFT purposes.

Financial group’s programmes against ML/TF should be applicable to all branches and majority owned subsidiaries of the financial group.[[4]](#footnote-4) These programmes should include policies and procedures for sharing information required for the purposes of CDD and ML/TF risk management. Group-level compliance, audit, AML/CFT and other functions with a role in oversight/management of group-level ML/TF risks should also be provided with customer, account and transaction information from branches and subsidiaries when necessary for AML/CFT purposes.[[5]](#footnote-5) This should be subject to adequate safeguards to ensure confidentiality of information and its use for the intended purposes only.

### What information is required to be shared for group-wide programmes?

Information-sharing in the financial group is meant to effectively identify, manage and mitigate ML/TF risks by the group. Sharing of the following information under ‘customer’, ‘account’ and ‘transaction’ categories is required for an effective group-wide compliance programme, and including information on unusual or potentially suspicious activity and information - in all three categories - gathered in the course of internal investigations (see paragraphs 47-51 for further details). The chart also explains the broad AML/CFT purposes that such sharing seeks to achieve. This is to reinforce the point that sharing of information for group compliance is meant to ensure comprehensive and effective ML/TF risk management and compliance.

| **Types of Information** | **Information elements (as available, when necessary)** | **AML/CFT purposes for sharing information within the group** |
| --- | --- | --- |
| Customer Information | Customer identification and contact information (name and identifier), details of beneficial owners, in case of legal persons and arrangements (as also information on nature of its business and its ownership and control structure), legal form and proof of existence, address of registered office and principal place of business; Legal Entity Identifier (LEI) information, financial assets records, tax records, real estate holdings, information on source of funds and wealth, economic/professional activity, and account files, whether the customer is a PEP (including close associates or family members) or not and other relevant elements from documents collected while on-boarding the customer or updating records etc. | Manage customer and geographical risks (customer and beneficial owners), identify global risk exposure as a result of on-boarding of the same customer or beneficial owner by multiple entities within the group, more efficient record-keeping of customer information. |
| Account Information | Bank/other account details, including the intended purpose of the account, expected location of transactions/activity as expressed by the customer and business correspondence etc. | Effective due diligence and transaction monitoring at group level, justification of transaction pattern vis à vis financial profile, follow-up on any alerts or abnormal trading pattern across the group. |
| Transaction Information | Transaction records, credit and debit card records and usage, past credit history, digital footprints (IP address, ATM usage information etc.), attempted/failed transaction information, currency transaction reports, information on closure of account or termination of business relationship due to suspicion etc. | Global transaction monitoring, alert processing and identifying suspicious transactions, flagging and checking the existence of similar behaviour across business lines within the group. |

It is given that all the exemplificative information as indicated in the above table may not be available or needed in each and every case. This would depend upon the products and services being provided to the customers, geographical location and the overall context. However, sharing of the relevant information by group entities, including subsidiaries and branches with the head office allows the group compliance to put in place comprehensive risk management processes. Consolidated screening and monitoring of customers and transactions to identify potential breaches of targeted financial sanctions also depends on the availability of information about listed entities and customer’s activities with different entities of a group. Such sharing, should be subject to sufficient safeguards including due regard to the specific purpose for use of such information, i.e. for financial crime risk management.

Furthermore, centralised storage of records should not be equated with group-wide sharing of the information contained in records. Access to electronically/centrally stored records should be managed in accordance with confidentiality and other obligations. It should also be noted that the global transaction monitoring must always be done in a manner that enhances compliance with risk management and reporting obligations in all the locations where a multi-national group operates. Thus, monitoring in one location should not weaken compliance with these obligations in other locations where the group operates.

### Why is sharing of this information important for group-wide programmes?

In the broader context, sharing of information for group-wide compliance is important for effective identification, mitigation and management of ML/TF risk by the financial group. This will also allow the group to exercise better internal controls and improve the quality of decision-making on due diligence, transaction monitoring and suspicious transaction reporting. Following are the main outcomes expected out of information-sharing for group-wide programmes:

1. *Global risk assessment*

For an effective group-wide compliance programme, financial institutions should understand the ML/TF risks they are exposed to on a global basis. Such risks may be due to customers, products, geographical profile of their operations, transaction pattern or other factors. A comprehensive understanding and identification of these risks will allow the financial institutions to better structure their risk profile and take commensurate measures. Information from branches, subsidiaries, affiliates and other parts of its business should feed into overall risk assessment. This will help identify and determine the nature and level of ML/TF risk the institution is exposed to, particularly where the shared information relates to customers or relationships that have exposure across a multi-national group's operations and across more than one geographic location of a multi-national group’s operation. Thus, it is important that the group compliance is able to obtain and has access to such information, including from its overseas operations, where required. For example, if Bank A, located in Country X, identifies a money launderer and closes his accounts, but that same money launderer has an account with Bank A’s subsidiary in Country Y, that subsidiary will continue to provide banking services to the money launderer as it will be unaware of the activity and bank actions in Country X. Financial institutions should also, when assessing the ML/TF risks they are exposed to on a global basis, take into consideration the barriers to information sharing as an autonomous risk and define mitigation measures accordingly.

Sharing of information with group compliance (i.e. at a head office level) does not assume that the ML/TF risks should be assessed only by the group compliance for the whole group in all the locations where it operates. Each operation in a given location should be responsible in its own right for assessing its ML/TF risk. For this purpose a local operation of a multi-national group in a given jurisdiction would equally require access to information from group compliance or from other parts of the group that is relevant to its own risk assessment. A multi-national group should, therefore include in its risk assessment and management framework a mechanism to determine when its operations are required to assess multi-jurisdictional risk in relation to a customer relationship and when it would be justified, or indeed required, to share customer or transaction information across more than one geographic location.

1. *Effective mitigation of customer, product, services and geographical risks*

Developing appropriate measures to mitigate customer, products and services and geographical risks requires having adequate information on customers, their transaction patterns, expected location of transactions/activity as expressed by the customer, products and services used and, where necessary, on the source and/or destination of funds. Information so obtained by the financial groups will help them devise appropriate solutions to manage and mitigate risks. For example, based on an overall assessment of customers or customers’ categories, financial institutions may devise policies on additional or enhanced due diligence measures, stricter transaction monitoring procedures, face-to-face interaction with certain customers, more frequent review of customer information etc.

Similarly information shared by a financial institution with group compliance on identified misuse of new or existing products or services and measures taken to mitigate the risks may help the group take a consistent approach in a multi-national environment. Such mitigation procedures at a group level can be implemented effectively only if the group compliance has adequate information about its customers, their transactions and activity level and any abnormal pattern based on available customer information. For example, a politically exposed person (PEP), located in Country X, a high risk jurisdiction for corruption, sends one high-value wire inconsistent with their profile, without an explanation in response to bank’s inquiries, which leads the bank to close the PEP’s account. The same PEP uses another account in Country Y with the same banking group to send structured wire transfer and lies about the source and purpose. The subsidiary in Country Y will not be aware of the account closure in Country X by its subsidiary which will prevent them from properly risk managing the customer. This may also prevent detection of potential STRs in the cross border context based on information gathered from various sources within a group.

1. *Consistent application of controls*

Local operations of a global firm have to be in line with local laws and regulations. At the same time, these should also be subject to its group wide compliance programmes to ensure consistent application of controls across the group level. Enforcement of group wide controls and procedures requires sharing of relevant information with financial institution’s group compliance. In the case of their foreign operations, where the minimum AML/CFT requirements of the host country are less strict than those of the home country, financial institutions should be required to ensure that their branches and majority-owned subsidiaries in host countries implement the requirements of the home country, to the extent that host country laws and regulations permit. If the host country does not permit the proper implementation of internal controls (including sharing of information, when necessary), financial groups should apply appropriate additional measures to manage the ML/TF risks, and inform their home supervisors. If the additional measures are not sufficient, competent authorities in the home country should consider additional supervisory actions, including placing additional controls on the financial group, including as appropriate, requesting the financial group to close down its relationships with the host country.[[6]](#footnote-6)

Information on customers’ identification and acceptance policies, internal and external audit reports, supervisors' on-site inspection reports and sanctions and remedial actions imposed as well as sample records evidencing due diligence measures undertaken, reporting done and record-keeping requirements complied with, where appropriate shared with the group compliance may help enable assessment of implementation. This will allow the firm to enforce its global controls, taking into account the specificities of each country and location. For example, lack of CDD and record-keeping measures undertaken by bank A’s subsidiary in country X may weaken the overall effectiveness of group controls of the bank. Financial institution at a global level may verify the implementation of these measures if its group compliance has access to such records on a sample basis.

1. *Common approach by financial conglomerates having multiple businesses*

Quite often, financial groups have their operations across multiple line of business (bank, securities, insurance, commodities etc.). Group-wide compliance means that such financial conglomerates should be in a position to monitor and share information on their customers’ identities, their transaction and account activities across the entire group. While some adjustments may be needed due to different AML/CFT requirements for each sector, sharing of information would enable a comprehensive risk management approach on a consolidated basis. For example, if financial group A has presence in banking, securities and insurance sector under the same group, unexplained cash deposits by a high-risk customer X in his bank account should trigger an alert about his transactions across other business lines. Absence of such information will allow the customer to continue his transactions in other sectors without similar monitoring or additional due diligence.

The BCBS’s 2016 Guidelines[[7]](#footnote-7) on *“Sound management of risk related to money laundering and financing of terrorism”* alsoprovides comprehensive guidance to banks on the effective management of ML/TF risk in a group-wide and cross-border context. It explains the rationale behind and principles of consolidated risk management; how group-wide AML/CFT policies and procedures should be consistently applied across the group, and, where reflecting local business considerations and the requirements of the host jurisdiction, should still be consistent with and supportive of the broader policies and procedures of the group; and how banks should address differences in home/host requirements. It also provides detail on how banks that are part of a group should share information with members of the same group with a view to informing and strengthening group-wide risk assessment and the implementation of effective group-wide AML/CFT policies and procedures.[[8]](#footnote-8)

### Sharing of information on suspicions that funds are the proceeds of crime or related to terrorist financing within the financial group in a cross-border environment

|  |
| --- |
| **Recommendation 20- Reporting of suspicious transactions**  If a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing, it should be required, by law, to report promptly its suspicions to the financial intelligence unit (FIU). |

*FATF Recommendation* 20 requires financial institutions to report suspicious transactions if it suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing. Recommendation 20 only requires the reporting of suspicious activity in good faith and that does not equate to criminal liability. That is a determination for the national authorities (e.g. law enforcement) to make. Financial institutions are required to file suspicious transaction reports with the financial intelligence unit of the host jurisdiction where they are operating.

Technological advances in recent years have improved the analytic and processing capacity of financial institutions, and their ability to dig deeper in transactions and to identify trends and typologies based on information-flow from multiple locations, products and services and sectors. Harnessing of this potential requires as much information as possible to be brought together, and is in the interest of both the public and the private sectors.

Sharing of information on transactions which are indicative of suspicion, and any internal analysis or examination conducted by branches and subsidiaries with group compliance, can promote effective implementation of group-wide compliance programmes.[[9]](#footnote-9) This applies both to domestic and cross-border environment where customers may have exposure across a group's operations and across more than one geographic location. This allows financial institutions to identify high-risk customers across the group’s business and deploy specific monitoring mechanisms or enhanced measures. This also enables emergence of a global picture of the risk exposure of the financial institution to such customers, thereby promoting implementation of an effective risk-based approach. Such sharing will enable the group compliance to have a look at the possible suspect customer’s activities or transactions across different verticals, lines of business and jurisdictions. This will allow them to conduct sophisticated analyses of suspicious activities, assess these analyses against the client database and build the scenario across its global operations.

In the context of terrorist financing, timeliness of information-sharing is critical. The instant sharing of relevant information within a financial group could be crucial, particularly where customers that were assessed as higher risk (due to their transaction history and/or country of origin) are involved. An initial suspicion by a financial institution that a transaction may involve TF may further be corroborated or confirmed if information on transactions involving the same customer or recipient of funds across the financial group is available. Such a chain of transactions would likely only be picked up if the initial suspicion was shared across the financial group and the customer or recipient was flagged for further attention. The process of sharing the information relating to a suspicion of terrorist financing and obtaining further corroborating information should, however, not cause a delay in the timely submitting of an STR in the host jurisdiction where the suspicion first arose or where the transactions in question have taken place.

The inability to lawfully share such information may potentially lead to inconsistent application of the group-wide compliance programme within the same corporate umbrella. As an example, it may result in a situation where one subsidiary has filed an STR about a particular client or transaction, but another group entity which is not aware, may fail to notice suspicious behaviour based on similar facts, warranting an STR filing. This inhibits the effectiveness of global group-wide compliance programmes. Furthermore, there may be cases in which such a scenario might render the group entity as a whole not compliant with STR requirements in the second jurisdiction, as knowledge of potential suspicious behaviour by the first affiliate could be imputed to the entity.

### Confidentiality of STR and tipping-off (Recommendation 21) and how it interacts with group-wide sharing

|  |
| --- |
| **Recommendation 21 - Tipping-off and confidentiality**  Financial institutions, their directors, officers and employees should be:  (a) …  (b) prohibited by law from disclosing (“tipping-off”) the fact that a suspicious transaction report (STR) or related information is being filed with the FIU. |

Concerns on sharing of information on suspicious transactions within the group and potential solutions

One of the main concerns that relates to sharing of STRs is ensuring their confidentiality. Ensuring the confidentiality of STRs is critical to an effective functioning of the reporting regime.Confidentiality of STRs is needed so that the subject of STR and third parties are not tipped-off, as this can adversely affect intelligence gathering and investigation, and can enable persons to abscond or dispose of assets. Confidentiality also protects the reputation of the person who is the subject of an STR. Finally, confidentiality protects the safety and security of the person filing the report, and breaches of confidentiality have the potential to undermine the entire suspicious transaction reporting regime. Unauthorised disclosure of STRs could also result in a financial institution facing criminal liability in many jurisdictions. These concerns necessarily place limits on the sharing of STRs.

The issue of STR confidentiality can get more complex if such sharing occurs across borders, where different national laws come into play. These may include, for example, national provisions relating to discoverability and production of available records (including STRs filed in host country and shared with group-compliance in home country) in home country’s judicial proceedings, access to databases of financial institutions by national authorities etc.

Concerns also exist on the treatment of foreign STRs or information that reveals the existence of a foreign STR in legal proceedings. This is unclear and varies considerably in both civil and criminal cases across countries. While some countries have regulations which require regulator notification of judicial requests and subpoenas concerning domestic STRs; so that the regulators can intervene to ensure STR confidentiality in the legal proceedings, these regulations do not protect foreign STRs submitted to a foreign FIU. Quite often, concerns also exist regarding the confidentiality of STRs once these are shared cross-border, including their potential misuse for unrelated purposes, leakage to media for political gains, and sharing without due process of law. From an FIU’s perspective, one of the key concerns is to avoid situations where third parties (including authorities in third countries) may have unjustifiable access to the relevant information especially if STRs are shared across jurisdictions systematically rather than because they have a multi-jurisdictional element to them.

Finally, there are concerns that group-wide STR sharing could potentially lead financial groups to submit STRs in their home jurisdiction, rather than the jurisdiction in which the relevant financial institution of the group is located. And a related concern that even if the STR is submitted in the relevant jurisdiction, the financial group’s internal investigation may take place outside the jurisdiction, leaving some relevant information outside the reach of the host FIU’s powers to request additional information from the financial institution. To allay these concerns, it is emphasised that financial institutions are required to file suspicious transaction reports with the financial intelligence unit of the host jurisdiction where they are operating, regardless of any sharing.

What are the possible ways in which such information can be shared within financial group?

There are different ways in which information relating to unusual or potentially suspicious activity can be shared within a financial group, based on the domestic or supra-national legal framework of jurisdictions concerned. This does not necessarily have to be by sharing an STR itself, which is prohibited in certain jurisdictions. This can be achieved, for example through: (a) sharing of information on suspicions (facts, transactions, circumstances and documents upon which suspicions are based, including personal information), together with the results of any internal analysis or examination. This could be without disclosing the fact that the STR is filed in such cases; or (b) sharing of STRs and underlying information; or (c) disclosing the fact that an STR has been filed and sharing underlying information (but not the STR itself).

STR confidentiality and tipping-off provisions are meant to ensure the integrity of the reporting regime. One of the key objectives of tipping-off provisions is that those related to such filings should not be alerted; otherwise it may frustrate the potential investigation and prosecution. These provisions are not intended to restrict information flow on transactions which may be unusual or indicative of suspicion for group compliance to promote effective ML/TF risk management. The emphasis should be on the sharing of information that adds value to improving compliance with risk management and reporting obligations in all the locations where a multi-national group may be operating. The overarching principle should be that the shared information may be found relevant by group compliance for its overall ML/TF risk management across the group. There should, therefore, be a cross-jurisdictional element to the shared information such as a customer that has exposure to operations of the group in more than one location or aspects of the flow of transactions or funds that affect operations in the relevant jurisdictions. Such information flow should be subject to sufficient safeguards to ensure that (a) confidentiality of information so shared is protected and (b) information is used only for AML/CFT purposes.

Financial institutions should determine appropriate criteria for sharing such suspicions for the purpose of group compliance. This may not be the same as for reporting of STR in a host country. For example, in some cases, there may still not be sufficient grounds to convert triggered red flags into to an STR, though sharing of such cases to group compliance may reveal further information which may help making a filing decision. Conversely, in some cases, the very nature of transaction or business relationship of customer with financial institution may not make it relevant for the purpose of group compliance. This may happen if the transactions are localised, without any potential for them to extend to other branches, subsidiaries or sectors. Financial institutions should make appropriate decisions in such instances based on the context, complexity and materiality of identified cases.

The objective of sharing information on suspicious transactions is to enhance the financial institution's compliance with risk management and reporting obligation in all the relevant jurisdictions. Hence systematic sharing of such information on a group-wide basis may not be necessary or conducive to improved compliance with risk management and reporting obligations. Financial institution should expressly address in its risk assessment and management framework where it should lay the basis for identifying the instances and the types of information that will be shared for group compliance. Criteria for reporting suspicions for the purpose of group compliance should be under periodical reassessment to take into account relevant events (such as group-wide audits or reviews) and be subject to supervisory scrutiny. Financial institutions should determine the extent and scope of such information sharing in accordance with laws and regulations in host countries.

Financial institutions should also establish adequate safeguards concerning the confidentiality of information shared, given it may be particularly sensitive in some cases. These should include policies, protocols and procedures for such sharing, including conditions of information flows between the different entities of the group when needed (e.g. when different entities of the group have the same client). Furthermore, existence of suspicion on a client from an entity of the group does not imply automatically/systematically filing an STR by other entities of the group concerned, though it may be an important element for the risk analysis and the risk profile of the business relationship and may require enhanced CDD measures, where needed.

## II. INFORMATION-SHARING BETWEEN FINANCIAL INSTITUTIONS WHICH ARE NOT PART OF THE SAME GROUP

**[Section to be added]**

# INFORMATION-SHARING IN THE CONTEXT OF SUSPICIOUS ACCOUNTS AND TRANSACTIONS

Though not required under *FATF Recommendations,* some countries under their own domestic legal framework specifically allow sharing of suspicious transaction information (not necessarily of the STR itself) between financial institutions which are not part of the same financial group, for example under specific safe-harbour provisions or through specific forums or gateways which have been established to enable such information to be shared (See Annex-1, highlighting some such instances). Such sharing may include information on current or prospective customers, representatives and/or beneficial owners associated with two or more financial institutions (including information on individuals, entities and organisations, suspected of ML/TF activities). Sharing of this information allows financial institutions to leverage on the AML/CFT efforts of one another, for better compliance and risk management.

Such sharing of information across financial institutions helps to gather additional information on customers or transactions presenting a higher risk or potentially related to money laundering or terrorist financing, including previously unknown accounts, activities, and/or associated entities or individuals. This also assists in building a more comprehensive and accurate picture of a customers’ activities, especially in case of complex transactions and funds flow that span across a number of financial institutions, entities and jurisdictions. The ultimate objective is to ensure better decision-making in due diligence, transaction monitoring and reporting by financial institutions.

Information-sharing in this context, where allowed, should be subject to sufficient safeguards and well laid out processes to protect the confidentiality of information and to ensure that it is used only for AML/CFT purposes. These purposes may include, for example, identifying and, where appropriate, reporting by the financial institutions on activities that may involve money laundering or terrorist financing, determining whether to establish or maintain an account or business relationship or to engage in a transaction; and assisting in compliance with AML/CFT obligations.

# CONCLUSIONS

Information-sharing is not an end in itself. It is a means to an end. An effective system of national coordination and cooperation and international cooperation hinges on how well different stakeholders, both in the public and private sector interact and engage with one another and exchange information, intelligence and analysis. With the rapidly evolving threat and risk scenario, especially regarding terrorism financing, it is vital that appropriate solutions to barriers to information are devised by national authorities and also the private sector in a coherent manner. These measures may involve authorities (for example, AML/CFT authorities and data protection and privacy authorities) engaging with one other, wherever appropriate to arrive at a shared ground. Clarity on data protection and other issues may help facilitate an efficient application of obligations.

AML/CFT and data protection and privacy, are both significant public interests. National legal regimes should facilitate both, so as to prevent money laundering, terrorist and proliferation financing, and other financial crimes in a way that pays sufficient regard to individuals’ rights to privacy, while providing a legally certain regime for financial institutions which ensures that AML/CFT and data protection laws do not cut across one another.

The private sector is an important partner in combatting ML/TF and holds valuable information which is of critical importance to law enforcement and other competent authorities. Effective and timely exchange of such information helps law enforcement in pursuing its objectives. Furthermore, it is a two-way relationship between the public and the private sector and this can be achieved if there are appropriate mechanisms for sharing of strategic, operational, tactical and targeted information by law enforcement with the private sector as well. Building of networks, an environment of trust and ongoing dialogue between authorities and the private sector may help achieve a positive outcome in this regard.

It also true that the ‘one-size-fits-all approach’ may not be appropriate in every circumstance. Countries and financial institutions may consider whether information flow will be more helpful if it happens in a centralised environment (where information is accumulated from different sources, filtered for quality and consistency considerations and then shared externally) or if a decentralised process (where each unit, branch or subsidiary has a responsibility to share information with the public sector) would be more timely and effective. This may depend upon the structure of financial institutions, their numbers and tools and techniques used to share information. In every case, financial institution should fulfil the host country reporting requirements and should periodically assess if the system implemented is adequate to a timely and effective information flow.

Finally, it is incumbent that national authorities responsible for AML/CFT and data protection recognize the important public policy goals that each seeks to advance and protect. As such, jurisdictions AML/CFT and data protection authorities should acknowledge derogations in law when necessary to prevent conflicts, and provide clear and consistent guidance to the private sector to prevent misunderstandings or conservative approaches to information sharing for AML/CFT purposes.

# ANNEX I – SELECTED EXAMPLES AND PRACTICES

This section highlights country examples on constructive engagement between AML/CFT and DPP authorities, and other practices to promote information-sharing within financial institutions, between the public and private sector and among the financial institutions. This section builds upon the information contained in Section 3 of the TF Risk Indicator Report and contains additional practices and examples provided by countries. These practices and examples relate to the following broad areas:

1. ***Interplay between AML/CFT and data protection frameworks.***

Some countries have issued guidance to financial institutions to ensure that they are able to reconcile and comply with the regulatory expectations contained in the two types of legislations. In some countries AML/CFT supervisory authorities also meet and consult with each other to better articulate their respective regulatory objectives. Such dialogue happens prior to rule making by the data protection and privacy authorities and also on an ongoing basis, with a view to provide further guidance and responses to frequently asked questions (FAQs). Creation of working groups between supervisory authorities, data protection authorities and regulators, FIUs and financial services to ensure a coordinated approach and consistent guidance on regulatory requirements may also help prevent the potential tension and conflict between the two legislations.

|  |
| --- |
| France  Each instruction, guideline or position of the French supervisory authority in the field of AML/CFT should, prior to its adoption and its publication, receive an opinion of an advisory committee called the Consultative Commission Anti-Money Laundering and Terrorism Financing (CCLCBFT) which has been set up by the board of the supervisory authority. The French Treasury Department, as well as the French Financial Intelligence Unit and other concerned authorities, including the French data protection and civil liberties’ authority (the CNIL - Commission for Data Protection and Liberties), are invited to participate to meetings of the CCLCBFT. It was especially the case when the French supervisory authority issued guidelines on exchange of information within a financial group and outside the group.  Moreover, the CNIL shall also issue opinions on the government’s draft legislation that will impact data protection or create new files in matter of ML/TF. Finally, from 2005, the French DPP authority has adopted a single authorisation (general standard) in cooperation with public authorities and private sector representatives. The single authorisation is regularly updated. The aim is to find a balance on the implementation of AML/CFT measures and the data protection requirements for a harmonised and more comprehensible framework by the concerned parties. Furthermore, this single authorisation is also a tool for simplification; nearly 1800 organisations have notified a commitment of compliance using this framework. Besides this single authorisation permits the sharing of customer data under conditions with competent French legal authorities in charge of the fight against ML/TF. |

In many cases data protection and privacy authorities are also consulted and requested to provide specific comments on AML/CFT rule-making process; in order to avoid any potential conflict and uncertainty between the two regulatory provisions. Data protection and privacy authorities are also encouraged to consult with AML/CFT authorities in the rule-making process. Such practices foster and develop an environment of collaborative partnership between the two authorities and reinforce the point that their policy goals and objectives are not necessarily mutually exclusive.

|  |
| --- |
| Canada  DPP authorities and AML/CFT authorities routinely work together prior to the drafting of relevant legislation. The *Personal Information Protection and Electronic Documents Act* (PIPEDA) is Canada’s federal private-sector privacy law. The Office of the Privacy Commissioner of Canada has posted guidance on its website, “Privacy and PCMLTFA: How to balance your customers’ privacy rights and your organisation’s anti- money laundering and anti-terrorist financing reporting requirements. There is also a set of Questions and Answers, developed with input from FINTRAC.[[10]](#footnote-10) The guidance acknowledges that the [Proceeds of Crime (Money Laundering) and Terrorist Financing Act](http://lois.justice.gc.ca/en/showdoc/cs/P-24.501/en?page=1) (PCMLTFA) requires organisations subject to the Act to undertake certain compliance activities, such as client identification and record keeping activities. In addition, certain transactions are required to be reported to the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC). It further states that the Office of the Privacy Commissioner of Canada supports efforts to combat money laundering and terrorist financing and that programme or initiatives should be implemented in a manner that is privacy sensitive and consistent with privacy laws. |

In some cases, data protection authorities are part of the AML/CFT institutional framework and are directly involved in the AML/CFT rule-making process. The close interaction and involvement of agencies helps better coordination and appreciation of different perspectives.

|  |
| --- |
| Spain  The main co-ordination mechanism for developing and co-ordinating Spain’s AML/CFT policies is the Commission for the Prevention of Money Laundering and Monetary Offences. It is comprised of over 20 key agencies, including the Spanish Data Protection Agency. One of the main functions of the Commission is issuing an opinion on draft legal provisions regulating matters related to the prevention of money laundering and terrorist financing. This high level co-ordination has permitted to adopt legislation where there are waivers of the rules laid down in the Data Protection Law. |

In certain jurisdictions, the data protection legislation provides for certain derogations and carve-outs from the obligations under the Act, which may be necessary in order to comply with obligations imposed by other legislation. This may relate to the restrictions on the right of access of the data subject, right to obtain consent, prior notification, right to be forgotten etc. These derogations are intended to address the need to strike a balance between security and privacy concerns. National authorities can consider providing more guidance in these areas, if found appropriate. In the European Union (EU) context, work on harmonising the European data protection Rules is underway.

|  |
| --- |
| European Union  In the EU context, the EU General Data Protection Regulation (GDPR) was adopted at the EU level on April 14, 2016 and will be directly applied in all EU countries. It replaces EU and national data protection legislation. This will become applicable on May 25, 2018. It is a further step towards the harmonisation of European data protection rules. The GDPR considers location data, IP addresses and online identifiers personal data in most cases; as this data could be used to identify individuals, in particular when combined with unique identifiers. The GDPR has also introduced additional transfer tools (codes of conduct and certifications) in order to facilitate exchange of information.  Italy  Domestic legislation provides clear gateways for the processing and sharing of personal data for the purposes of compliance with the AML/CFT laws and regulations. In some instances, for further clarity, national data protection authorities have issued a general order on AML measures on group-wide communications, which facilitates group-wide data sharing in financial intermediaries. The consent from the data subject is not required in such cases. |

In certain jurisdictions, financial institutions are enabled to share customer information through specific exemptions under the data protection legislation and by lifting restrictions on sharing of information for the purposes of AML/CFT. Financial institutions should carefully consider all such derogations while making a determination on their own procedures and practices with regard to sharing of information.

|  |
| --- |
| Singapore  The exchange of customer information between financial institutions is subject to Singapore’s Banking Act and Trust Companies Act, which supersede the general data protection provisions laid out in the Personal Data Protection Act (PDPA). Financial confidentiality provisions under the Banking Act and Trust Companies Acts are lifted for the combatting of money laundering and terrorist financing (e.g. for compliance with requests made by a parent supervisory authority, internal audits, or risk management purposes by head-offices). Further, the PDPA requirements are also lifted and financial institutions are also required to share information with their head offices and their branches and subsidiaries within the financial group under the MAS AML/CFT Notices, where necessary for money laundering and terrorism-financing risk management purposes. |

***Group-wide Information-sharing***

Sharing of STRs by a subsidiary or branch of a financial institution with its head office complements the group-wide risk management processes and discharge of oversight responsibilities by head office. Moreover, further sharing of STRs within the group also promotes a more effective internal control procedures and risk management. This is specifically allowed in certain jurisdictions, subject to appropriate confidentiality controls.

|  |
| --- |
| **USA**  In January 2006, FinCEN and federal banking agencies (OCC, FRB, FDIC and OTS) determined that a U.S. branch or agency of a foreign bank may share a SAR with its head office. The January 2006 Guidance also stated that a U.S. bank or savings association may share a SAR with its controlling company (whether domestic or foreign). The sharing of a SAR or, more broadly, any information that would reveal the existence of a SAR, with a head office or controlling company (including overseas) promotes compliance with the applicable requirements of the Bank Secrecy Act (main AML/CFT law) by enabling the head office or controlling company to discharge its oversight responsibilities with respect to enterprise-wide risk management, including oversight of a depository institution’s compliance with applicable laws and regulations.  Further, in November 2010, the joint guidance issued by FinCEN and federal banking agencies provided that a depository institution that has filed a SAR may share the SAR, or any information that would reveal the existence of the SAR, with an affiliate, provided the affiliate is subject to a SAR regulation. The sharing of SARs with such affiliates facilitates the identification of suspicious transactions taking place through the depository institution’s affiliates that are subject to a SAR rule.  France  Article L. 561-20 of the French monetary and financial code authorises exchange of information in this context. Furthermore, financial institutions have to fill in -on a yearly basis- an AML/CFT questionnaire including legal obstacles that they met in the area of information exchange with their branches or subsidiaries. In such situations, the foreign laws and regulations that prohibit/hinder a financial institution to implement equivalent AML/CFT measures in their branches and subsidiaries abroad must be sent by the REs to the French supervisory authority. The FIU must be also informed of these difficulties by the REs. |

1. ***Information-sharing between financial institutions not part of the same group***

Timely and spontaneous sharing of relevant information by financial institutions more generally among one another with sufficient safe harbour provisions and protection from legal repercussions may help fight ML/TF more effectively, reinforce the integrity of the financial system and prevent its abuse by criminals. It also has the ability to provide better and more comprehensive intelligence to law enforcement authorities. In some jurisdictions, there are specific legislative enablers and safe harbour provisions to facilitate such sharing of information among the financial institutions which are part of the framework.

|  |
| --- |
| USA  Section 314(b) of the USA PATRIOT ACT (Information-sharing Between Financial Institutions) provides that two or more financial institutions and any association of financial institutions may share information with one another regarding individuals, entities, organisations, and countries suspected of possible terrorist or money laundering activities. A financial institution or association that transmits, receives, or shares such information for the purposes of identifying and reporting activities that may involve terrorist acts or money laundering activities shall not be liable to any person under any law or regulation of the US, any constitution, law, or regulation of any State or political subdivision thereof, or under any contract or other legally enforceable agreement (including any arbitration agreement), for such disclosure or for any failure to provide notice of such disclosure to the person who is the subject of such disclosure, or any other person identified in the disclosure. |

In some countries, exchange of information between two financial institutions which do not belong to the same financial group is permitted if some criteria are met.

|  |
| --- |
| France and Romania  In France, exchange of information between two financial institutions which do not belong to the same financial group is permitted if some criteria are met (Art. L. 561-21 of the financial and monetary code). Among these conditions, financial institutions are required to ensure that their counterpart applies AML/CFT measures consistent with the French requirements implementing the *FATF Recommendations.*  In Romania, Article 25 (4) of the AML/CFT Romanian Law permits financial institutions to exchange information with another financial institution. In particular, paragraph (b) permits credit and financial institutions to exchange information subject to secrecy when they (1) are within the same group, (2) are situated in the EU, the EEA or a third state which imposes similar AML/CFT requirements (3) apply CDD and record-keeping measures which are equivalent to those under the AML/CFT Law and (3) are subject to AML/CFT supervision. Credit and financial institutions may also exchange information subject to secrecy, even when they are not within the same financial group, if (1) they are situated in the EU, the EEA or a third state which imposes similar AML/CFT requirements (2) the information relates to the same client and transaction (3) they are within the same business category (4) are subject to similar secrecy and protection of data requirements. |

In some countries, specific bilateral arrangements to facilitate information-sharing among financial institutions for AML/CFT purposes have been reached between jurisdictions. This highlights the importance of mitigating specific national/regional ML/TF risks through the mechanism of bilateral or multilateral arrangements.

|  |
| --- |
| USA and Mexico  Ongoing efforts have taken place between the U.S. and Mexico to jointly increase financial transparency and to prevent ML/TF in the context of correspondent banking.  As part of on-going monitoring requirements, US banks are required to monitor all transactions when they are an intermediary financial institution and file STRs as appropriate. US banks regularly send Requests for Information (RFIs) to respondent institutions to request additional information related to an unusual transaction. This is intended to clear alerts rather than file STRs. Due to the Mexican bank secrecy provisions and Data Privacy Law, Mexican banks could not respond, which could result in more STRs and termination of respondent accounts. Mexican banks inability to respond to U.S. banks’ RFI may result in U.S bank filing of STRs and potentially terminating the correspondent account. In order to address this, in December 2014 the Mexican AML/CFT General Provisions applicable to banks were amended to allow, for the first time, the possibility of Mexican banks sharing information with foreign banks, for AML and CFT purposes.  Specifically, the Mexican government amended its AML/CFT General Provisions applicable to banks and has set in place a legal mechanism by which Mexican banks can share information of their clients and occasional customers, as well as of their transactions with foreign banks, exclusively for AML/CFT purposes. Pursuant to the Mexican Credit Institutions Law, banks shall treat their clients’ and occasional customers’ information as confidential. Banks are therefore forbidden from divulging the transactional history, or personal data of their clients’ or occasional customers’ to anyone but the account holders, beneficiaries, trustees, creditors or legal representatives. As an exception, banks shall provide said information if requested by: (i) a Judge through a subpoena; (ii) the Attorney General’s office; (iii) the Military Attorney General’s office; (iv) the Ministry of Finance authorities for AML/CFT or tax purposes, or (v) the federal oversight authority. Likewise, banks may share the relevant information with other banks for AML/CFT purposes, regarding their clients' and occasional customers' information, as well as of their transactions.  Prior to starting the sharing such information, the Mexican Ministry of Finance has to approve the foreign banks. Likewise, before Mexican and foreign banks begin to exchange information, they have to convene in writing the confidentiality of the information, as well as to state the information and positions of the individual officers authorised to conduct the exchange. Such agreement has to be filed before the National Banking and Securities Commission.  U.S. and Mexican authorities and banks jointly developed the questionnaire currently used as a template for the information-sharing mechanism. In this regard, before or at the time of sharing information, Mexican banks shall provide the authorities copy of the information shared and relevant data thereof.  With this mechanism, Mexican banks can now share information with non US banks as well, subject to the same protocols. |

There is a case for exploring how private sector entities could share specific threat information and high risk customer information with one another. In some jurisdictions databases to share STRs and related information have been created to facilitate information-sharing among obliged entities, as well as administrative and law enforcement authorities. This facilitates better information-sharing, as well as intelligence to assist in decision-making by authorities and the private sector, wherever relevant.

|  |
| --- |
| Spain  Article 33 of the Law on the prevention ML/TF permits obliged persons to exchange information relating to the transactions reported to the FIU with the sole purpose of preventing or forestalling transactions related to ML/TF when the characteristics or pattern of the specific case suggest the possibility that, following its rejection, a transaction wholly or partially similar to the latter may be attempted with other obliged persons. To that end, central data bases can be created to share this information. Obliged persons and the judicial, law enforcement and administrative authorities competent for the prevention or suppression of ML/TF may consult the information contained in the files created. Regarding the obliged entities, access to the data shall be limited to the internal compliance units established by obliged persons.  Romania  The annual report of the Romanian FIU is a strategic analysis product and primarily aims to provide relevant feedback to reporting entities. It shows the FIU’s perspective considering its position as collector of information from the entire financial and non-financial system. The material provides a description of the main categories of suspicious financial behavior, based on the information from STRs submitted. Through its partnership with the reporting entities, the FIU seeks to support their need to know: What they should report? What the other entities are reporting from their field? The feedback increases the trust and helps reporting entities regulate the suspicious behavior detection systems. In addition, the reports are relevant to the common effort of the LEAs. |

1. ***Information-sharing between financial institutions and authorities***

A close relationship between the private and public sector is a critical element of a well-functioning AML/CFT system. The FATF Standards require countries to develop strong legal and operational frameworks to inform the private sector of ML/TF risks and to ensure that the private sector takes ML/TF risks into account in the course of its business. In the TF context, in particular, this may require combining information obtained from reporting entities with contextual and sanitised information from authorities.

|  |
| --- |
| Russia  Under the provisions of the Federal law on AML/CFT, a system of cooperation between FIU- Rosfinmonitoring, supervisory body- the Bank of Russia and REs is provided for in cases where there has been a denial in conducting transactions, opening an account or a contract has been terminated. In all such cases REs have to report to the FIU, where information is analysed and then transferred to the Bank of Russia in order to be communicated to the credit institutions and non-credit financial institutions via secured channels. The information received by REs is to be taken into account by them in conducting risk assessment of their clients thus facilitating determination of relevant level of risk and elaboration of corresponding commensurate risk mitigation measures. |

1. ***Public/Private Partnerships***

The private sector holds a wealth of data, which can be utilised by the law enforcement for investigative purposes. In some countries, a public-private partnership has been created to foster information exchange between the public and private sector and among financial institutions which are part of that partnership. The objective of such formal or informal platforms is to provide a conducive environment for feedback and guidance between public and private sectors, as well as to share operational intelligence, information on risks and prevent, detect and disrupt possible threats. This document only sets out the models used in some countries to establish partnerships or forums for cooperation. The practical use of such partnerships and other fora for operational information-sharing will be set out in more detail in other FATF guidance and best practices documents.

|  |
| --- |
| Switzerland  Switzerland has different mechanisms or platforms to mutually exchange information with the private sector. In 2010, in the context of the revision of the FATF Standards, the Swiss authorities established a working group with the private sector bodies (ISFIN) to ensure mutual exchange of information in relation to the development of the regulatory framework in the field of AML/CFT. More recently, in the broader context of the interdepartmental coordinating group on combatting ML and FT established in 2013 – that is also responsible for the NRA – an additional contact group with the private sector has been set up. This group encompasses experienced selected AML/CFT experts in different sectors subject to AML/CFT legislation, such as banks, insurances and MVTS. It is established as a permanent platform to exchange views on the evolution, understanding and mitigation of existing and emerging ML/FT risks. It has already identified areas of future work between the public and the private sectors, such as typologies of TF and correspondent banking. This group helps enhance the communication with the private sector and awareness-raising on AML/CFT matters.  ***Hong Kong, China***  The Fraud and Money Laundering Intelligence Taskforce is a public-private intelligence sharing mechanism involving the Hong Kong Police, the Hong Kong Monetary Authority and the banking industry with the aim of improving the detection, prevention and disruption of fraud, money laundering and other types of financial crimes relevant to Hong Kong’s economy.  Launched in May 2017 under a 12-month pilot project, the taskforce builds on existing levels of informal cooperation and sharing; preparatory meetings have taken place through 2016 to provide a formal structure for banks and competent authorities to improve collective understanding of threats to enhance targeting and intervention activity for law enforcement and better risk management for banks.  The taskforce operates at both strategic and operations levels with threat-specific information alerts disseminated to the wider financial sector through a secure platform. |

These partnerships acknowledge the importance of involving the private sector, not only as a source of information, but also as a recipient for sensitive information and intelligence held by the public sector to better detect potential terrorist financing. Such sharing often happens in a secured environment after proper clearances are obtained, in order to facilitate further data-mining, operational analysis and scanning by the private sector to fill potential intelligence gaps. The engagement must be an ongoing process and not just transactional and driven by particular events, as the private sector should also have an accurate understanding of the constantly changing risk environment to complement the efforts of law enforcement.

|  |
| --- |
| Canada  **Promoting TF-vigilance and STR Reporting by REs**: Immediately after the attacks in Ottawa & Quebec, FINTRAC issued an advisory to REs to highlight the importance of filing STRs that may relate to similar types of TF threats. STR filings increased by 22% in the month of the Ottawa attacks (over 8,700 in October 2014). In addition to issuing reminders following other ISIL related attacks, FINTRAC has also developed and shared relevant TF indicators with REs.  **Developing a real partnership with REs and sharing Operational Alerts and Briefs:** Over the last few years,FINTRAC has worked closely with major financial institutions in fight against ML/TF. FINTRAC has developed a new line of products which include “Operational Alerts”. Its purpose is to provide up-to-date indicators of suspicious financial transactions and high risk factors related to specific methods of ML/TF that are important either because they represent new methods, re-emerging methods or long-standing methods that present a particular challenge. This is intended to operationally support REs in identifying, assessing and mitigating related risks, as well as the reporting of related suspicions to FINTRAC. FINTRAC also developed “Operational Briefs” to provide clarification and guidance on issues that impact the ability of REs to maintain a strong regime of compliance with the Canadian legislation. More specifically, these products are focused on risk and vulnerabilities associated with exploitation for ML/TF, and on meeting STR obligations. FINTRAC is also currently developing a suite of TF-relevant “Operational Alerts” to provide Canadian REs with important contextual knowledge on TF, and attempt to provide indicators/red flags that REs can operationalise and use in their in house transaction monitoring and internal investigative processes, and ultimately increase the volume and quality of TF-related financial intelligence from REs. |

The private sector is often looking for assistance and more detailed contextual information from the public sector to help interpret the data they already have. This could include, for example, sharing a list of relevant individuals (i.e. people under monitoring, surveillance or investigation) suspicious behaviour. Such list-based approaches may help in identifying specific transactions and to detect the network or associations of subjects related to those listed. However, sharing lists of subjects is a sensitive issue as preserving the confidentiality of on-going investigations and operations is a priority for law enforcement authorities. This also has the potential to flag such customers as high risk and may lead to suspension or termination of business relationships, without due process of law or consideration, leading to legal challenges. Even if it is not possible to divulge the particular facts of a case, a general indication of the type of activity occurring can assist them to provide actionable financial intelligence. The sharing of indicators provides reporting entities with the ability to better detect suspicious activity and provide more effective STRs to the FIU.

The private sector maintain certain non-financial data about a customer for CDD purposes such as Internet Protocol (IP) addresses, mobile phone numbers, email and residential address and real-time geolocation data for online banking users. In combination with information from competent authorities, such information can become useful for law enforcement for detection and investigation purposes.

1. ***Information-sharing in the context of suspicious accounts and transactions***

Specific safe harbours provisions or specific forums and gateways can allow the sharing of suspicious transaction information, without necessarily the full content of the STR itself. Under strict provisions to protect the confidentiality of the information, those specific gateways can allow better information sharing not only between financial institutions that don’t belong to the same group, but also in an inter-agency context. Such specific gateways aim at an effective and timely exchange of such information and helps law enforcement in pursuing its objectives of countering money laundering and terrorist financing.

|  |
| --- |
| EU-OF2Cen  EU-OF2Cen initiative is an EU-funded Italian project on internet fraud that now is rolled out at EU level. Its aims to enable the systematic, EU-wide sharing of internet fraud related information between banks and law enforcement services for the prevention of payments to fraudsters and money mules and for the investigation and prosecution of the perpetrators involved. The project is co-funded by the European Commission and supported by several key stakeholders from the banking sector and law enforcement. |

Collaborating and sharing information, experiences and trends on risk indicators, for example the ones associated with TF, FTFs and small terrorist cells and raising awareness in a proactive manner by authorities helps build the capacity of the private sector. Meaningful results have been achieved through these successful public partnerships at FATF and Egmont group (for example, the recent TF Risk indicator report finalised by FATF, EGMONT bulletin regarding FTFs etc.)

|  |
| --- |
| USA  FinCEN’s regulations under Section 314(a) of the USA PATRIOT Act enable FinCEN to reach out to more than 43,000 points of contact at more than 22,000 financial institutions to locate accounts and transactions of persons that may be involved in terrorism or money laundering. FinCEN makes these requests for its own analytical and investigative purposes and on behalf of federal, state, local, and certain foreign (e.g. European Union) law enforcement agencies. Section 314(a) provides lead information only (financial intelligence) and is not a substitute for a subpoena or other legal process, which is typically used following the identification of relevant information to obtain the information for further investigative or evidentiary purposes.  Through an expedited communication system, FinCEN’s 314(a) process enables an investigator to provide sensitive investigative lead information directly to reporting entities. FinCEN provides a secure e-mail system to disseminate this sensitive information. Based upon the initial information that the financial institutions provide, the investigative focus quickly zeros in on relevant locations and activities. In addition FinCEN will organise and host information-sharing discussions with appropriate financial institutions to issue requests for information pursuant to Section 314(a). This cooperative partnership between the financial community and law enforcement allows disparate bits of information to be identified, centralised and rapidly evaluated.  Furthermore, the Domestic Security Alliance Council, or DSAC, is a security and intelligence-sharing initiative between the FBI, the Department of Homeland Security, and the private sector, including the largest US banks. Created in 2005, DSAC enables an effective two-way flow of vetted information between the FBI and participating members.  European Bankers Alliance initiative  The European Bankers Alliance initiative was launched in 2015, involving leading international financial institutions operating in the EU and Europol. It aims to help financial institutions develop jointly with law enforcement 'red flag' indicators related to human trafficking, to scan their systems for suspicious transactions and then alert the police. |

Terrorism and TF information, by its nature, is highly sensitive and needs protection. A lack of trust between competent authorities and the private sector may inhibit sharing sensitive data. The public sector has the difficult task of balancing the confidentiality of sensitive operational information and creating awareness of TF risks with stakeholders. This highlights the importance of building a close relationship based on mutual trust and confidence. Strong formal and informal relationships with the private sector can assist in breaking down some of the barriers/delays in accessing information. In certain jurisdictions for example, often individual contacts are maintained by authorities with the money laundering officers of the financial institutions via whom information can be obtained.

|  |
| --- |
| UK  The Joint Money Laundering Intelligence Taskforce is a shared endeavour between financial institutions, industry regulators, Government and law enforcement operating in the UK. It was established in February 2015 and is now a permanent part of the UK’s response to money laundering and terrorist financing. Its purpose is to provide an environment for the financial sector and government to exchange and analyse intelligence to detect, prevent and disrupt money laundering and wider economic crime threats against the UK. Its work includes strategic information-sharing on common money laundering and terrorist financing methodologies, risks and typologies which are developed and shared with the wider financial sector through targeted alerts. It also has a tactical information-sharing function which seeks to fill intelligence gaps where suspected laundering crossed multiple financial institutions. This tactical information-sharing function is delivered through a co-located operations group, where vetted members of financial institutions meet with law enforcement officers every week to progress enquiries of mutual interest. This work is underpinned by clear legal framework (provisions of section 7 of the Crime and Courts Act) and formal Information-sharing Agreement. Enquiries progressed through this co-located operations group have resulted in arrests, the recovery of criminal funds, changes to banks internal systems and controls and new bank led investigations. |

1. ***Guidance and Feedback***

It is also important to provide the private sector with guidance and feedback, including to clarify regulatory expectations regarding the implementation of AML/CFT requirements, or to provide feedback on their reporting. For the private sector, this reinforces the need to commit substantial resources to compliance and engagement with law enforcement. Information shared on the emerging trends, patterns of behaviour and threats is vital for the private sector in order to enable them to run or modify their transaction monitoring systems, keeping in view the evolving situation and also to sensitise their frontline staffs who have a direct day to day relationship with customers.

Authorities may also discuss and share the types of information and intelligence that are of value to the private sector in identifying suspicious activity. While sanitised case studies and typologies on money laundering and terrorist financing can often be produced by the FIU in the form of an annual report, newsletter or e-bulletin, more detailed versions of case studies or analysis of past pattern can be shared with specific entities though appropriate channels, such as the forums and partnerships noted above. Another useful mechanism used to disseminate case studies and typologies are National Risk Assessments. These assessments are useful in engaging with the private sector at an early stage and in increasing the awareness of specific risks.

Information about particular countries which may pose a greater risk of terrorist financing or certain business that may pose a heightened security risk can also be shared by authorities with the private sector. In some cases, authorities may provide detailed data analysis on geographical areas concerning borders, logistical or transit areas. In other cases, financial information seized by law enforcement (e.g. bills of lading, receipts, etc.) may be shared with financial institutions, which may then use it to check against records in their own system to identify any relevant suspicious transactions.

|  |
| --- |
| France  The French FIU gives feedback to all entities which submit STRs. This opportunity to provide feedback is administered both generally and specifically. General feedback and guidance is provided through conferences, annual reports, participation in the AML Group of the Bankers’ or Insurance’s Association and compliance meetings with financial institutions. Specific feedback and guidance is given through informal contact with staff in companies, through offering acknowledgement of the receipt of reporting and offering review of reported cases. Furthermore, since the 3rd of June 2016, to organise the sending of information from financial institutions with the aim of reinforcing the fight against TF, the FIU has the power to designate natural or legal persons that might present higher ML/TF risks, which implies that financial institutions shall put in place enhanced CDD measures and special monitoring on these designated transactions or individuals.  Russia  General cooperation with the private sector participants, including for the purposes of improving quality of information-sharing with competent authorities and feedback, is conducted regularly through established under the Interagency Commission on AML/CFT Consultative Council where largest financial institutions associations are represented and through established as a working body of the abovementioned Interagency Commission Compliance Council representing particular entities carrying out operations with money and other assets. |

Guidance, feedback and outreach provide REs with meaningful or “targeted” information with the explicit purpose of helping the private sector provide better suspicious activity reporting. This cycle (or “feedback loop”) ultimately leads to even better outreach by the competent authorities to the reporting institutions that further enhance reporting standards. This may also help the private sector needs to build typologies across a number of parameters. This can be carried out keeping in view the sensitivity of the information and the kind of input solicited from the private sector.

|  |
| --- |
| China  The People’s Bank of China summarised main features of suspicious transactions related to TF, developed TF suspicious transaction monitoring model, and shared this model with key financial institutions and financial institutions in key regions. Use of this model leads to a significant increase of the number of TF related STR reported by financial institutions. A commercial bank successfully screened transactions of one individual related to ISIL. At present, the PBC is making continuous optimisation and adjustment of the model based on practice.  Australia  Regular meetings with relevant private sector institutions– e.g. AUSTRAC engages with private industry through quarterly forums with major reporters and efforts to share information about behaviour patterns. |

Providing feedback on the quality of reporting is vital to ensure that financial institutions develop a sense of ownership and are able to update their systems and procedures. This also facilitates a clear articulation of the supervisory expectations and a better response from the financial institutions to meet those objectives. Guidance, especially when shared with a wider audience is also helpful in developing a good industry practice across the sector.

|  |
| --- |
| France  Many FIUs and sector regulators provide such feedback on a regular basis, with a view to improve the quality and quantum of reporting being made by the financial institutions. For example, France provides feedback during bilateral meetings with reporting entities on an annual basis and provides general feedback during industry forums.  Turkey  In Turkey, MASAK regularly meets with compliance officers of the banks in relation to AML/CFT matters which also include terrorist financing risks. In those meetings, compliance officers of banks are informed of the latest developments and the parties exchange ideas with each other.  Australia  Australia provides guidance and feedback on STRs to a number of key stakeholders on a periodic basis. Each quarter the FIU and law enforcement will meet with the four largest banks to discuss compliance issues and provide feedback on STRs. These meetings have resulted in a 300% increase in STRs relating to TF, following targeted outreach on TF risk indicators.  Hong Kong, China  The Joint Financial Intelligence Unit (JFIU) and the Hong Kong Monetary Authority (HKMA) have worked together to increase both the quality and quantity of STRs in the territory. A guidance paper was issued in December 2013 by the HKMA and JFIU providing feedback from thematic examinations (such as specific guidance on quality and consistency of reports) and specific industry training was jointly provided in 2014. Immediately following this work STR volume increased by 14% from 27,328 in 2013 to 31,095 in 2014. In parallel JFIU provides sector wide feedback in annual AML training for all sectors and individually on a needs basis while the HKMA continues to include reviews of STRs made by banks in its on-site work with a focus on quality. General feedback and guidance to private sectors is also provided by JFIU and HKMA, for example through STR quarterly reports promulgated in JFIU’s website, conferences and AML/CFT seminars.  Specific feedback and guidance is also given through informal contact or ad-hoc meetings with the reporting entities offering views of the reported cases. |

Feedback from the private sector on drafts of risk profiles and risk indicators may be helpful in order to refine the final product; before they are issued by the authorities as a formal guidance. Some countries have developed a TF platform for this purpose as well as for providing feedback on STRs and share new trends and methods.

|  |
| --- |
| The Netherlands  In the TF context, the Netherlands authorities test TF indicators with the private sector to assess their feasibility and usefulness. Draft risk profiles are refined based on the preliminary results provided by reporting entities. Once finalised, risk profiles are disseminated by the competent authority to the reporting entities in the form of guidance. In this case, the continuing guidance and feedback enhances the effectiveness of the development of TF indicators. |

Information regarding real time incidents needs to be more detailed and specific to enable the private sector to take immediate action. Data held by the private sector can also assist authorities to identify specific threats and to provide real-time information during or after a terrorist incident, for example. However, concrete information relating to specific individuals and events are often subject to restrictions. Practical challenges exist with respect to ongoing or active terrorism or terrorist financing investigations. In some cases, authorities and private sector entities are therefore not able to act in good faith because of legal restrictions, privacy protection or liability issues. Establishing exceptions or protocols should be considered to allow authorities to share information with the private sector, as needed on an urgent basis, when there is a real-life incident unfolding or where there is actual, or potential for, loss of life.

Some countries have developed a separate online portal and other tools for making requests for information from the private sector and for sharing of information in a secured and efficient manner. This ensures that such requests are prioritised and are addressed in a timely manner, especially in matters involving terrorism or terrorist financing, where the objective is to prevent such attacks.

|  |
| --- |
| China and Turkey  Online portals for making requests and receiving reports from the private sector and for providing information to the private sector are being used in certain countries (e.g. China - Digital Information Inquiring System) between the public security and the banking sector. In Turkey, MASAK requests the financial data in banks electronically through red network established with each bank and the data imported electronically via red network. The security of data is ensured through adequate safety protocols and authentications. |

***Sector-specific engagement, outreach and guidance***

Some countries have developed specific engagement programmes with sectors that appear vulnerable to threats, including TF threats. Such sectors may or may not be within the regulated community, but may be important in view of the emerging pattern and analysis. Local authorities and other stakeholders in vulnerable terrorist areas, including the NPO sector may also be involved to collaborate and identify preventive and other measures to address these threats.

|  |
| --- |
| France and Switzerland:  Reaching out to vulnerable sectors is an important strategy of many jurisdictions in the fight against terrorism and TF. For example, Ministry of Finance (MoF), France communicates with art and antiquities dealers in order to draw their attention to the specific TF risks related to their field of business, especially with regard to ISIS’s ongoing financing activities. The MoF has published a guide for NGOs, which invites financial institutions to undertake concrete measures to sensitise their customers to these specific risks (antiques, oil trade with Iraq). Similarly, following the publication of the NRA in Switzerland, the Swiss authorities initiated a dialogue with the art trade sector to discuss the AML/CFT measures applied by this sector. Separate meetings were held with the sector to raise awareness. This included, representatives of a major international auction house involved in the business.  Canada  Outreach to the charitable sector is conducted to advise charities of their legislative obligations and how to protect themselves from terrorist abuse. This includes general guidance on topics related to sound internal governance, accountability procedures and transparent reporting, as well as specific tools such as a checklist on avoiding terrorism abuse and a web page on operating in the international context. Outreach can take on a variety of forms, including a web presence/RSS feed, email distribution lists, webinars and face-to-face meetings. |

1. ***Mechanisms of Information-sharing***

Two-way relationships between the private and public sector are necessary to combat ML/TF. Mechanisms for information-sharing can include formal meetings and informal briefings, both at the one-on-one level and with multiple entities. Many countries hold at least a yearly forum or seminar with the private sector to discuss emerging threats, risks and trends. Operational entities such as law enforcement or security agencies are often included to provide practical case examples or specific information on risk. In other cases, discussions on MLTF risks take place as part of the conferences, seminars, and training for reporting entities. Additionally, this outreach may also occur at the initiative of the private sector to enable more expansive discussion of the potential criminal activity.

There may also be a case for a having a mechanism or process within a jurisdiction for the private sector to report potential TF transactions or at least those that appear to indicate that a terrorist act may be imminent to law enforcement/security services in near real time. This presupposes that the competent authority has the channel to receive this type of information and can act accordingly. Examples include dedicated telephone “hotlines or a legal obligation on financial institutions to report such cases on an immediate basis rather than within the time-frame of a STR filing obligations.

In some cases, specific TF working groups or task forces have been established between the public and private sector. These types of task forces provide a forum for operational collaboration which is instrumental in improving the analysis and investigation functions of all parties involved.

|  |
| --- |
| Egypt  The Federation of Egyptian Banks (FEB), established as a non-profit independent entity, connects all Egyptian banks and foreign banks working in Egypt. The objectives are to discuss and share common issues between the members of the federation; this is in addition to giving opinions of draft laws and suggesting amendments of current legislation related to the banking sector.  In 2003 a Compliance Officer Association was created as an initiative of the FEB. All compliance officers of the banks operating in Egypt are members in this association. Regular meetings are held on issues regarding combatting ML/TF. The Central Bank and FIU are always invited to attend these meetings to provide feedback and technical assistance on the issues raised by the compliance officers. |

1. In the EU context, personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; (Article 4(1) of the General Data Protection Regulation) [↑](#footnote-ref-1)
2. [www.fatf-gafi.org/publications/fatfrecommendations/documents/consolidated-fatf-standard-information-sharing.html](http://www.fatf-gafi.org/publications/fatfrecommendations/documents/consolidated-fatf-standard-information-sharing.html) [↑](#footnote-ref-2)
3. BCBS Core Principles for Effective Banking Supervision, September 2012: [www.bis.org/publ/bcbs230.pdf](http://www.bis.org/publ/bcbs230.pdf) [↑](#footnote-ref-3)
4. Interpretive Note to Recommendation 18, paragraph 4 [↑](#footnote-ref-4)
5. Interpretive Note to Recommendation 18, paragraph 4 [↑](#footnote-ref-5)
6. INR 18.5 [↑](#footnote-ref-6)
7. See: [www.bis.org/bcbs/publ/d353.pdf](http://www.bis.org/bcbs/publ/d353.pdf) [↑](#footnote-ref-7)
8. “Regardless of its location, each office should establish and maintain effective monitoring policies and procedures that are appropriate to the risks present in the jurisdiction and in the bank. This local monitoring should be complemented by a robust process of information-sharing with the head office.” (Paragraph 72) [↑](#footnote-ref-8)
9. The Egmont group of FIUs issued a ‘*white paper on enterprise-wide STR sharing: issues and approaches’* in February 2011*.* It sets out key issues for a cross border STR sharing regime and also presents possible approaches to facilitate enterprise STR sharing. The paper concludes that the cross-border element of enterprise-wide STR sharing necessitates that jurisdictions coordinate their actions in this field. [↑](#footnote-ref-9)
10. See [www.priv.gc.ca/faqs/index\_e.asp#q021](https://www.priv.gc.ca/faqs/index_e.asp#q021) [↑](#footnote-ref-10)