FATF

FATF GUIDANCE

PRIVATE SECTOR INFORMATION SHARING

NOVEMBER 2017

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit **www.fatf-gafi.org**

This document and/or any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

Citing reference:

FATF (2017), *Guidance on private sector information sharing,* FATF, Paris
www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-information-sharing.html

CONTENTS

INTRODUCTION

BACKGROUND AND CONTEXT

1. 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. Financial institutions should not be unduly prevented from sharing information for the purpose of ML/TF risk management.

2. 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 financial institutions operating through various structures.

3. 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 effectiveness of the domestic co-ordination and co-operation regime.

4. 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 effectiveness of AML/CFT efforts and conversely, inadvertently facilitate operations of such criminal 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.

5. Sharing information is key to promoting financial transparency and protecting the integrity of the financial system by providing financial institutions, and relevant competent authorities the intelligence, analysis and data necessary to prevent and combat ML/TF. Similarly, financial institutions look to 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. Public and private sector institutions can be source as well as target of information flow. 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.

6. In June 2016, FATF issued Consolidated Standards on Information sharing[1] 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.

[1] Consolidated FATF Standards on Information Sharing.

PURPOSE OF THIS GUIDANCE, TARGET AUDIENCE, CONTENT AND THE STATUS OF THIS GUIDANCE

7. The purpose of this Guidance is to:

i. Highlight the usefulness of information sharing among entities of the private sector (particularly financial institutions) to increase the effectiveness of their ML/TF prevention efforts.

ii. Identify key challenges that inhibit sharing of information group-wide and between financial institutions not part of the same group;

iii. Clarify 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;

iv. Highlight country examples of collaboration between data protection and privacy and AML/CFT authorities to serve mutually inclusive objectives;

v. 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;

vi. Support the effective implementation of the AML/CFT regime, through sharing of information, both in the national and international context.

8. The target audiences of this Guidance are:

i. Countries and their national competent authorities with responsibility for AML/CFT;

ii. Practitioners in the private sector, including financial institutions that have group-wide AML/CFT programme obligations to fulfil or that process customer transactions with other institutions; and

iii. National and supra-national data protection and privacy (DPP) authorities.

9. The paper sets out the challenges to information sharing and provides guidance both in the context of group wide and between financial institutions not part of the same group. Annex-1 articulates how differences in DPP regimes or their application can affect the information flow. Annex-2 includes country examples and approaches on addressing some of these challenges, including of national DPP and AML authorities working together to meet their respective objective. It also sets out innovative practices adopted by countries to promote group-wide information sharing and between financial institutions which are not part of the same group. The section further 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. It should be noted that these examples are presented for information only. These examples are illustrative in nature and not to be construed as FATF recommended approaches. These examples are also cross-referred with respective sections of the guidance. When considering the general principles outlined in the Guidance, national authorities will have to take into consideration their national context, including the legal framework. This Guidance is non-binding and it draws on the experiences of countries and of the private sector and may assist competent authorities and financial institutions to effectively implement some of the Recommendations.

GENERAL INFORMATION SHARING ISSUES

10. Information sharing plays a vital role in allowing financial institutions and supervisory and law enforcement authorities to better deploy resources on a risk based approach, and develop innovative techniques to combat ML/TF. The size and geographical scope of the international financial system makes it imperative to improve coordination and collaboration between all the stakeholders if the measures to identify and prevent ML/TF are to succeed. Enabling greater information sharing is a key element of collaboration whether it involves sharing across borders, between entities of the same financial group, between different financial groups or between private and public sector or vice versa.

11. Improvements in information sharing are also critical to enabling the full exploitation of the potential improvements to AML/CFT safeguards, and access to financial services, promised by new technologies and evolving business models. However, there remain obstacles to effective information sharing which can obstruct this progress and create legal and regulatory uncertainty. Challenges which have been identified are discussed below:

A. Legal Issues

12. Legal constraints 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 some instances, regulated entities are uncertain as to the sharing permitted under these legal regimes, and this clear lack of understanding inhibits effective information sharing. Countries should therefore overcome the challenges and implement an effective information sharing regime concerning application of different legal provisions in this context by providing appropriate clarifying guidance of their laws and regulations to eliminate ambiguity regarding sharing.

13. In particular, these challenges may emerge due to following concerns:

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

14. 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[2]. 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 balances an individual's rights to protection of personal data and privacy. AML/CFT and DPP public policy goals are not mutually exclusive and should recognise support and be balanced.

15. Differences in DPP laws across jurisdictions may create implementation challenges, particularly for the private sector in sharing information. The issue may be further compounded if there is a lack of regulatory guidance, or an inconsistent approach towards AML/CFT requirements and DPP obligations. The perceived conflict between AML/CFT and DPP objectives may be due to lack of adequate coordination between different authorities at the rule making stage, leading to lack

[2] Personal data could mean any information relating to a natural person who can be identified, directly or indirectly, 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.

of the proper balance between data protection on one hand and prevention or combating of crimes on the other hand. The apparent complexity of different DPP approaches and the fear of penalties and risk avoidance have a significant impact on availability, access, processing or sharing of information by the private sector, even when such sharing is permitted.

16. While there are some situations where DP authorities try to provide support to public authorities and private stakeholders, there are many cases where, more clarity from national regulators and public authorities on how to effectively manage differing regulatory requirements may be helpful in this regard. For example, global financial institutions operating in multiple jurisdictions would benefit from data protection authorities issuing clarifying interpretation and guidance on the extent to which sharing personal data across borders for AML/CFT purposes is permissible under the public interest or other derogation(s) contained in different data protection regulations on data transfers (*e.g.* the extent to which transfers of data made for the purpose of complying with AML/CFT is permissible).

17. Countries should examine and if needed, amend and/or clarify the national legislations in order to ensure the proper balance. A dialogue between national authorities responsible for data protection and privacy and AML/CFT is useful, to adopt compatible and coherent policies such that financial institutions are able to meet legal requirements. National authorities could also consider developing and sharing, where necessary, an analysis of national laws and regulations to support effective information sharing (Paragraphs 3-7 of Annex-2).

ii. Financial institution secrecy provisions

18. Financial institution secrecy laws can inhibit information sharing. For example, financial institution secrecy can sometimes not be invalidated by "legitimate interest" or security concerns, depending on national legislation. In this respect, it should be noted that under Recommendation 9, countries are required to ensure that financial institution secrecy laws do not inhibit implementation of the FATF Recommendations.

B. Operational Challenges

19. Operational challenges may occur at an institutional and/or national level. 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. Outsourcing rules which place a restriction on how much work can be centralised offshore and conversely data or onshoring rules which mandate that data, IT system and operational process remain onshore can create limitations leading to operational complexity and process fragmentation.

20. 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 a global footprint through acquisition, necessitating the integration of different IT systems into those of the acquiring institutions.

21. In certain cases, information exchange between the public and private sector as well as among private entities relies on predefined templates that allow for automatic analysis and

aggregation of information. These templates should be flexible enough to take into account other relevant information (such as IP addresses, phone numbers, usernames, job title and organisation etc.) that is available to financial institutions. Standardisation of data formats may also promote data sharing by enabling integration.

C. Challenges for Supervisors

22. From the perspective of supervisors, lack of information sharing may inhibit implementation of consolidated supervision for AML/CFT purposes (e.g., as required under Recommendation 26). For example, in case of financial institutions operating through a network of branches/subsidiaries in a number of countries, host country laws (applicable to such branches/subsidiaries) may not permit the home supervisor of the parent bank to have access to, and examine all the customer's information maintained by such branch/subsidiary. This may necessitate separate arrangements between the home and host supervisor whereby the home supervisors examine such customer files on behalf of the parent (home) supervisor. This may hinder the timely and comprehensive review of records and also adversely impact the effective application of the consolidated group supervision for AML/CFT purposes.[3]

23. Supervisors should thus promote bilateral or multilateral agreements that efficiently support information sharing for AML/CFT purposes, specifying the information to be exchanged when exercising consolidated or group-wide supervision, along with the definition of timelines for the provision of that information. While these arrangements cannot overcome legal impediments that hinder information sharing, in case the consolidated supervision of the group is hindered due to any reasons (including lack of access to relevant information), or if the group is exposed to excessive risks that are not properly managed, home supervisor may limit the range of activities that the group may conduct and subject it to escalating supervisory measures, including directing the financial group to close the foreign offices in extreme cases.

[3] Essential Criteria 8 of the BCBS Core Principle 13 (home-host relationships) requires that the home supervisor is given on-site access to local offices and subsidiaries of a banking group in order to facilitate their assessment of the group's safety and soundness and compliance with customer due diligence requirements.

INFORMATION SHARING UNDER FATF RECOMMENDATIONS

24. This section sets out key FATF Recommendations (R.18, R.20 and R.21) and their expectations in the context of information sharing within financial group. The section also covers information sharing between financial institutions not belonging to the same group, as provided under FATF Recommendations.

A. Information sharing within financial groups

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.

i. Meaning of 'financial group' or 'group-wide' in the context of information sharing

25. A financial group's programmes against ML/TF should be applicable to all branches and majority owned subsidiaries of the financial group.[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] This should be subject to safeguards sufficient to ensure confidentiality of information and its use for the intended purposes only.

26. The term "Group wide" (or "enterprise-wide") used in the context of AML/CFT Programme requirements for the financial group under FATF Recommendation 18 includes all the entities (in domestic and cross border environments) comprised by the definition of financial group laid down in the FATF Glossary. 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.

27. 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."

[4] Interpretive Note to Recommendation 18, paragraph 4.
[5] Interpretive Note to Recommendation 18, paragraph 4.

ii. Information required to be shared for group-wide programmes

28. Information sharing in the financial group is meant to effectively identify, manage and mitigate ML/TF risks by the group. This should include information and analysis of transactions or activities which appear unusual (if such analysis was done); and could include an STR, its underlying information, or the fact that an STR has been submitted. Countries may determine the scope and extent of this information sharing, based on the sensitivity of the information, and its relevance to AML/CFT risk management (see paragraphs 50-54 below for further details). This should be in accordance with the legislative framework (both of home and host countries), determining the scope, extent and mechanism of such information sharing.

29. The table below 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. All the information as indicated in the below table may not be available, collected or needed in each and every case. This would depend upon the products and services being provided to the customers, geographical location, the existing legal framework as well as risk and context. Nevertheless, intra group information sharing may lead to an effective group-wide compliance programme.

Table 1. **AML/CFT Purposes for Information Sharing**

Types of Information	Examples of 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), in case of legal persons and arrangements: 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, targeted financial sanction information and any other information, whether identified from public sources or through internal investigation relating to ML/TF, risk categorisation of customer etc.	Manage customer and geographical risks, identify global risk exposure as a result of on-boarding of the same customer by multiple entities within the group, more efficient record-keeping of customer information.
Beneficial Owner Information	Beneficial owner identification and contact information, real estate holdings, information on source of funds and wealth, economic/professional activity, and account files, whether the beneficial owner is a PEP or not and other relevant elements from documents collected while on-boarding a customer or updating records.	Manage beneficial owner and geographical risks, identify the same beneficial owner for multiple entities within the group, more efficient record-keeping of beneficial owner information.

Types of Information	Examples of information elements (as available, when necessary)	AML/CFT purposes for sharing information within the group
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, analysis made to detect unusual or suspicious transactions etc.	Global transaction monitoring, alert processing and identifying suspicious transactions, flagging and checking the existence of similar behaviour across business lines within the group.

iii. Importance of sharing of information for group-wide programmes

30. 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. It 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. The sharing of 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.

31. The BCBS's 2017 Guidelines[6] on *"Sound management of risk related to money laundering and financing of terrorism"* also provides 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

[6] See BCBS Guidelines on Sound Management of Risks Related to Money Laundering and financing of Terrorism.

strengthening group-wide risk assessment and the implementation of effective group-wide AML/CFT policies and procedures.[7]

32. The following are the main outcomes expected of information sharing for group-wide programmes:

a) Global risk assessment

33. 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 from each entity belonging to the same group. A comprehensive understanding and identification of these risks will allow the financial institutions to better structure its risk profile and take commensurate measures. Information from branches, subsidiaries and other parts of its business should feed into overall risk assessment. It will help identify and determine the nature and level of ML/TF risk of each entity belonging to the group and the level of ML/TF risk of the group on a global basis, particularly where the shared information relates to cross border relationships. 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 required information sharing, which may inhibit effective implementation of FATF Recommendations, as an autonomous risk and consider mitigation measures accordingly.

34. 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 and should have information relevant for its own risk assessment. 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 local 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.

35. 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. 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. Consideration should be given to local legal constraints on access to confidential

[7] "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).

information and addressed in the global risk assessment with commensurate measures implemented by the financial group.

b) Effective mitigation of customer, product, services and geographical risks

36. 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 in devising 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.

37. 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.

c) Consistent application of controls

38. 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 the 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, as required under FATF Recommendations), 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.[8] This may be required, for example, when the risks outweigh the institution's ability to manage the risk through commensurate measures.

[8] INR 18.5.

39. 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.

d) Common approach by financial conglomerates having multiple businesses

40. 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.

B. Sharing of information on suspicions that funds are the proceeds of crime or related to terrorist financing within the financial group

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).

41. 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.

42. 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. Advances in data science techniques and analytics enable financial institutions to sift through large amounts of structured and unstructured data to identify patterns and trends. Harnessing of this potential requires as much information as possible to be brought together, often in a centralised pool, and is in the interest of both the public and the private sectors.

43. Sharing of information and analysis of transactions or activities which appear unusual (if such analysis was done); including an STR, its underlying information, or the fact that an STR has been submitted by branches and subsidiaries with group compliance promotes effective implementation of group-wide compliance programmes.[9] Similarly, branches and subsidiaries should receive such information from group-level functions when relevant and appropriate to risk management. 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. It allows financial institutions to identify higher risk customers across the group's business and deploy specific monitoring mechanisms or enhanced measures. It 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, which may occur before or after filing of an actual STR by the financial institutions, where required will enable the group compliance to look at the suspect customer's activities or transactions across different verticals, lines of business and jurisdictions. This will also allow them to conduct sophisticated analyses of suspicious activities, assess these analyses against the client database and build the scenario across its global operations (paragraph 8 of Annex-2).

44. 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 TF 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.

45. 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 further scrutiny or an STR filing as needed. 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 subsidiary could be imputed to the entity. However this does not imply that intentional non-compliance to a financial group is imputed when the inability to communicate effectively is the result of the inability to lawfully share such information in the first instance. It is also incumbent upon the financial institutions to document appropriate criteria for the sharing of information (in accordance with laws and regulations in the host country) in support of a group-wide risk management compliance program and to ensure that safeguards are in place for the protection of the confidentiality of the information and its restricted use for the intended purpose of AML/CFT. Where there are challenges to the effective implementation of group-wide risk management, financial

[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.

institutions should apply appropriate additional measures to manage the ML/TF risks and inform their home supervisors, as appropriate.

C. Confidentiality of STR and tipping-off 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. These provisions are not intended to inhibit information sharing under Recommendation 18.

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

46. One of the main concerns that relates to sharing of STRs (or sharing the fact that a STR has been filed or the underlying STR information) is ensuring their confidentiality, which is critical to the 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.

47. 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.

48. Another concern that relates to sharing of STRs relates to how information can be shared domestically and internationally. 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 may 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. In order to ensure the confidentiality of STRs which are shared across jurisdictions, countries should consider extending

the same legal protections to foreign STRs which are given to domestic STRs within their legal system.

49. Finally, there are concerns that group-wide suspicious information sharing could potentially lead financial groups to systematically submit STRs only in their home jurisdiction, rather than in the jurisdictions in which the relevant financial institutions of the group are located. A related concern is that even if the STR is submitted in the relevant jurisdictions, the financial group's internal investigation may take place only in one jurisdiction (of the parent company), leaving some relevant information outside the reach of the host FIU's powers to request additional information from the financial institution. Such coordination and internal investigation across the group should be handled expeditiously so as to not lead to delay in the timely filing of the STR with the financial intelligence unit in the host jurisdiction. 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[10] where they are operating promptly, regardless of any sharing.

ii. Possible mechanisms for sharing of suspicious information within financial group

50. There are different ways in which information relating to unusual or 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 and analysis of transactions or activities which appear unusual, if such analysis was done (e.g. facts, transactions, circumstances and documents, including personal information). These information elements are illustrative and not meant to provide an exhaustive list. Sharing of relevant information in such cases could be without disclosing the fact that an STR is filed; or (b) disclosing the fact that a STR has been filed; or (c) disclosing the fact that an STR has been filed and sharing underlying information (e.g. information on suspicions and the results of any internal analysis or examination, (but not the STR itself); or (d) sharing of STRs and underlying information. This can be depicted as follows:

Table 2. **Possible ways for sharing suspicious information within financial group**

Possible ways	Information on suspicions, internal analysis or examination	Fact that an STR is filed	The STR itself
(a)	✓		
(b)		✓	
(c)	✓	✓	
(d)	✓	✓	✓

[10] Under the EU framework, financial institutions have to report suspicious transactions to the FIU of the Member State in whose territory the obliged entity transmitting the information is established. This means that in situations of free provision of cross-border services, STRs must always be submitted to the home FIU; if financial institutions operate establishments in another Member State, they must submit STRs to the host FIU. In some specific circumstances and subject to limitative criteria, national laws may go beyond EU passporting rules. The European Court of Justice confirmed that, subject to the conditions that no effective mechanism ensuring full and complete cooperation between the Member States exists which would allow AML/CFT crimes to be combated effectively, and on condition that the legislation is proportionate, EU law would not preclude Member State's national legislation which requires credit institutions operating in that Member State without being established there, to forward directly to these Member State's authorities information necessary for combatting ML/TF (see C-212/11 - Judgment of the Court (Third Chamber) of 25 April 2013 - Jyske Bank Gibraltar Ltd v Administración del Estado)

51. One of the key objectives of information sharing in this respect is to improve compliance with risk management and reporting obligations in all the locations where a multi-national group may operate. The overarching principle should be that the shared information may be found relevant by group compliance for an overall analysis and ML/TF risk management across the group or for some entities belonging to 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 sharing should be subject to adequate controls and monitoring by the group compliance to protect confidentiality of information and ensure its use only for ML/TF risk management.

iii. Criteria for sharing information within financial group

52. Financial institutions should determine appropriate criteria for sharing such information for the purpose of group compliance. This need not be the same criteria as for reporting of STR. For example, in some cases, there may still not be sufficient grounds to convert triggered red flags into to an STR, though sharing of information on any further analysis carried out in such cases to group compliance, may reveal additional information which may help making a filing decision. Depending on the circumstances, a financial institution may reach the STR reporting threshold at the same time as the unusual or potentially suspicious activity is initially detected (including prior to the execution of the transaction for attempted transactions). Or, in many cases, further analysis will be needed in order to determine whether the threshold for suspicion is met. This analysis may or may not result into filing a STR. Further, the very nature of transaction or business relationship of customer with financial institution may make some information irrelevant 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.

53. Systematic sharing of such information on a group-wide basis in each and every case may not be necessary or conducive to improved compliance with risk management and reporting obligations. Financial institutions should expressly address in their 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.

iv. Safeguards to protect information shared

54. Financial institutions should establish sufficient safeguards concerning the information shared to ensure that (a) confidentiality of information so shared is protected (including against tipping-off) and (b) information is used only for AML/CFT purposes and not for any other purpose. These should include policies, protocols and procedures for such sharing and setting up of access controls and firewalls, 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) so that such information is ring-fenced, and accessible only by AML/CFT staff and only for specific AML/CFT purposes. Furthermore, the 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.

v. Resolving legal barriers and engagement with private sector

55. Countries should seek to address any legal and regulatory barriers which impede the flow of information within the financial group, thereby inhibiting effective implementation of FATF Recommendations. This may require a thorough assessment of the existing provisions (DPP, financial secrecy, AML/CFT or any other legislation) restricting information sharing. A proactive engagement with the private sector can also identify areas where there is a divergent view between the public sector and private sector on expectations of the existing requirements. This may be followed by issuing appropriate guidance and clarifications to create an enabling environment for sharing of information.

INFORMATION SHARING BETWEEN FINANCIAL INSTITUTIONS NOT IN THE SAME GROUP

56. Effective AML/CFT systems at national and international level also require information sharing between different financial institutions, which are not part of the same financial group. This includes information sharing between different institutions both within a single country, and internationally, and is affected by all the constraints and obstacles noted above. Key FATF Recommendations requiring information sharing between financial institutions which are not part of the same financial group are R.13 (correspondent banking), R.14 (MVTS), R.16 (wire transfer) and R.17 (Third party reliance). Each of these requires specific information to be provided or available, in order to implement essential preventive measures.

57. Sections III and IV set out information sharing between different financial institutions based on key FATF Recommendations, and also describe the benefits of voluntarily sharing additional information, and how this can be facilitated.

A. Information sharing under FATF Recommendations

i. In the context of correspondent banking relationships (R.13)

58. Financial institutions are required to gather sufficient information about a respondent institution to fully understand the nature of its business and to assess respondent institution's AML/CFT controls and be satisfied with the mode of use of payable-through accounts. This would include an understanding of types of customers the respondent institutions intends to service through such relationship, the expected nature of transactions, their value etc. In some specific cases the correspondent institution may require additional information from respondents to effectively monitor respondent's transactions. Such monitoring may require the respondent banks to provide specific transaction and customer information to correspondent banks to allow them to dispose the alerts generated by their transaction monitoring systems. However, this review of information by the correspondent bank should not be triggered by and does not amount to a requirement to conduct CDD on the customer of the respondent but as a consequence of the monitoring of the transactions to or from the respondent bank.[11]

59. Respondent institutions should be able to provide additional targeted information requested by correspondent in some specific cases on specific customers and transactions. Due to absence of such information on account of information sharing restrictions, correspondent banks may not be able to apply appropriate AML/CFT controls to manage the risks associated such relationships.[12] In such cases, without further information, correspondents may have no alternative but to suspend the business relationship. This could eventually lead to a delay in processing or even the termination of correspondent banking relationships, thereby exacerbating the de-risking phenomenon (paragraph 12 of Annex-2).

60. To avoid such a scenario, appropriate mechanisms should exist to allow respondent financial institutions to share the requested information with correspondents. For this purpose, authorities of the respondent institutions should understand and clarify the cases in which correspondent institutions may request information and the type of information they may request, so that an appropriate sharing mechanism is put in place by respondent financial institutions to

[11] See FATF Guidance on Correspondent Banking Services (in particular, paragraphs 3, 4, 5 and 18).
[12] See FATF Guidance on Correspondent Banking Services (in particular, paragraphs 32, 33 and 41).

enable such information-flow. Countries could also consider encouraging responsiveness from respondent banks and expressly set out their obligations to share information with their correspondent.

61. Where warranted, countries should consider conducting evaluation of their existing legal framework to address challenges to information sharing in this respect, to ensure their own data protection, financial secrecy provisions or other related regulations are not causing their financial institutions to lose access to correspondent banking services. A dialogue and engagement between public and private sector may also further help identify specific areas or issues where guidance may be needed.

ii. In the context of Money or Value Transfer Services (MVTS) (R.14)

62. Under R.14, MVTS providers working through agents (regardless of their location) are required to include them in their AML/CFT programmes and monitor them for compliance with these programmes. This would require sharing of information from agents to their MVTS providers to enable them to effectively monitor their transactions. This would enable the MVTS providers to not only fulfil their oversight responsibility but also add value to the transaction monitoring and reporting mechanisms put in place by agents through sharing of feedback and further information.

63. In appropriate cases, targeted sharing of information on suspicious transactions may also help MVTS providers better manage their ML/TF risk, and ensure compliance with existing risk management and reporting obligations. Countries could consider issuing necessary guidance in this respect and identify and address any specific barriers that prevent sharing of such information.

iii. In the context of wire transfer (R.16)

64. FATF Recommendation 16 requires countries to ensure that financial institutions include required and accurate originator information, and required beneficiary information, on all domestic and cross-border wire transfers and related messages, and that the information remains with the wire transfer or related message throughout the payment chain. The objective of R.16 is to ensure that the basic information on originator and beneficiary of wire transfers should be immediately available to FIU/LEAs and also to ordering, intermediary and beneficiary financial institutions for transaction monitoring and filing STRs, sanctions screening, freezing and tracing of wire transfers.[13]

65. In case the relevant information is missing, intermediary and beneficiary financial institutions are required to have risk based policies and procedures for determining (a) when to execute, reject or suspend a wire transfer lacking required originator or beneficiary information; and (b) the appropriate follow-up action. This could, for example, include asking the previous financial institution in the payment chain for providing the missing or incomplete information as soon as possible. More fundamentally, such basic information about the originator and beneficiary is necessary for financial institutions to effectively execute wire transfers, and the transmission of such information would accordingly generally be authorised by non-AML legal frameworks.

66. Information sharing restrictions which impede financial institutions from sharing such information may lead to a considerable delay in processing. Countries should create enabling regulatory framework that removes barriers to information sharing in this respect. Appropriate guidance and feedback may further clarify regulatory expectations from financial institutions.

[13] FATF Interpretive Note to Recommendation 16, paragraph 1 and 2.

67. Further, consistent with paragraph 22 of the INR 16, MVTS providers are required to comply with all of the relevant requirements of Recommendation 16 in the countries in which they operate, directly or through their agents. In the case of a MVTS provider that controls both the ordering and the beneficiary side of a funds transfer, the MVTS provider: (a) should take into account all the information from both the ordering and beneficiary sides in order to determine whether this gives rise to suspicion; and (b) where necessary should file an STR with the appropriate FIU, and make relevant transaction information available to the FIU.[14] This would also require information flow in respect of cross border transactions executed by an MVTS provider. Countries should remove any existing barriers to information sharing and consider issuing appropriate guidance so that MVTS providers are able to comply with these requirements.

iv. In the context of third party reliance (R.17)

68. Under Recommendation 17, financial institutions may be allowed to rely on third parties (whether domestic or cross-border), to perform elements (a)-(c) of the CDD measures set out in Recommendation 10 or to introduce business. These elements are: (a) identification of customer, (b) identification of beneficial owner, and (c) purpose and intended nature of business relationship. The relying financial institution is required to immediately obtain necessary information concerning such elements, and to take adequate steps to be satisfied that copies of identification data and other CDD documents will be made available from the third party without delay, when so requested.

69. Use of third party reliance procedures is thus pre-conditioned on the ability of the financial institutions to be able to obtain relevant information from third parties. The need to understand the purpose and intended nature of business relationship may also necessitate sharing of additional information such as financial position of customers. This may help determine if the transactions being conducted are consistent with the financial institution's knowledge of customer, their business and risk profile. Information sharing restrictions or regulatory uncertainty may impede the ability of financial institutions to rely on third parties, especially in a cross border context. This may require intervention from host authorities of third parties to address any existing challenges, which prevent third parties from sharing information with financial institutions of the home countries, where permitted for reliance purposes.

v. In the context of regulation and supervision of financial institutions (R.26)

70. In the context of effective implementation of FATF Recommendations, for cross-border supervision, supervisors of the home jurisdiction should have access to the customer, account and transaction information maintained by the financial institution in the host jurisdiction, to the extent permissible under the legal frameworks of both jurisdictions. This should include STR and related information, where this is necessary to assess compliance with AML/CFT obligations and the robustness of risk management procedures. While host supervisors will be assessing compliance with local laws and obligations, home supervisors should have the ability to assess compliance with group-wide AML/CFT policies and procedures. Lack of such access may inhibit the ability of the home supervisor to effectively assess group compliance, thereby impacting the effective implementation of FATF Recommendations. If impediments to information sharing prove to be insurmountable, and there are no satisfactory alternative arrangements, the home supervisors should make it clear to the host supervisor that the financial institution may be subject to additional

[14] See paragraph 67 of FATF Guidance on RBA for MVTS, February 2016.

supervisory actions, such as enhanced supervisory measures on the group, including, as appropriate, requesting the parent group to close down its operations in the host jurisdiction.[15]

[15] See BCBS Guidelines on Sound Management of Risks Related to Money Laundering and financing of Terrorism, June 2017: Section IV

INNOVATIONS IN INFORMATION SHARING

Information sharing beyond the FATF Recommendations

71. Sharing of additional information between financial institutions - beyond the required information noted above that is required by the FATF Recommendations - can have wider benefits by strengthening the understanding of risks and vulnerabilities. It can also ensure better compliance and leveraging of capacities by the private sector and preventing criminals from exploiting individual financial institutions' lack of awareness of their activity with other institutions.

72. For example, some jurisdictions have found that sharing alerts or information about customers who are refused or exited due to ML/TF concerns can prevent arbitrage of the financial system by criminals, who may attempt to engage with many different institutions. Consolidating information on payments by multiple institutions can identify criminals structuring payments using multiple institutions to avoid detection by other means.

73. However, such information sharing can also raise a range of public policy concerns about how the information will be used (or misused), including unfair commercial practices, encouraging de-risking and financial exclusion, potentially breaching STR confidentiality and increased risk of tipping-off, customer confidentiality, data protection and privacy, financial institution secrecy, as well as the general information sharing challenges described in the earlier part of this guidance.

74. For example, sharing of customer information between financial institutions could potentially raise competition concerns resulting from selective sharing of information with only a small group of participants. De-risking and defensive STR filing behaviour may be exacerbated, e.g. if financial institutions feel obliged to file an STR on a customer simply because they have learnt that other financial institutions have done so (and without conducting their own internal investigations). Overreliance on a system of sharing of suspicious information or a common platform could potentially lead to moral hazard where a financial institution would regard a potentially suspicious customer as suspicious before proper due diligence is done, and hence preventing the customer from accessing the entire financial system.

75. Countries should carefully consider the legal, policy and operational concerns noted above, and design means of mitigating them. This would for example, include consideration of measures to avoid abuse of the sharing mechanism, unauthorised use of the information obtained and violation of the underlying principles of such sharing arrangements, as well as potential implications of such behaviour.

76. Countries should also provide clarity on what types of information can be shared, with whom, under what circumstances, for what purposes, and subject to which restrictions, depending on the sensitivity involved and the need to ensure confidentiality of information. This understanding could be documented and be supported by information security guidelines and access protocols. This would avoid varied interpretation, ambiguity in understanding and inconsistency in implementation, all of which can impede information sharing under these provisions. Suitable oversight mechanism and transparency would also ensure the confidence in and accountability of all stakeholders.

77. Nonetheless, in recent years, countries and the private sector have made great strides in data analytics that aid in the detection of ML/TF activities and trends. In order to share such information, sufficient safeguards and mechanisms within existing legal frameworks are permitting

information sharing that provides improved and more real time and actionable information, leading to positive outcomes. Some such mechanism and processes are described below and in Annex-2.

A. Types of information sharing

78. A range of information can be shared in this context, and in a number of different ways. This is set out below:

i. Information on risks, crime trends and typologies

79. Financial institutions can collaborate to share analytical and strategic information on recent risk and crime trends, methods, techniques, common typologies and modus operandi identified to abuse the financial system. Such information, stripped of personal data, would accordingly not implicate data protection and privacy, tipping off, or other protections for personally identifiable information. Such information sharing may provide good insights which can be used by participating financial institutions in their operations. This promotes a greater collaborative environment among participants and can also help keep the risk assessment up-to-date based on current trends and methods.

80. Often law enforcement authorities are also part of these initiatives and can provide a more comprehensive update on these crime trends and typologies, including through case examples and specific information on ML/TF risks. This can raise general awareness of the current financial crime scenario, strategic and operational risks derived from such crimes and their possible impact on the financial industry as a whole.

ii. Information on transactions and customer information

81. Some countries under their own domestic legal framework specifically allow sharing of certain transaction information, and other information on suspicious transactions (but not necessarily of the STR itself) between financial institutions which are not part of the same group. This may include information on customers, representatives and/or beneficial owners associated with two or more financial institutions or covered entities, including information on individuals or entities suspected of ML/TF. This applies, for instance, in cases where financial institutions share or have the same customers (paragraphs 10-14 of Annex-2).

82. Such information sharing may provide additional elements to asses customers' risk more effectively or may also facilitate confirmation of initial suspicion for example, when a newly opened account with some activity for a few months suddenly receives a huge wire transfer and it becomes necessary to request information from the remitting bank to confirm the source of funds and other related details. Countries could consider encouraging financial institutions to share specific threat information and high risk customer information with one another. This facilitates sharing of intelligence and assists in decision-making by authorities and the private sector, wherever relevant.

B. Mechanisms for information sharing

83. A number of possible models are currently being developed which may encourage such voluntary sharing of information. It could include include bilateral information exchange between financial institutions and/or **shared KYC utilities and/or centralized data repositories**, which capture key elements of customer and transaction information and disseminate such information to participating financial institutions with appropriate protocols and access controls. Such utilities can contain different types of information for AML/CFT purposes. It includes identification information on customer and/or beneficial owner and additional information to support risk assessment and risk profiling of customer by financial institutions. These utilities can be used at the time of on boarding a customer, to access customer information, as well as on an ongoing basis, to perform further customer due diligence measures. Such utilities can also contain updated information on respondent institutions, which can facilitate their risk assessment and ongoing due diligence by correspondents. In all such cases, the ultimate responsibility for due diligence remains with the financial institution using such utilities.

84. These utilities and databases can be hosted by the authorities or the private sector or both through a public private partnership. For example, in some countries databases to share information on international wire transfers conducted or either the fact that STRs have been filed and/or the content itself of STRs and related information have been created to facilitate information sharing in appropriate cases among reporting entities, as well as administrative and law enforcement authorities. However, such utilities and/or repositories, whoever hosted by, could give rise to questions on where the ultimate responsibility for monitoring lies, and who should be held accountable for failures – another form of moral hazard.

85. In some cases, **specific information sharing arrangements** to facilitate information sharing among financial institutions for AML/CFT purposes have been reached between jurisdictions. This can provide statutory gateway to facilitate information sharing between financial institutions in a cross border environment for AML/CFT purposes.

86. **Public private partnerships** for information sharing are also being developed in a number of jurisdictions and have achieved positive outcomes. Through such partnerships, information is shared across law enforcement, FIU, vetted participants from the private sector as well as international partners in some cases, to facilitate a more comprehensive view of transactions and customers' behaviour. Such sharing often happens in a secured environment in order to facilitate further data-mining, operational analysis and scanning by the private sector to fill potential intelligence gaps.

87. **Industry forums or platforms-** Initiative can also be steered by financial institutions by creating structures such as inter- bank forum or through their banking/industry associations to share information on recent crime trends, modus operandi and typologies across participants. Representatives of law enforcement and supervisors could also collaborate in such initiatives to further support the work.

88. Information sharing on customers and suspicious transactions may be facilitated by safe harbour provisions for financial institutions, provided that the safe harbour is not abused, and they have established and maintained adequate procedures to protect the security and confidentiality of the information. Such safe harbours can carve out specific legal protection to enable information sharing between financial institutions for AML/CFT purposes.

89. Annex-2 of the guidance provides information on the approaches taken by a number of countries to facilitate such information sharing. These are set out in detail in particular, in paragraphs 10-22, 29-30 and 32-34 of the Annex. These examples are presented for information only and their inclusion in this guidance does not amount to their endorsement by the FATF. Further, the Annex is only illustrative and does not contain an exhaustive list of all the examples, which may be leading to diverse outcomes. It, however highlights how different types of information (strategic as well as operational and customer related) can be shared following different models or mechanisms in different contexts for AML/CFT purposes.

90. There are significant benefits of information sharing between financial institutions and at the same time, there are potential risks that need to first be addressed or mitigated. It is also affected by the same challenges as noted above. Countries are encouraged to assess how such voluntary information sharing which is beyond what is required by the FATF Standards can improve their AML/CFT system, and to develop their legislative framework to enable such sharing of information.

GUIDANCE AND FEEDBACK

91. Lack of guidance and feedback by public sector authorities on information shared by the private sector may hinder private sector's ability to effectively monitor transactions and provide well-developed reports to FIUs. In appropriate cases, countries could consider putting in place enhanced "feedback loop", whereby more consistent and more fully explained feedback is provided to the private sector on suspicious transactions reports. Further developing communications channels where the private sector receives feedback on thematic cases or information on targeted areas of focus would help provide clarity on regulatory expectations (paragraphs 23-28 of Annex-2). Countries could also consider developing specific engagement programmes with sectors that appear vulnerable to ML/TF threats (paragraph 31 of Annex-2).

92. Lack of guidance and feedback by public sector authorities may 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. Countries should also consider publishing information on the existing legal mechanisms, gateways and permissions, which permit financial institutions to share information, both group-wide and across financial institutions. This will provide greater clarity and assurance, and promote a consistent understanding across the private sector.

CONCLUSIONS

93. 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.

94. Legal constraints such as different legal frameworks of data protection and privacy and their implementation, financial institution secrecy provisions and operational challenges may impede information sharing in group wide context as well between financial institutions not part of the same group. 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 include authorities (for example, AML/CFT authorities and data protection and privacy authorities) engaging with one other, wherever appropriate to arrive at a shared ground. This engagement can also identify areas where there is a lack of clarity or divergent views between the public sector and private sector. Clarity and guidance on such issues may help facilitate an efficient application of obligations.

95. 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 and data protection, while providing a legally certain regime for financial institutions which ensures that AML/CFT and data protection laws do not cut across one another. It is incumbent that national authorities responsible for AML/CFT and data protection recognize 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.

96. 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.

ANNEX-1 – DIFFERENCE IN DPP REGIMES AND THEIR APPLICATION

1. As stated in section 1 of this guidance, the differences in legal frameworks of DPP laws across jurisdictions, may create implementation challenges, particularly for the private sector, both in the group-wide and inter-institutional context of information sharing. These challenges can emerge due to following specific factors:

i. **Barriers to group-wide sharing of information.** Some jurisdictions treat group-wide sharing of information containing personal data 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.

ii. Principle of data minimisation under DPP framework requires that an organisation should only process the personal data that it actually needs to process in order to achieve its processing purposes, which are not defined in sufficiently clear and specific manner. It often leads to ambiguity on legality of information sharing. When personal data processing is required under domestic AML/CFT framework, ambiguity arises when the law does not prescribe the obligation to process personal data in sufficiently clear way, more particularly due to lack of regulatory guidance on the purposes for which such data can be collected, processed and shared. 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.

iii. **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. Furthermore, there may also be an absolute prohibition in certain jurisdictions on transfer of personal data (or some of such 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 across jurisdictions for such purposes can help facilitate information sharing.

iv. **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.

v. **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 which do not allow processing such information.** 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.

vi. **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 is not easy. 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 data protection and 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 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.

vii. **The right of anonymity and to data deletion may limit the period of record-keeping requirements and their availability for 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 right to data protection.

ANNEX-2 – SELECTED EXAMPLES AND PRACTICES

2. 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. Country examples are presented for information and meant to be illustrative only. Their inclusion in this guidance does not amount to an endorsement by FATF. 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:

A. Interplay between AML/CFT and data protection frameworks.

3. 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 respective regulatory requirements

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.

4. In many cases data protection and privacy authorities are also consulted and invited to provide specific comments on AML/CFT measures 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 development of measures. 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.[16] The guidance acknowledges that the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (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 programmes or initiatives should be implemented in a manner that is privacy sensitive and consistent with privacy laws.

5. 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.

6. In certain jurisdictions, the data protection legislation provides for certain derogations and carve-outs which may be necessary 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 aimed at balancing 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.

[16] See the Office of the Privacy Commissioner of Canada

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.

7. 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.

B. Group-wide Information sharing

8. 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.

9. In some financial groups, analysis of suspicious information shared with group compliance is conducted by a monitoring and analysis centre, which is established centrally within a financial group to consolidate its focus on suspicious customers and to reduce the number of access points so as to prevent information from leaking. Such a centre can take prompt actions on different circumstances of suspicious transactions and alert other departments through their group system, which aims to prevent the customers from having exposure in more than one location or aspects of the flow of transactions or funds that affect operations in the relevant jurisdictions.

C. Information sharing between financial institutions not part of the same group

10. 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.

11. 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.

12. Specific bilateral arrangements to facilitate information sharing among financial institutions for AML/CFT purposes have been reached between some jurisdictions. It 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.

13. In other cases, countries have mandated financial institutions to share specific information on certain financial transactions through centralized databases operated by such institutions or a financial authority, and take that information into account as part of the risk assessment that such institutions must carry out on their customers.

Mexico

In 2017, based on the same rationale as that related to credit bureaus, an AML/CFT regulation was issued to mandate banks to provide to a centralized database operated by the central bank or by such banks certain information on every international wire transfer or domestic wire transfer in foreign currency that they send or receive on behalf of their customers. In addition, under that regulation, banks are obligated to obtain from the database certain aggregate information of the wire

transfers processed by their customers in the banking system as a whole and take that information into account to carry out the due diligence on their customers that request a wire transfer, and the general risk assessment of them. Customers must consent with their respective banks that they submit and obtain that information from the database. The applicable AML/CFT regulation specifies the information that banks must submit to the database as well as the statistical information that the database will provide to the banks. The central bank has developed this database and banks will be able to exchange the information on their customers transactions at the end of 2017 and in a second stage, banks will have to provide certain KYC information and documents of such customers and check that information in the database.

14. 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.

D. Information sharing between financial institutions and authorities

15. 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.

a) Public/Private Partnerships

16. 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.

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.

Australia

On 3 March 2017, AUSTRAC launched Fintel Alliance, which brings together government, industry, academia and international partners in collaborative and secure information sharing environment, thereby constituting a holistic approach to discovering, understanding and disrupting serious and organised crime, bribery and corruption and terrorism through the analysis of financial intelligence. The Fintel Alliance membership continues to grow with new applications currently being assessed. As of the end of April 2017, the Fintel Alliance comprises 19 partners including AUSTRAC, the AFP, NSW Police, the ATO, Australian Banks – ANZ, Commonwealth, Macquarie

Bank, National Australia Bank, Westpac, Western Union and PayPal. The UK National Crime Agency has joined the Fintel Alliance, and AUSTRAC is in discussions with other potential international partners.

The Fintel Alliance has established an Operations Hub where Government and industry intelligence analysts work side by side in joint operational projects, sharing information in near real-time. Three projects were undertaken to establish operations:

- examining the Panama Papers;
- identifying and profiling online money mules; and
- enhancing the use of Australian Cyber Online Reporting Network data.

17. 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.

18. 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.

19. 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.

b) Information sharing in the context of suspicious accounts and transactions

20. 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.

21. 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.

22. 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.

c) Guidance and Feedback

23. 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.

24. 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.

25. Information about particular countries which may pose a greater risk of terrorist financing or certain businesses 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.

26. 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 and leads to several successful investigation and prosecution of TF Crime. 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.

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.

27. 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.

28. 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.

29. 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.

30. 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.

d) Sector-specific engagement, outreach and guidance

31. 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.

e) Mechanisms of Information sharing

32. 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.

33. 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.

34. 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.

FATF

PRIVATE SECTOR INFORMATION SHARING

The guidance identifies the key challenges that inhibit sharing of information to manage ML/TF risks, both group-wide within financial groups, and between financial institutions which are not part of the same group. It articulates how the FATF standards on information sharing apply and highlights examples of how authorities can facilitate the sharing of information, as well as examples of constructive engagement between the public and the private sectors.

www.fatf-gafi.org | November 2017