Enterprise-wide STR Sharing:

Issues and Approaches

Egmont Group of Financial Intelligence Units

February 2011

Table of Contents

Abbreviations

AML	anti-money laundering
BCBS	Basel Committee on Banking Supervision
CFT	combating the financing of terrorism
CDD	customer due diligence
DBG	designated business group
EU	European Union
FATF	the Financial Action Task Force
FIU	financial intelligence unit
ML	money laundering
PEP	politically exposed person
STR	suspicious transaction report
TF	terrorist financing

Figures and Tables

Executive Summary

Many financial groups operating in multiple jurisdictions seek to implement a risk-based, enterprise-wide approach to anti-money laundering/combating the financing of terrorism (AML/CFT) compliance. In some cases, however, jurisdictions prevent the sharing of suspicious transaction reports (STRs) or related information across borders, limiting the ability of a financial group to fully implement enterprise-wide compliance policies.

A survey of the Egmont Group of Financial Intelligence Units (Egmont Group) conducted in 2008 established that jurisdictions have a diverse set of laws, regulations, and policies on enterprise-wide STR sharing. While a significant number of jurisdictions indicated that domestically-generated STRs could be shared across borders within a financial group, many jurisdictions indicated that the legal protections for the confidentiality of STRs generated in other jurisdictions were unclear or non-existent.

The continued assurance of STR confidentiality is the critical element in any effort to promote enterprise-wide STR sharing and, by extension, the risk-based approach to AML/CFT compliance. Confidentiality of reporting allows the suspicious transaction reporting system to function, protecting the interests of banks, governments (including financial intelligence units [FIUs]), and the public. The loss of confidentiality of an STR could put at risk a present or future law enforcement investigation or violate the financial privacy of the STR subject.

The major benefits from enterprise-wide STR sharing are expected to result from more effective AML/CFT compliance by financial groups operating in multiple jurisdictions. The ability to share information on suspicious transactions across the financial group should enhance all aspects of compliance, including customer due diligence, transaction monitoring, and suspicious transaction reporting. Financial groups should be able to incorporate a wider, enterprise-wide view of the activities of the STR subjects, thus giving FIUs more valuable information. Enterprise-wide STR sharing may also result in efficiency gains in the processing of STRs within financial groups.

Jurisdictions seeking to allow domestic banks to share STRs with their head office, a subsidiary, a branch, or an affiliate in another jurisdiction might do so in a number of ways. One approach taken by governments has been to allow sharing only with entities in certain approved jurisdictions with strong confidentiality protections, thus limiting the risk of a STR confidentiality violation. Alternatively, a government might choose to allow sharing only with the bank's head office, as opposed to its foreign subsidiaries, branches, and affiliates, which would allow the head office to implement a more comprehensive and inclusive AML/CFT program and limit the exposure of the STR across multiple jurisdictions. Bilateral or multilateral agreements among jurisdictions may also provide a suitable mechanism for ensuring confidentiality for STRs shared across borders.

FIUs have clear stakes in the issue of STR sharing, whether or not they possess regulatory powers themselves. By their very nature, FIUs cannot operate without a properly functioning suspicious

transaction reporting system. FIUs will want to be certain that in whatever manner their jurisdictions choose to handle the issue, the processes that are created do not interfere with existing, well-defined channels for the sharing of STRs, both between the FIU and private sector, as well as in the context of the Egmont Group.

Introduction

Financial groups operating globally face a series of challenges rooted in the fact that the world is organized into a number of sovereign jurisdictions, each with its own laws and regulations. The present White Paper explores one of these challenges: the sharing of suspicious transaction reports (STRs) filed by one part of a financial group with other parts of the organization.

A critical aspect of the suspicious transaction reporting system in any jurisdiction is the confidentiality afforded to STRs. This confidentiality, when incorporated into domestic law, reflects an agreement among government, industry, and the public that the reporting system can work effectively only if the STR subject remains unaware that such STRs exist. Banks that have filed STRs need assurances that their customers will not discover that their transactions are being reported to the government. Governments need to be certain that those suspected of illicit activity are not made aware that their transactions have been judged suspicious, in order to protect ongoing or future investigations. STR confidentiality protects the public by securing personally identifying information and ensuring that the mere suspicion of an individual for illicit financial activity does not reach the public domain, unfairly damaging the reputation of the STR subject.

A key component of STR confidentiality is the prohibition against "tipping off," in other words, notifying any person involved in the transaction that the transaction has been reported. Financial Action Task Force (FATF) Recommendation 14 reads, in part, "[f]inancial institutions, their directors, officers and employees should be … prohibited by law from disclosing the fact that a suspicious transaction report or related information is being reported to the FIU."[1] Jurisdictions incorporate the prohibition against tipping off into their legislation, meaning that there are potentially a variety of specific formulations of the concept across the globe.

The notion of enterprise-wide STR sharing may come into conflict with jurisdictions' existing rules on STR confidentiality, depending on how those rules are written. For example, if a bank that is part of a global financial group seeks to share an STR with its head office in another jurisdiction, there may be limitations on providing the actual STR or information revealing its existence to the head office. Whether or not such a disclosure would constitute tipping off or otherwise violate STR confidentiality depends on how the issue is handled in domestic law or regulation, if at all.

> "The principal aim of monitoring in a risk-based system is to respond to enterprise-wide issues based on each financial institution's analysis of its major risks."
>
> – FATF, June 2007

Beyond STR confidentiality, another key aspect to anti-money laundering and combating the financing of terrorism (AML/CFT) regimes worldwide, particularly over the past several years, has been the risk-based approach to compliance by banks and other regulated entities.

[1] "FATF 40 Recommendations, Glossary, and Interpretive Notes," Financial Action Task Force, 20 June 2003, p. 5, available at http://www.fatf-gafi.org/document/6/0,3343,en_32250379_32236920_43689670_1_1_1_1,00.html.

Implementation of a risk-based approach to AML/CFT compliance allows resources to be allocated more effectively, but depends fundamentally on a bank's ability to collect information and properly gauge risk. In the context of a financial group operating in multiple jurisdictions, successful application of the risk-based approach requires enterprise-wide information sharing and resource allocation. For example, with respect to monitoring of customers and transactions, the FATF notes, "[t]he principal aim of monitoring in a risk-based system is to respond to enterprise-wide issues based on each financial institution's analysis of its major risks."[2]

> "…a bank should aim to apply the same risk management, customer acceptance policy, procedures for customer identification, and procedures for monitoring its accounts throughout its branches and subsidiaries around the world."
>
> – Basel Committee on Banking Supervision, October 2004

Independent of the risk-based approach *per se*, group-wide compliance brings its own benefits. As noted by the Basel Committee on Banking Supervision (BCBS) in its 2004 document entitled "Consolidated KYC Risk Management," "…a bank should aim to apply the same risk management, customer acceptance policy, procedures for customer identification, and procedures for monitoring its accounts throughout its branches and subsidiaries around the world."[3] The BCBS document identifies a number of benefits to group-wide compliance, including greater efficiencies and reduction of legal and reputational risk.

The focus on STR sharing within a financial group, as opposed to STR sharing among unaffiliated banks, reflects the idea that affiliated banks are far more likely than unaffiliated ones to be able to add value to global AML/CFT efforts through the sharing of STRs. A worldwide financial group operates as part of a global profit-seeking business model, leveraging economies of scale when possible and holding itself out to customers as being able to service needs in multiple jurisdictions. In practice, banks have a strong inclination to conduct business with their affiliates, as opposed to their competitors.

The present White Paper explores the issue of enterprise-wide STR sharing, looking at both the potential benefits of sharing and the risks inherent in allowing STRs to leave the jurisdiction in which they were originally filed. In general, the effects of STR sharing will likely be seen on a case-by-case basis, either in terms of the loss of confidentiality of an individual STR or in terms of an additional STR filing or piece of information resulting from the process of sharing. The paper also outlines a series of approaches jurisdictions might take to allow enterprise-wide STR sharing and considers the implications of each of the approaches for elements of governments, including financial intelligence units (FIUs). The paper does not endorse any particular approach to implementing enterprise-wide STR sharing, as the relative merits of each approach may vary depending on the exact nature of a jurisdiction's AML/CFT regime.

---

[2] "Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing," Financial Action Task Force, June 2007, p. 27.

[3] "Consolidated KYC Risk Management," Basel Committee on Banking Supervision, October 2004, p. 5.

The White Paper currently focuses on STR sharing among banks in a single financial group. Future work may consider the implications of enterprise-wide STR sharing in the context of other parts of the financial sector, including the insurance and securities industries.

It is hoped that the present paper will be of interest to all FIUs, as STRs are integral to an FIU's function. Many FIUs have direct roles in the administration of their respective domestic STR reporting systems, whether through the issuance of regulations or the supervision of regulated entities. Furthermore, as entities that receive, analyze, and disseminate STRs, FIUs are central players in their domestic AML/CFT systems. Many of the benefits envisioned from greater enterprise-wide STR sharing would accrue to FIUs in the form of greater compliance by regulated entities and higher-quality STRs. In terms of risks, FIUs have a clear stake in ensuring that mechanisms for enterprise-wide STR sharing do not undermine STR confidentiality.

The issue of STR sharing is relevant to a variety of jurisdictions, from those with the biggest global financial centers and the headquarters of multiple worldwide financial groups to those with smaller financial sectors that might be proportionally more dependent on cross-border financial transactions, including through subsidiaries, branches, and affiliates of foreign banks.

International cooperation will be critical in making progress on this issue, since no single jurisdiction can make cross-border enterprise-wide STR sharing a reality on its own. A financial group operating in several jurisdictions would need the ability to share STRs across all of those jurisdictions in order to fully realize the potential advantages of enterprise-wide STR sharing.

The Egmont Group's work on the issue of enterprise-wide STR sharing began in 2008 with the discussion of the issue at the Plenary meeting in Seoul, South Korea. The FIU of the United States, the Financial Crimes Enforcement Network (FinCEN), subsequently distributed a survey to Egmont-member FIUs, to which 60 FIUs responded. The Egmont Group also discussed enterprise-wide STR sharing at the Plenary in Doha, Qatar, in 2009. A Sub-group was formed in late 2009 to focus on the issue. Current membership in the Sub-group includes the FIUs of Australia, Belgium, France, Malaysia, Mexico, Peru, Spain, and the United States.

Definitions

The following definitions are intended to provide a common understanding of terms used throughout the current White Paper. The inclusion of definitions in the White Paper is not meant to imply that jurisdictions' legal and regulatory definitions of these terms should be exactly equivalent to one another, or to suggest changes to existing internationally-recognized definitions.

Affiliate: any company that controls, is controlled by, or is under common control with another company. Branches and subsidiaries potentially may qualify as affiliates under this definition, depending on the ownership structure being considered.[4]

Branch: an operating entity which does not have a separate legal status and is thus an integral part of the parent bank.[5]

Enterprise-wide STR Sharing: the dissemination of an STR of a bank, filed under the respective laws and/or regulations of the jurisdiction where the bank is located, to a bank within the same financial group, whether or not the receiving bank is located in another jurisdiction. This paper also sometimes employs the phrase "cross-border STR sharing" to emphasize the international nature of the sharing. For an enterprise that operates in multiple jurisdictions, the terms are synonymous.

Financial Group: an organization's one or more banks, and the branches, subsidiaries, and affiliates of those banks.[6]

Head Office: the parent bank of a financial group or the unit in which AML/CFT risk management is performed on a business line basis.[7]

Subsidiary: a legally independent institution which is wholly-owned or majority owned by a bank.[8]

---

[4] The concept of affiliate may be defined differently by various jurisdictions, but it is widely-accepted within the banking supervision field.

[5] Compare with "Principles for the Supervision of Banks' Foreign Establishments," Basel Committee on Banking Supervision, May 1983, p. 2. The referenced text describes types of "foreign banking establishment[s]." The definition used in this paper is slightly different in order to capture both foreign and domestic branches, but otherwise utilizes the same framework as in the referenced text.

[6] Compare with "Consolidated KYC Risk Management," Basel Committee on Banking Supervision, October 2004, p. 4, footnote 2.

[7] See "Consolidated KYC Risk Management," Basel Committee on Banking Supervision, October 2004, p. 4, footnote 2.

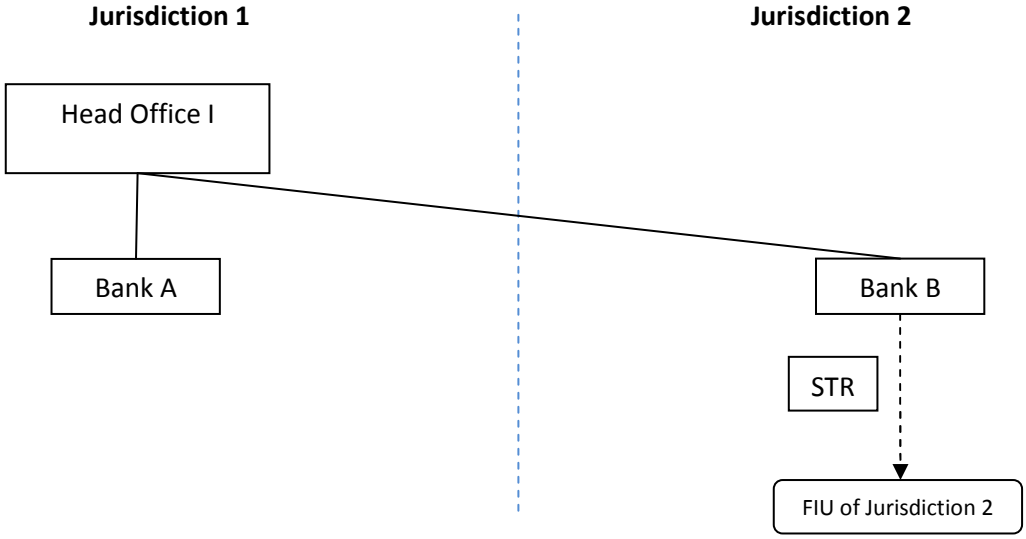
[8] Compare with "Principles for the Supervision of Banks' Foreign Establishments," Basel Committee on Banking Supervision, May 1983, p. 2. The referenced text describes types of "foreign banking establishment[s]." The

Suspicious Transaction Report: a report filed by a bank or other entity with its jurisdiction's financial intelligence unit based on a suspicion or reasonable ground for a suspicion that funds are the proceeds of a criminal activity or are related to terrorist financing.[9] For the purposes of this White Paper, it is convenient to define two additional terms relating to STRs, as follows:

> **Domestic Suspicious Transaction Report:** From the perspective of a given jurisdiction, an STR filed in that jurisdiction by a bank or other entity under domestic laws and/or regulations regarding STR filings. (See figure 1.)
>
> **Foreign Suspicious Transaction Report:** From the perspective of a given jurisdiction, an STR that was filed under the laws and/or regulations of a foreign jurisdiction. Under enterprise-wide STR sharing, a foreign STR may under certain circumstances be shared with a bank or other entity in the given jurisdiction. (See figure 1.)

In Figure 1, Bank B is filing an STR with its FIU. From the perspective of Jurisdiction 2, the STR is a domestic STR. From the perspective of Jurisdiction 1, the STR is a foreign STR. Under enterprise-wide STR sharing, Bank B may share the STR with Bank A since Banks A and B are members of the same financial group.

Figure 1 – Domestic and Foreign STRs



definition used in this paper is slightly different in order to capture both foreign and domestic subsidiaries, but otherwise utilizes the same framework as in the referenced text.

[9] Compare with "FATF 40 Recommendations, Glossary, and Interpretive Notes," Financial Action Task Force, 20 June 2003, p. 8, available at http://www.fatf-gafi.org/document/6/0,3343,en32250379_32236920_43689670_1_1_1_1,00.html .

Egmont STR Sharing Survey

In order to develop a greater understanding of jurisdictions' current laws, regulations, and practices regarding enterprise-wide STR sharing, a questionnaire was circulated in late 2008 within the Egmont Group. Sixty FIUs responded to the survey, yielding a response rate of 56 percent. Not all FIUs responded to each question; the number of respondents to individual questions varied between 52 and 60.

The questionnaire consisted of 19 questions divided into 5 sections: enterprise-wide sharing; sharing among unrelated entities; sharing with foreign governments; privacy and data protection; and general questions. Many of the questions focused on the extent to which banks and other financial institutions are permitted to share STRs domestically and internationally, both with other members of a single financial group and with unrelated institutions. The questionnaire asked about the sharing of STRs themselves and the sharing of information relating to or underlying STRs. The questionnaire also sought to distinguish between sharing by banks and by other types of reporting entities.

Questions were generally written to allow for "yes" or "no" answers, with space for additional comments or references to laws and regulations. The full text of the questionnaire is provided in the Appendix, along with a summary of the results listed by question.

Domestic Sharing

On the issue of sharing STRs within a single jurisdiction, the survey focused on two issues: 1.) sharing among different offices of a single corporate entity, and 2.) sharing among different offices of different corporate entities under common ownership or control. The latter situation corresponds to enterprise-wide STR sharing in a domestic context.

Question 1: Does your jurisdiction allow for the sharing of STRs among different offices of a single corporate entity, domestically (for example, can a bank have one single compliance office maintaining all STRs for all domestic branches of the bank)?

Yes: 93% **No: 7%**

Domestic sharing within a single corporate entity, such as among branches of a single bank, is widely permitted by the jurisdictions surveyed, with 93 percent of respondents indicating that it is allowed. Indeed, some FIUs indicated that a centralized AML/CFT compliance unit was required for a single corporate entity. When the scope of the question was expanded to the sharing of information related to or underlying the STR, rather than the STR itself, the percentage of positive responses was similarly high. Two jurisdictions are less restrictive with respect to sharing such associated information than with sharing STRs themselves, while three jurisdictions are more restrictive. Rules relating to domestic sharing within a single corporate entity are generally the same for banks as for other types of reporting entities, with only two FIUs indicating that the rules for banks differ from those for other reporting entities in their jurisdictions.

While domestic sharing within a single corporate entity is almost universally allowed, domestic enterprise-wide STR sharing among different offices of different corporate entities under common ownership or control is permitted in less than half of the jurisdictions responding to the survey. In one case, an FIU stated that its prohibition against tipping off disallows sharing STRs with "any person," which would include another juridical person. Similarly, in a few jurisdictions, each corporate or reporting entity with a "legal personality" is required to have its own compliance office, and different compliance offices within a single financial group are not permitted to share STRs with one another. Another FIU cited data protection concerns specifically as the reason that domestic enterprise-wide STR sharing could not occur.

Surveyed jurisdictions generally did not distinguish between banks and other reporting entities in terms of authorizing domestic enterprise-wide sharing. Only three FIUs indicated that sharing is generally allowed for reporting entities, but not for banks. One of these FIUs noted that sharing is prohibited only for those types of institutions covered by its banking secrecy law.

About one quarter of FIUs reported that STRs could be shared among unrelated corporate entities in the domestic context. An additional five percent indicated that underlying or related information could be shared, as opposed to the STR itself. As might be expected, jurisdictions that allow sharing among unrelated corporate entities typically also allow sharing among corporate entities under common ownership or control. A few FIUs answered that sharing among unrelated entities is possible while sharing among related entities under common control is not. This unexpected result may be related to the specific wording of the relevant questions (questions 2 and 7), which are not perfectly analogous, particularly with respect to the examples they include.

Cross-border Sharing

The survey results indicated that cross-border sharing of STRs among offices of different corporate entities under common ownership or control is allowed in only 40 percent of jurisdictions. In the majority of cases, if a jurisdiction allows sharing of STRs themselves, it also allows the sharing of information related to or underlying the STR. At the same time, 6 of the 33 jurisdictions that do not allow sharing of the STR do allow the sharing of related or underlying information. Put another way, of a total of 59 jurisdictions responding to the question, 29 of those jurisdictions allow either the sharing of the STR itself or information related to or underlying the STR. Only a few FIUs indicated that their jurisdiction's policy for reporting entities in general is different than its policy for banks.

Question 4: Does your jurisdiction allow for the sharing of STRs among different offices of different corporate entities under common ownership or control, across jurisdictions (for example, (i) can a foreign bank with a subsidiary in your jurisdiction share STRs among that subsidiary and its headquarters or affiliates in other jurisdictions; (ii) can a bank headquartered in your jurisdiction share STRs among that headquarters and subsidiaries in other jurisdictions)?

Yes: 40% **No: 60%**

One FIU cited domestic legislation that specifically prohibits sharing any information that an STR had been

filed with a variety of foreign entities, including the head office and foreign branches. On the other hand, several FIUs noted that foreign bank branches are considered components of the bank, permitting cross-border STR sharing between branches and the head office.

A number of European FIUs made reference to Section 28 of the European Union's Third Money Laundering Directive (Directive 2005/60/EC) as a legal basis for domestic laws allowing some degree of cross-border STR sharing. Respondents described existing or planned domestic rules to implement Section 28 that would allow institutions to share under certain circumstances across the European Union (EU) and other specially-designated jurisdictions.

Sharing of STRs among unrelated corporate entities across jurisdictions, such as sharing between two unrelated banks, is permitted in about one quarter of the jurisdictions surveyed. With only one exception, jurisdictions allowing cross-border sharing among unrelated corporate entities also allow some other kind of cross-border sharing, whether across related corporate entities or among different offices of different corporate entities under common control. As might be expected, jurisdictions are more likely to allow cross-border sharing when corporate entities are related than when they are not. One FIU reported that cross-border STR sharing among unrelated institutions would be possible only through FIU channels.

Treatment of Foreign STRs

Question 12: Do the protections for STRs and prohibitions against disclosure in your jurisdiction depend upon or otherwise assume that they apply only with respect to required reporting entities in your jurisdiction, or to reports originated or filed there?

Yes: 56% **No: 44%**

The survey asked a series of questions regarding the treatment of foreign STRs, i.e., STRs that have been filed with an FIU in one jurisdiction and subsequently shared by a bank or other financial institution in that jurisdiction with the bank's head office, subsidiary, branch, or affiliate in another jurisdiction. Only 22 percent of FIUs indicated that financial institutions could share foreign STRs or related information with foreign government authorities other than the FIU, such as financial supervisory authorities. In 34 of the 40 jurisdictions where such sharing is not permitted, the prohibition is a matter of settled law. In only 8 percent of jurisdictions surveyed could a financial institution share STRs directly with a foreign FIU, as opposed to sharing them with its domestic FIU.

Slightly over half of the survey respondents indicated that existing protections against disclosure of STRs are applicable only to domestic reporting entities or domestic STRs, as opposed to foreign STRs. One FIU noted that a foreign STR could be used in a judicial or administrative proceeding, subject to rules regarding evidence. A few FIUs provided comments indicating that the legal status of foreign STRs is unclear. For example, one FIU noted that the idea of a "foreign source STR" did not exist in its domestic law. Another FIU indicated that its laws did not distinguish between foreign and domestic STRs.

Analysis and Issues for Consideration

Overall, the survey demonstrated that there exists considerable variation in the laws, regulations, and policies regarding the sharing of STRs and STR-related information both domestically and across jurisdictions. Jurisdictions incorporate limitations on domestic and cross-border sharing through domestic law in a variety of ways, including provisions on STR confidentiality or tipping off and the requirements surrounding AML/CFT compliance. In some jurisdictions, the legal definitions of corporate entities affect the extent to which STR sharing is permitted. In cases where sharing is not allowed, it is not always clear whether domestic legislation was purposely constructed to prohibit sharing, or whether the prohibition is an unintended consequence of the wording of the legislation.

In addition to explicit limitations on sharing, it is clear that current protections relating to STR confidentiality do not always extend to foreign STRs. Fifty-six percent of respondents indicated that foreign STRs would not be protected in the same way that domestic STRs are protected, and in the majority of cases, this is a matter of settled law. This statistic may in fact be a cause for some concern for those jurisdictions that currently allow STRs to be shared outside of their borders, unless specific arrangements to preserve confidentiality have been made on a bilateral basis. More broadly, jurisdictions' varying and possibly inconsistent approaches to STR sharing and the protection of foreign STRs may pose a significant threat to the worldwide system of suspicious transaction reporting and thus be of concern to all FIUs.

Potential Risks of Cross-Border STR Sharing

In order to implement laws or regulations that would permit enterprise-wide STR sharing within a particular jurisdiction, it is critical to analyze the potential risks that are inherent to such an endeavor. Under any enterprise-wide STR sharing regime, numerous parties would be affected, including financial groups, law enforcement agencies, FIUs, and primary regulators of banks. This section explores those risks that involved parties will likely encounter if STRs were to be shared across international borders. Table 1, at the end of this section, summarizes the potential risks for each major set of actors in a jurisdiction's AML/CFT regime.

Violation of STR Confidentiality

When an STR is shared across borders, it could travel to a foreign jurisdiction that provides less confidentiality to the STR than the jurisdiction where it originated. This loss of confidentiality could occur in a variety of ways. A foreign jurisdiction could have insufficient STR confidentiality laws. There may be corruption problems in the foreign jurisdiction. Further, a foreign jurisdiction may grant its own law enforcement authorities access to foreign STRs without having to utilize agreed upon formal international information sharing channels.

The operation of judicial systems in different jurisdictions may also present risks to STR confidentiality. Some jurisdictions may have an absolute rule that STRs and information that would reveal the existence of an STR cannot be revealed by any type of judicial action, such as by discovery process, order of the court, or use as evidence in criminal or civil litigation. However, not all jurisdictions may adhere to this standard. Therefore, an STR could travel from a jurisdiction where the STR is not discoverable by legal process to a foreign jurisdiction where the STR could be revealed in a judicial setting.

> The potential risk to STR confidentiality associated with STR sharing must be considered in the context of other debates underway within global financial groups on the protection of sensitive data in the modern age.

It is important to note that banks are increasingly looking to centralize IT databases, and in some cases, they might be compelled by their regulators to maintain backup data in remote locations. Where data are stored in electronic form and retrievable through the Internet, there may be risk to STR confidentiality in other jurisdictions independent of enterprise-wide STR sharing. Therefore, the potential risk to STR confidentiality associated with STR sharing must be considered in the context of other debates underway within global financial groups on the protection of sensitive data in the modern age.

Impact on integrity of suspicious transaction reporting system. The confidentiality of the STR is one of the foundations of the AML/CFT system. This principle has allowed reporting entities in the banking sector to file STRs in spite of banking secrecy laws. The principle of confidentiality enables FIUs to build relationships based on trust with reporting entities. Undermining the confidentiality principle carries the very serious risk of damaging existing relationships between FIUs and reporting entities, ultimately

reducing the quality of STRs that FIUs receive. Significant reductions in STR confidentiality could put at risk the suspicious transaction reporting regime itself.

Impact on financial privacy. Banks are at risk of violating financial privacy provisions if personal information that is contained within an STR passes to a jurisdiction that does not have financial privacy provisions. Many STRs contain highly confidential financial information and unproven allegations about private citizens and legal entities, both of which could damage the interests or reputations of the STR subjects if made public. To the extent that banks engage in "defensive" filing of STRs[10] or file STRs based solely on name matches to watch lists, the concern about unfair damage to the reputations of STR subjects is intensified. Also, institutions must consider the possibility that identity theft or other fraud could result if STRs are disseminated inappropriately.

STR confidentiality is at the center of the AML/CFT system and was one of the core conditions enabling the full participation of reporting entities. Depending on how enterprise-wide STR sharing is implemented, it could increase the risk of non-controlled disclosures of STRs. Given the concern for data protection and privacy in many jurisdictions, any non-controlled disclosures could damage the image of banks. The possibility of violation of STR confidentiality, particularly on a large scale, constitutes a legal and reputational risk for a bank. As such, it is also a concern for a prudential financial regulator.

Impact on law enforcement investigations. If an STR is sent to the bank's head office, subsidiary, branch, or affiliate in a foreign jurisdiction that has poor confidentiality protections, permits access to STRs by individuals through a judicial process, or suffers from significant levels of corruption, criminal and civil investigations and trials in either jurisdiction could be compromised. Additionally, if the STR is permitted to pass through multiple jurisdictions, there is an increased risk that the STR subject may become aware of the report, which may undermine law enforcement investigations.

Another concern is that the STR filed in one jurisdiction could be accessed by a foreign law enforcement body by a using a warrant or other similar domestic legal process. This would circumvent the Egmont Group process that already exists among jurisdictions for STR sharing between governments. If a law enforcement body is given such access to STRs of another jurisdiction, there is a strong possibility that an investigation might be negatively affected or two or more law enforcement agencies of different jurisdictions may, unknowingly, be working on the same case.

Impact on security of compliance staff. Violation of STR confidentiality could reveal information about the identity of a compliance staff member at the bank that is filing the STR. Under certain circumstances, such a disclosure could put the staff member at risk.

[10] Defensive filing refers to the practice of institutions filing STRs on transactions that they do not deem truly suspicious in order to reduce the risk of regulatory penalties for non-filing of STRs.

Other Risks

Disruption of the flow of STRs to FIUs. An issue of particular concern to FIUs relates to the effects of enterprise-wide STR sharing on the flow of STRs from banks to FIUs. When a bank receives an STR from its head office, a subsidiary, a branch, or an affiliate located in another jurisdiction, it may be required under its domestic laws to consider filing a related STR with its domestic FIU. Whether or not the receiving bank chooses to file the second STR will depend in part on the STR regime under which it operates. The receiving bank's jurisdiction may have different rules relating to the degree of suspicion required for an STR filing, a different monetary threshold for STR filing, or a different list of predicate crimes covered under the reporting regime. Also, the receiving bank may not agree with the original filer of the STR that the transaction in question is suspicious. Under this scenario, should the receiving bank choose to file an STR, it must be sent by the reporting bank to the territorially competent FIU, i.e., the FIU in its jurisdiction.

The Egmont STR sharing survey included a question asking FIUs whether domestic institutions in their jurisdictions could file STRs directly with foreign FIUs. Only eight percent of respondents indicated that such filing would be possible. Direct STR filing from a bank to a foreign FIU is a concern because it could disrupt the flow of STRs in a variety of ways, including by causing linguistic or formatting problems and increasing the number of channels of exchange of information.

Increase in defensive filing. As mentioned above, a reporting entity receiving a foreign STR from its head office, a subsidiary, a branch, or an affiliate may be compelled to file a corresponding STR with its domestic FIU. Depending on the correspondence between the STR reporting regimes of the two jurisdictions, the receiving entity may feel the need to file an STR even when it does not consider the transaction truly suspicious. This would be a form of defensive filing, making it more difficult for FIUs to determine which STRs are most important to analyze.

Increased resource demands on FIUs. An FIU or other competent authority could allow financial groups to implement an STR sharing system itself. On the other hand, an FIU with appropriate legal authority (such as one with regulatory powers) may decide to play a more active role and assist in coordinating the sharing process. In the latter case, an FIU could find itself unable to manage the additional responsibility without additional resources.

Table 1: Potential Risks and Impacts of Enterprise-wide STR Sharing

	Type of Entity Most Affected				
	Public	Financial Group	FIU	Law Enforcement	AML/CFT Regulator
Violation of STR Confidentiality					
Violation of privacy or identify theft of STR subject	X	X			X
Exposure of current or future investigation to STR subject	X			X	
Exposure of details of bank employee responsible for filing STR		X			
Undermining of suspicious transaction reporting system	X	X	X	X	X
Other Risks					
Disruption of flow of STRs to FIUs			X		X
Increase in "defensive filing"		X	X		X
Increased resource demand on FIUs			X		

Potential Benefits of Cross-Border STR Sharing

Notwithstanding the risks outlined in the previous section, enterprise-wide STR sharing has potential benefits for a jurisdiction's AML/CFT regime from the perspective of all of the entities in the system, including the financial sector, FIUs, law enforcement agencies, and regulators. All of these actors would have a wider access to information, leading to a more robust suspicious transaction reporting process. Banks would be able to exchange more information inside the financial group, with potential gains in both efficiency and effectiveness. FIUs and law enforcement agencies may receive a greater number of high-quality STRs, with a particular increase in information related to transnational cases. Regulators and supervisors may have a greater assurance that the institutions they regulate and supervise are discharging their AML/CFT responsibilities in an effective and efficient way. This section explores in more detail the potential benefits of enterprise-wide STR sharing to the AML/CFT system and the actors within it. Table 2, at the end of this section, shows the potential benefits for each major set of actors in a jurisdiction's AML/CFT regime.

Better AML/CFT Compliance

The possibility of transmitting relevant data on suspicious transactions within a single financial group would allow the exchange of information on subjects, transactions, trends, and patterns of money laundering and terrorist financing (ML/TF) throughout the group. This would allow the financial group to analyze the information as a whole, leading to the creation of enhanced compliance programs to protect its customers, products, and services from criminal activities.

Allowing STRs to be shared with the head office of a financial group would also increase the head office's ability to supervise the process by which each individual entity in the group conducts due diligence, monitors transactions, and files STRs.

Better customer due diligence. Enterprise-wide STR sharing may allow the different banks within a financial group to apply more effective customer due diligence (CDD), including a better awareness of potential activities of national politically exposed persons (PEPs). These two situations will have a positive impact in FATF Recommendations 5 and 6, relating to CDD and PEPs, respectively.

In many cases, a bank will impose greater scrutiny upon a customer who is an STR subject filed by that institution. Countermeasures might include the closing of the account, with processes in place to prevent the same customer from opening another account with the institution. However, in the absence of STR sharing, subsidiaries, branches, and affiliates may be unaware that a customer had previous interaction with another subsidiary, branch, or affiliate within the same financial group, leading to the possibility that they may open a new account with the customer or process transactions initiated by the customer using another institution. Therefore, enterprise-wide STR sharing may help a financial group protect itself from being abused by a customer denied further business by one of its banks or subsidiaries, branches, or affiliates of its banks.

Better transaction monitoring and STRs. Under enterprise-wide STR sharing, banks will be able to share STR information across the financial group at national and international levels, thereby, achieving an improvement on the flow and quality of the information. STRs may be of greater quality because banks would be better able to connect activities occurring across jurisdictions. For the same reason, banks may also file a greater number of STRs, as they may be more aware of suspicious transactions.[11] The information that banks transmit to the relevant authorities may be of a higher quality and, therefore, of greater usefulness when used to investigate ML/TF for eventual prosecution.

Banks may find that it is easier to detect and give the proper follow-up to suspicious transactions that due to their small amount would not otherwise have been detected. With the expansion of communication, banks may also be able to create a better alert system regarding transactions potentially related to ML/TF.

Expanding and standardizing information channels within a financial group should help to strengthen the whole financial group's corporate structure. The communication between banks and the authorities in charge of fighting ML/TF at all levels should be better since banks should be able to provide better quality and more relevant information.

Better information for law enforcement investigations. Enterprise-wide STR sharing should cause FIUs to receive more STRs related to international cases. The biggest reporting entities, particularly in financial sectors, are frequently part of an international financial group and often send the highest number of reports. Under STR sharing, an STR filed in one jurisdiction and shared with the head office, a subsidiary, a branch, or an affiliate in another will, in some cases, trigger a related STR in the second jurisdiction.[12]

With this information, FIUs can better fight the different stages of money laundering -- layering, placement, and integration -- even if these stages happen in several jurisdictions or if the primary offense occurs in another jurisdiction. Enterprise-wide STR sharing may also speed up processing cases, as FIUs will likely get information about activities in foreign jurisdictions via domestic STRs and not only from responses to their requests to other FIUs for information.

Furthermore, FIUs often will have no way of knowing that STRs relevant to their cases have been filed with FIUs in different jurisdictions. Proactive sharing of STR information and other financial intelligence (i.e., "spontaneous disclosures,") would make such information known, but FIUs spend much of their time and resources responding to explicit requests for information. Sharing within a financial group

[11] As noted in the section on potential risks, there is also the possibility of a greater number of "defensive" filings, i.e., STRs filed only to reduce the risk of regulatory penalties for non-filing of STRs.

[12] The shared STR will not always trigger a second STR, for a number of reasons. For example, the recipient may not consider the transaction suspicious, or the underlying activity may not be a predicate offense or even illegal in the second jurisdiction.

across borders increases the chance that information related to a cross-border transaction will be distributed to all of the FIUs that would find that information useful.

Better knowledge of international ML/TF trends and methods. The sharing of STRs may lead to a better understanding of the methods and techniques used by those engaged in financial crime. Comprehensive knowledge will be acquired through the ability to share STRs, providing a better understanding of the elements of financial crime within a specific jurisdiction or across multiple jurisdictions. Developing better international typologies may result in better decision making, both in the private and governmental sectors. As these typologies are subsequently provided to banks to strengthen their due diligence systems, information sharing within the same group could enhance this positive feedback loop in the AML/CFT system. Examples of the applications of information on international ML/TF trends and methods include national threat assessments and risk management tools for supervisors.

Other Benefits

Easier implementation of the risk-based approach. The sharing of STRs may add to a financial group's ability to implement a risk-based approach to AML/CFT compliance, by allowing the group to better understand the risks it faces as a whole. A key benefit of the risk-based approach for financial groups is the ability to be more efficient in discharging AML/CFT responsibilities, as limited resources are directed to those areas of the business judged to be most risky from the perspective of ML/TF. More efficient AML/CFT compliance by banks also benefits regulators, FIUs, and law enforcement agencies.

Efficiency gains in STR processing. If a bank is able to receive from its head office, a subsidiary, a branch, or an affiliate precise STR information that may be related to another suspicious transaction, it will have the opportunity to augment the information contained in its own STRs with information that would otherwise be unavailable.

Furthermore, if banks are able to share STR information, they will increase their efficiency in handling the information since they will not duplicate information. The procedures for producing and filing STRs could also be simplified. Institutions may have a greater ability to unify information processing systems for STRs, reducing costs.

Finally, by standardizing STR handling policies, financial groups may be able to create group-wide corporate processes for transaction monitoring and STR filing, leading to a higher level of confidentiality for STRs and related information. Independent of STR sharing rules, however, there may be limits on the degree to which policies can be standardized, depending on differences in AML/CFT or data protection legislation across jurisdictions.

Table 2: Potential Benefits of Enterprise-wide STR Sharing

	Type of Entity Most Affected				
	Public	Financial Group	FIU	Law Enforcement	AML/CFT Regulator
Better customer due diligence, transaction monitoring, and suspicious transaction reporting					
Better customer due diligence		X	X	X	
Better transaction monitoring and STRs		X	X	X	
Better information for law enforcement investigations	X			X	
Better knowledge of international ML/TF trends and methods		X	X	X	X
Other Benefits					
Easier application of risk-based approach to compliance by financial groups		X			X
Efficiency gains in STR processing		X	X		X

Key Considerations for a Cross-border STR Sharing Regime

The Egmont Group's main objective is to improve cooperation in the fight against ML and TF, especially in the areas of information exchange, training and the sharing of expertise. Initiatives to facilitate the sharing of STRs within global financial groups are consistent with this objective. However, appropriate safeguards against the misuse and inappropriate disclosure of information will be necessary to ensure ongoing confidence in the integrity of international and domestic AML/CFT frameworks.

This section discusses a number of issues that jurisdictions should consider when contemplating adjustments to their AML/CFT frameworks to promote cross-border, enterprise-wide STR sharing. In particular, this section will address how to make sharing feasible and effective, as well as the types of illicit activity it would likely be most helpful in detecting.

Making Cross-border STR Sharing Feasible

At present, domestic legal arrangements in many jurisdictions impede a financial group's ability to share STRs across borders. The main legal obstacles being encountered are:

- Tipping off provisions within national AML/CFT frameworks
- Data protection and privacy laws; and
- Confidentiality provisions.

As discussed previously, these domestic legal impediments are in place for a variety of important reasons. For example, if a jurisdiction authorizes the sharing of STRs across borders it exposes itself to the risk that it may be held responsible if the laws of one or more of the receiving jurisdictions do not sufficiently protect the confidentiality of the STR being shared. Furthermore, a domestic investigation and legal proceeding may be compromised if an STR becomes discoverable through another jurisdiction's compulsory regulatory, law enforcement, or legal processes.

To overcome these significant and justified concerns, a wide range of operational controls will need to be put in place, and existing legal frameworks and agreements will need to be reviewed and enhanced.

Legal consistency. Any cross-border sharing of confidential information should only take place within the parameters of an effective and enforceable legal framework. Much of the international community's efforts in this area should be focused on the creation and enforcement of agreed upon standards that ensure adequate safeguards against the deliberate, as well as unwitting, inappropriate release of sensitive information to third parties.

Ideally there would be complete standardization of information sharing protocols between jurisdictions. Although they relate to information sharing protocols between authorities, the Egmont Group's "Principles for Information Exchange" or similar mechanisms for sharing between authorities may

provide a basis or model for understanding and establishing the necessary protocols for the cross-border exchange of sensitive information. The standardization of protocols would ensure that banks are not required to consider and navigate multiple, possibly conflicting national requirements. As an example of multiple or conflicting requirements, one jurisdiction may only allow a bank to share information with the head office whereas another may permit sharing across the financial group.

Such an initiative would require wide-ranging international collaboration and concerted efforts to minimize the effects of the disparities between jurisdictions' domestic legal and policy frameworks. Domestic legal frameworks may need to be adjusted to address existing impediments including privacy and confidentiality laws, as well as tipping-off provisions within AML/CFT laws.

An example of successful cross-border legal harmonization (within a supra-national organization) is the EU Data Protection Directive which regulates the processing of personal data within the European Union. When the European Commission realized that diverging data protection legislation in the EU member states would impede the free flow of data within the EU zone, it decided to standardize data protection regulation. The EU has put in place a procedure to recognize foreign jurisdictions as compliant with EU requirements, such as data protection and respect of privacy, for the international exchange of information.[13]

Case Study – U.S.-EU Safe Harbor Privacy Principles

The Safe Harbor Privacy Principles were created to facilitate the exchange of personal data between the U.S. and EU in accordance with both jurisdictions' data protection and privacy requirements. In 2000, the U.S. Department of Commerce issued the Safe Harbor Privacy Principles and a number of related documents. The European Commission subsequently confirmed that these safeguards provide adequate protection under the Article 25.1 of the EU's Data Protection Directive regarding the transfer of personal data to countries outside of the EU. As part of the framework, the U.S. Department of Commerce maintains a publicly-available, regularly-updated list of U.S.-based organizations that have declared their adherence to the Safe Harbor Privacy Principles. A similar arrangement was made between the governments of the U.S. and Switzerland in 2009.

Commonalities between jurisdictions. Allowing the sharing of STRs only among a financial group's banks and the subsidiaries, branches, and affiliates of those banks that are located in jurisdictions with comparable legal and political systems would be a good way to maintain confidence in the integrity of the information exchange. However, it may be difficult in practice to define comparability, depending on the jurisdictions in question.

[13] See Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regards to the processing of personal data on the free movement of such data. Currently the EU has recognized the following countries as compliant with EU requirements: Argentina, Canada, Guernsey, Iceland, Isle of Man, Liechtenstein, Norway, Switzerland, and under some conditions the United States.

Common or similar laws would be most important in the areas of data protection, confidentiality and disclosure of information, as well as STR reporting. Equivalency between AML/CFT requirements would ensure the exchange of confidential information such as the content of an STR will only be done in order to exercise the due diligence obligations. Equivalency in personal data protection and privacy protection requirements is important in order to avoid non-controlled disclosure, which would have a detrimental effect on the suspicious transaction reporting regime in general. The whole system would be challenged, and particularly enterprise-wide STR sharing, as it would infringe on the necessary trust that serves as the basis of the AML/CFT system.

Two different methods could be used to ensure equivalency in the framework of data protection, respect for privacy, and AML/CFT legislation. An authority of a jurisdiction could be designated to assess the equivalency of its laws with those in other jurisdictions, as is done in the EU. Another solution might be to enter into bilateral or multilateral agreements. Cross-border legal arrangements applicable to the sharing of STRs should aim to ensure that:

- The information is only used for the purpose for which it is intended, i.e., the enterprise-wide management of AML/CFT compliance (transaction monitoring and STR reporting) and ultimately the detection of money laundering and/or terrorism financing, as well as associated predicate crimes;

- The authorities of the jurisdiction of the bank that shared the STR continue to control the information and should give their consent to enable the foreign authorities to use it;

- There is the highest level of protection of the identity of the individual that reported the original suspicion; and

- There are similar rules on STR reporting requirements (triggers for obligation to report, timeframes) including an obligation on a head office, subsidiary, branch, or affiliate that receives a shared STR to consider whether, subject to its domestic AML/CFT laws, it needs to file a related STR with its respective FIU.

Making Cross-border STR Sharing Effective

Global financial groups play an increasingly important role in combating ML and TF, especially through their reporting of suspicious transactions to FIUs and, indirectly, to law enforcement agencies. According to the Basel Committee on Banking Supervision's "Consolidated KYC Risk Management," in order to effectively capture instances and patterns of suspicious transactions there should be consistent identification and monitoring of customer accounts globally, as well as oversight at the group level.[14]

To be effective, the monitoring of customer accounts and transactions through decentralized databases requires wide-ranging and robust information sharing across the financial group, including sharing of

[14] "Consolidated KYC Risk Management," Basel Committee on Banking Supervision, October 2004

STRs and STR-related information. Policies and procedures that encourage and facilitate the proactive sharing of suspected, as well as confirmed, illicit activity increase the effectiveness of risk identification and mitigation and should provide authorities with a more complete picture of attempted and actual criminal activities.

However, any measures that facilitate the increased sharing of STRs need to be undertaken with due recognition of the potential risks associated with any sharing of sensitive information. Appropriate operational controls to minimize the potential for abuse or misuse need to be in place to prevent potential damage to the integrity of the STR reporting regime, which is predicated on the confidentiality and protection of information.

Good relationships between competent authorities. Good relationships between international authorities would provide an additional layer of assurance that the integrity of the system can be protected. Existing legal frameworks and controls can be complemented and strengthened by regular contact and information exchange between relevant authorities. This creates an environment of mutual trust and increases confidence that any sharing of STRs within financial groups is not abused by foreign governments.

Operational controls within banks. Examples of operational controls may include (but are not limited to):

- Enterprise-wide policies on the exchange of STRs and STR-related information and the maintenance and retention of sensitive customer information;
- Well-defined procedures for the transmission of sensitive data, though it would be very difficult to establish a common security standard where there are differences between locations in IT systems and procedures;
- The requisite technological set-up, including state-of-the-art data encryption facilities, for example;
- Appropriate corporate governance arrangements including oversight and control by senior management; and
- Regular review of the effectiveness of current arrangements, addressing questions such as:
  - Has the increased sharing of information had the desired effect or met its objectives? For example, is the enterprise-wide transaction monitoring system being regularly updated or adjusted with the latest information?
  - Are all relevant policies and procedures being adhered to and working in practice?
  - If breaches of protocols have taken place in the review period, how have they been remedied?
  - How many STRs resulting from enterprise-wide information sharing have been submitted to FIUs or other government agencies?

When STR Sharing Would be Particularly Valuable

Customers in multiple jurisdictions. According to feedback received from some banking industry associations, situations where customers conduct business transactions within the same financial group in different jurisdictions are ideally suited to the concept of enterprise-wide sharing of STRs. Such transactions generally occur in the normal course of their business with the bank, but may come to the attention of staff if they do not accord with their knowledge of the customer.

The sharing of STRs within financial groups could prompt the probing of a customer's activity in another jurisdiction, which might result in the identification of other suspicious activity or provide valuable additional information which would be able to be provided to the domestic FIU.

Terrorist financing. Terrorist financing is difficult to detect and can involve legal sources of funds. Transaction monitoring is likely to play a key role, particularly where customers that were assessed as higher risk (due to their transaction history and/or country of origin, for example) are involved.

An initial suspicion by a bank that a transaction may involve the financing of terrorism may be confirmed if further transactions with other banks within the financial group, involving the same customer or recipient of funds, are reported. 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.

In situations where terrorist financing is suspected it is essential that the reporting and sharing of relevant information occur without delay. The instant sharing of suspicious information within a financial group (and, if confirmed by the foreign subsidiary, branch, or affiliate, subsequent reporting to the foreign FIU) could be a critical factor in the prevention of a major terrorist incident.

Transnational crimes. As globalization has expanded international trade, the range of organized criminal activities has broadened and diversified. The traditional hierarchical forms of organized crime groups have diminished and have been replaced with loose networks who work together in order to exploit new market opportunities. For example, organized crime groups involved in drug trafficking are also commonly engaged in smuggling of other illegal goods.[15]

The increasing links between various categories of transnational organized crime call for a more integrated approach to address this nexus, including the receipt of information from and information exchange within a global financial group to unravel complex international financial transactions.

Convergence of fraud and money laundering. Reports from the financial sector indicate the increasing convergence of money laundering and large-scale fraud. As the use of banks to perpetrate massive fraud is becoming more prevalent, many banks are looking into combining their AML and fraud units.

[15] "UNODC and organized crime," www.unodc.org/unodc/en/organized-crime/index.html, accessed on June 7, 2010.

To effectively counter complex, multi-jurisdictional fraud, FIUs and law enforcement agencies will need to increasingly cultivate partnerships with banks for proactive initiatives and to enhance their understanding of sophisticated financial transactions. Banks' ability to share STRs within their financial groups may contribute greatly to their analytical efforts to detect fraud and protect banks and innocent customers.

Corruption. Proceeds of corruption are particularly likely to be transferred to a foreign jurisdiction, as corrupt officials both seek to conceal evidence of their crimes and facilitate escape should they be discovered. The ability to share STRs within a financial group would increase the chances of identifying such funds. At the same time, operational controls would be of critical importance for sharing corruption-related STRs in order to ensure that the STR subjects were not made aware of the STRs as a result of the activities of insiders within the financial group involved in the sharing of corruption-related STRs.

Possible Approaches to Facilitate Enterprise-wide STR Sharing

In order for enterprise-wide STR sharing to become a reality, approaches must be considered that both preserve the benefits and reduce the risks associated with sharing. This section presents potential approaches and the advantages, disadvantages, and governmental implications for each approach. In general, each of the approaches incorporates some limitation on sharing designed to reduce the potential for violation of STR confidentiality. These limitations may also reduce some of the benefits anticipated from sharing described previously in the paper.

The approaches are intended to serve as a starting point for jurisdictions to consider when implementing their own enterprise-wide STR sharing regime. The approaches presented below are not necessarily mutually exclusive. Jurisdictions may wish to consider a staged approach to STR sharing, beginning with an initial limited approach before moving on to a more wide-ranging approach.

Category of Offenses Approach

Under the category of offenses approach, enterprise-wide STR sharing would be permitted for suspicious transactions involving classes of criminal offenses. For example, this approach may include sharing STRs for transactions that involve (or appear to involve) severe offenses such as terrorist financing, nuclear arms proliferation, or the sale, distribution or creation of weapons of mass destruction. When a bank files an STR that involves such an offense, the bank would be permitted to share the STR within its financial group.

Advantages. The category of offenses approach allows FIUs to maintain a high degree of control over what types of STRs could leave the jurisdiction. By limiting sharing to STRs that implicate certain severe offenses, many of the perceived risks of enterprise-wide STR sharing could be mitigated since only a small number of STRs would leave the jurisdiction. Moreover, this approach would allow a financial group to implement enterprise-wide compliance procedures for those offenses that would be most detrimental to their legal and financial interests.

Disadvantages. Relative to the other approaches presented in this section, this approach does not guarantee the same degree of confidentiality and protection of STRs. The other approaches in this section incorporate limitations on the distribution of an STR, such as by jurisdiction or bank. Additionally, financial groups may view this approach as limiting their ability to implement enterprise-wide compliance programs because their STR sharing capabilities would be confined to certain offenses, rather than all reportable offenses. Therefore, financial groups may not be able to realize the full potential of enterprise-wide compliance. Also, from a legal or regulatory perspective, banks may have difficulty discerning which STR offenses permit cross-border sharing and which offenses do not permit sharing, depending on the level and quality of guidance provided by FIUs or regulators.

Furthermore, banks are often not in a position to judge accurately the nature of the underlying criminal activity of a suspicious transaction. While they may have a suspicion about a transaction, it is left to the

FIU or other competent authority to analyze the STR in combination with other information sources to evaluate relevance for possible criminal investigation. Whether this problem would result in underutilization or overutilization of STR sharing would be case specific. In some cases, the bank would lack information that would put the STR in the proper category of offense to allow sharing, and therefore an STR would not be able to be shared. In other cases, the bank might incorrectly suspect the activity to be in a covered category of offense, leading to STR sharing beyond the scope that was intended by the jurisdiction.

Implications for governments. This approach would likely require minimal investment by jurisdictions. Ultimately, the banks would have the burden of ensuring that the STR involves an offense for which sharing is permitted under the laws or regulations of where the STR was filed.

Limited Jurisdiction Approach

Under the limited jurisdiction approach, enterprise-wide STR sharing would be permitted on a case-by-case basis when the competent authority of a jurisdiction designates another jurisdiction as satisfactory for STR sharing purposes. For example, the FIU of Jurisdiction A would designate Jurisdiction B as having satisfactory laws or regulations in place so as to allow STR sharing. A bank located in Jurisdiction A could then share with its head office or a subsidiary, branch, or affiliate within the same financial group that is located in Jurisdiction B. Each jurisdiction would have its own set of criteria to evaluate whether or not to permit sharing with another jurisdiction. For example, a jurisdiction may consider the degree of confidentiality that will be afforded to a shared STR under the laws and regulations of another jurisdiction.

Advantages. The limited jurisdiction approach would give FIUs the ability to limit many of the potential risks involved with enterprise-wide STR sharing. A jurisdiction could either permit or prohibit banks from sharing STRs depending on the risks that another jurisdiction may pose. Additionally, banks may support the limited jurisdiction approach because the burden to determine which jurisdictions are permissible for sharing purposes falls on the competent authority, not the bank. This approach would also allow financial groups to implement enterprise-wide compliance programs across those jurisdictions where STR sharing is permitted.

Disadvantages. The process a jurisdiction uses to identify appropriate jurisdictions for sharing could become complex. Jurisdictions could consider defining strict, non-political considerations for STR sharing, such as FATF or FATF-style regional body mutual evaluations. However, a jurisdiction's process for determination may include political or foreign policy considerations. This problem may be particularly acute in the case that one jurisdiction allows STR sharing while the other jurisdiction does not.

As with the limited offense approach, the limitation of sharing to certain jurisdictions might prevent the full potential of enterprise-wide STR sharing from being realized.

Implications for governments. In implementing the limited jurisdiction approach, a competent authority would need to possess personnel with a high degree of expertise in foreign laws and regulations. Also, the competent authority would need to expend some effort in order to evaluate and re-evaluate the AML/ CFT regimes of foreign jurisdictions.

Case Study – France

France implemented the EU's Third Money Laundering Directive (Directive 2005/60/EC) with its new AML/CFT law of January 30, 2009. Following the framework of Directive 2005/60/EC, the French law imposes conditions on STR sharing within a group.

The French Monetary and Financial Code (CMF) stipulates that STRs are strictly confidential, with a few exceptions. One exception relates to information sharing within the same financial group.

According to Article L. 561-20 of the CMF, reporting entities which belong to the same group, to the same network, or to the same professional organization shall inform each other of the existence and contents of reports filed with TRACFIN, the French FIU. With respect to group-wide sharing, four conditions are defined:

- The exchange of information is made only inside the same group;
- The information is necessary for the due diligence of the group;
- The exchange of information is done with entities established in jurisdictions which have equivalent AML/CFT systems; and
- The exchange of information is done with entities established in jurisdictions which guarantee sufficient protection of privacy and fundamental rights and freedoms. A list of these jurisdictions has been established.

The third condition refers to a list of third jurisdictions which have equivalent AML/CFT obligations, which is drawn up by the Minister of Economy. In addition to EU and European Economic Area countries (Iceland, Liechtenstein, and Norway), this list includes the following jurisdictions: Argentina, Australia, Brazil, Canada, Hong Kong, Japan, Mexico, New Zealand, Singapore, South Africa, Switzerland, and the United States.

Limited Bank Approach

The limited bank approach would permit STR sharing when the competent authority of a jurisdiction designates a bank as having satisfactory policies, procedures, and controls for sharing within its financial group. A jurisdiction may choose to evaluate the relevant policies, procedures, and controls of the financial group as well. For example, a competent authority may designate Bank A as having sound

policies, procedures, and controls in place. The competent authority would then allow Bank A to share STRs within its financial group. In evaluating each bank, a competent authority may look at a number of matters. For instance, an authority may evaluate the controls that a bank has in place to ensure the confidentiality of the STR from one jurisdiction to another.

Advantages. The limited bank approach gives jurisdictions the ability to limit many of the potential risks associated with STR sharing. If a jurisdiction believes that the controls of a bank's compliance program are insufficient for permitting an STR to cross international borders, then the jurisdiction has the freedom of not permitting the dissemination of the STR outside of the jurisdiction.

Disadvantages. There may be difficulties associated with a competent authority labeling one bank's AML/CFT compliance program as suitable for STR sharing purposes, but another bank's program as inadequate. The characterization of AML/CFT compliance programs could create controversies and criticism for the competent authority. Moreover, this approach would limit the number of financial groups that could implement enterprise-wide AML/CFT compliance programs.

Jurisdictions may have difficulty in assessing a bank's head office, subsidiaries, branches, and affiliates in other jurisdictions in order to determine which banks are authorized to share. In such instances, a competent authority could not prevent a bank from sending an STR to its head office, a subsidiary, a branch, or an affiliate in a jurisdiction that is of high risk from the perspective of STR confidentiality. Even if a bank establishes appropriate controls such as information security protocols, this will not substitute for a lack of prevention under the laws of the jurisdiction of the receiving head office, subsidiary, branch, or affiliate. The entity receiving the STR might not be able to decline to produce it when the demand is made by a judicial, law enforcement, or other government entity.

Implications for governments. Under the limited bank approach, a competent authority would be required to have personnel with a high degree of expertise in evaluating and re-evaluating the sufficiency of a bank's AML/CFT compliance program for STR sharing purposes. The collection of relevant information on the financial group more broadly may prove difficult. Also, the approach may raise issues of competitive neutrality and regulatory equity, with the potential for legal challenges from affected reporting entities.

Case Study – Australia

Australian provisions regarding "tipping off" make the disclosure of STR information an offence unless one of the permitted exceptions applies. One of the exceptions applies to members of a "designated business group (DBG)."

Chapter 2 of the *Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007* (No. 1) details the following circumstances under which reporting entities may form a DBG:

- An entity is related to the other members of the DBG (e.g., where one is either a holding company or a subsidiary of the other company), and each member of the DBG is either a reporting entity, or a company in a foreign country that would be a reporting entity if it were resident in Australia; or
- The entities are providing a designated service under a joint venture agreement where each member of the DBG is a party to the joint venture agreement; or
- The entities meet the special requirements permitting accounting practices, legal practices or money services providers to form DBGs.

The principal purpose of forming a DBG is to allow certain obligations under Australia's AML/CTF legislation to be shared among members of the group. In some circumstances, a foreign related entity may be able to join a DBG, such as when it is a parent of one or more Australian entities or when it is a subsidiary of an Australian entity. The formation of DBGs is not restricted to the banking sector, as businesses in other sectors are also able to form and join DBGs.

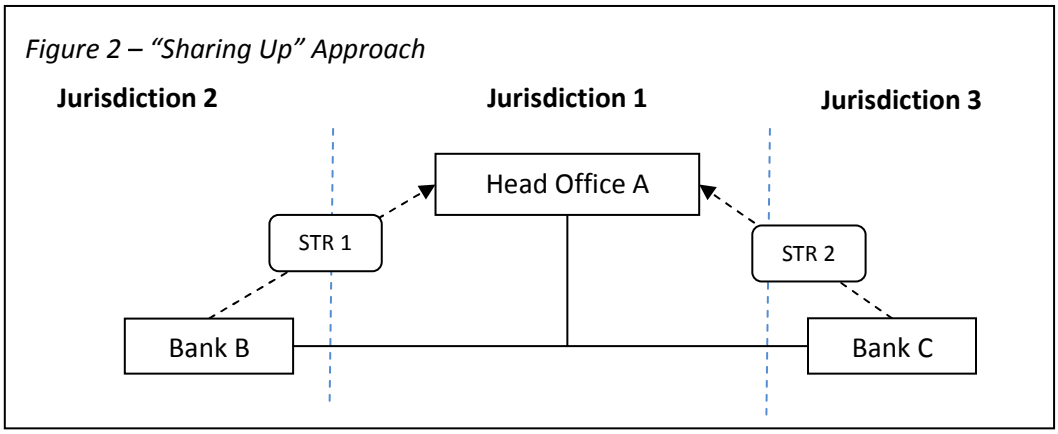
Creation of a DBG also permits the sharing of STR information among the DBG members. The requirements for sharing of STR information within a DBG are set out in section 123(7) of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006.*

Note that while Australia's concept of a designated business group has some similarities to the limited bank approach or potentially a hybrid approach, the Australian approach differs from the limited bank approach in that it does not involve a case-by-case approval of each DBG.

"Sharing Up" Approach

The sharing up approach would permit banks to "share up" to the head office for STR sharing purposes, even if it is located in another jurisdiction. For instance, in Figure 2 Banks B and C could share their STRs with their Head Office A. However, Head Office A would not be permitted to "share down" STRs that are filed by Bank B to Bank C or STRs that are filed by Bank C to Bank B.

Figure 2 – "Sharing Up" Approach



Advantages. The sharing up approach would be a strong endorsement by jurisdictions to promote the idea of enterprise-wide AML compliance. By allowing a head office to have access to STRs that are filed by banks within the financial group, it could implement an effective AML/CFT compliance program across the financial group. Furthermore, limiting sharing to only one direction would reduce the number of STRs that would be disseminated to foreign jurisdictions, lessening STR confidentiality issues.

Disadvantages. An FIU may not be able to control when a bank sends an STR to a foreign head office that is located in a jurisdiction that may be deemed high risk for STR confidentiality purposes. Furthermore, the inability of the head office to share down to its other banks may be viewed as an impediment to implementing an enterprise-wide AML/CFT compliance program. By preventing downward sharing, separate banks in the same financial group may not be able to realize some of the positive aspects of enterprise-wide STR sharing, such as improved suspicious transaction reporting and customer due diligence.

Implications for governments. As with the category of offenses approach, the sharing up approach would require minimal investment by jurisdictions. Ultimately, the bank would have the burden of ensuring that the confidentiality of the STR could be maintained in the foreign jurisdiction.

Case Study – United States

On January 20, 2006, the U.S. FIU, FinCEN, and four other U.S. banking regulators issued the document "Interagency Guidance on Sharing Suspicious Activity Reports with Head Offices and Controlling Companies." That guidance confirmed that under U.S. law and regulation, a U.S. branch or agency of a foreign bank may disclose an STR to its head office outside the United States. The document also confirmed that a U.S. depository institution may disclose an STR to controlling companies, whether domestic or foreign.

The 2006 guidance requires that a depository institution have written confidentiality agreements or arrangements in place specifying that the head office or controlling company must protect the confidentiality of the STRs through appropriate controls.

The recipient head office, controlling entities or parties may not disclose further any STR, or the fact that such a report has been filed. However, the institution may disclose without permission underlying information (that is, information about the customer and transaction(s) reported) that does not explicitly reveal that an STR was filed and that is not otherwise subject to disclosure restrictions.

Multilateral or Bilateral Agreement Approach

Under the multilateral or bilateral agreement approach, two or more jurisdictions would reach an agreement to permit STR sharing between banks of a financial group operating in their respective jurisdictions. The agreement would consist of many components to reduce or eliminate the risks and concerns of each individual jurisdiction. The language of the agreement could address such issues as the scope of sharing within a financial group, concerns regarding the confidentiality of the STR in a foreign jurisdiction, and other issues that may require clarification or assurance.

Advantages. This approach would give a jurisdiction the greatest degree of control in terms of reducing or eliminating potential risks associated with STR sharing. A jurisdiction would have a strong understanding and would receive assurances about what happens to an STR once it leaves its borders. The FIU of a jurisdiction could ensure that the confidentiality and integrity of the STR would remain intact even when the STR enters a foreign jurisdiction. This approach would likely be favored by banks because it reduces their burdens and liabilities involved with sending the STR into a foreign jurisdiction because such issues would be worked out in the agreement.

Disadvantages. This approach may require a considerable investment of time and effort by two or more foreign jurisdictions to reach an agreement on the conditions to permit STR sharing. Additionally, as with other approaches, a financial group's ability to implement an enterprise-wide AML/CFT compliance program may be limited if only those banks in jurisdictions that are subject to the multilateral or bilateral agreements are permitted to share with each other.

Implications for governments. As with many of the mentioned approaches, the multilateral or bilateral agreement approach would require jurisdictions to devote additional resources for the purposes of the administration of the system. Jurisdictions would be required to devote personnel with a high degree of expertise in the laws and regulations related to STR issues to negotiate with other foreign jurisdictions to reach an agreement.

Hybrid Systems

A number of the systems listed in this section of the paper could be combined to create a more ideal enterprise-wide STR sharing system. The following are some examples:

- The limited jurisdiction and limited bank approaches could be combined such that only certain banks could share STRs with their head office, another bank or a subsidiary, branch, or affiliate of that bank, as well as its own subsidiaries, branches and affiliates, within the same financial group and located in approved foreign jurisdictions.
- The category of offenses, limited jurisdiction, and limited bank approaches could all be combined such that certain banks could share STRs, as noted above in the combined limited jurisdiction and limited bank approaches, but for certain offenses only.

Most of the approaches mentioned in this section are flexible and the basic components of each approach could be combined to create an STR sharing system that could satisfy the needs and requirements of different jurisdictions.

Table 3: Approaches to Enterprise-wide STR Sharing

	Category of Offenses Approach – only certain severe offenses are allowed for STR sharing	**Limited Jurisdiction Approach** – only certain foreign jurisdictions would be permitted for STR sharing	**Limited Bank Approach** – only certain banks allowed to share STRs
Legal, regulatory, and policy considerations	Jurisdictions would need to review and, if required, amend their laws accordingly since many jurisdictions adopt different approaches with regards to the STRs submitted by their banks.		
	An international body or organization may need to develop a standard international requirement to allow cross-border STR sharing.		
	Jurisdictions would need to furnish guidelines and procedures for the STR sharing since this could potentially compromise the security of the information shared and issues of tipping off to other unrelated parties. Without clear guidelines to banks, the STR sharing may lead to tipping off or the unknowing violation of the compliance requirement.		
	Different jurisdictions will have different definitions of transnational crime.	There may be difficulty in making non-political determinations about the AML/CFT regimes of other jurisdictions.	There may be issues of competitive neutrality if some institutions can share while others cannot.
Resource considerations	Jurisdictions would need to make a determination on types of offenses that will be allowed for STR sharing.	Jurisdictions would need to assess other jurisdictions' AML/CFT regimes to ensure that only jurisdictions with effective AML/CFT regimes will be considered for STR sharing.	Jurisdictions would need to frequently conduct examinations on banks to ensure compliance for STR confidentiality purposes.
Additional considerations	Banks may have difficulties in STR sharing if the offenses are not well defined by the jurisdiction and also may also not be well placed to determine the underlying offense of an STR.	Different jurisdictions may have different confidentiality provisions which only allow sharing certain information (e.g., banking secrecy rules)	Jurisdictions may have difficulty in assessing the bank's head office, subsidiaries, branches, and affiliates in other jurisdictions in order to determine which domestic banks are authorized to share.

Table 3: Approaches to Enterprise-wide STR Sharing, cont.

	"Sharing Up" Approach – cross-border STR sharing would be allowed only to head offices	**Bilateral/Multilateral Agreement Approach** – Jurisdictions would enter into agreements to permit STR sharing
Legal, regulatory, and policy considerations	Jurisdictions would need to review and, if required, amend their laws accordingly since many jurisdictions adopt different approaches with regards to the STRs submitted by their banks.	
	An international body or organization may need to develop a standard international requirement to allow jurisdictions to allow cross-border STR sharing.	
	Jurisdictions would need to furnish guidelines and procedures for the STR sharing since this could potentially compromise the security of the information shared and issues of tipping-off to other unrelated parties. Without clear guidelines to banks, the STR sharing may lead to tipping off or unknowingly violate the compliance requirement.	
Resource considerations	This approach will require minimum investment by jurisdictions, as the burden of ensuring STR confidentiality in the foreign jurisdiction of the head office falls on the bank.	Jurisdictions would be required to devote personnel with a high degree of expertise in the laws and regulations related to STR issues to negotiate with other jurisdictions to reach an agreement.

Conclusion

The promise of more effective and efficient AML/CFT compliance through enterprise-wide, cross-border STR sharing can be realized only if individual jurisdictions can be assured that such sharing does not significantly increase the chance of the violation of STR confidentiality. Violation of confidentiality might occur unintentionally, through fraud or malfeasance, or intentionally, as part of a legal proceeding or sharing outside of traditional FIU channels. The benefits of STR sharing will mean little if the system of reporting suspicious transactions is undermined.

The survey of Egmont Group FIUs conducted in 2008 established that jurisdictions have a diverse set of laws, regulations, and policies on enterprise-wide STR sharing. Whether or not these policies have been put in place specifically to regulate STR sharing is not clear. It is true that in either case, the practical effect is the same. However, a jurisdiction that does not actively consider the issues surrounding enterprise-wide STR sharing when crafting an AML/CFT regime takes some risk. For example, a jurisdiction that does not allow sharing may be limiting its banks from understanding and reporting the full range of ML/TF risks. On the other hand, a jurisdiction that allows sharing without regard to the legal status of its STRs abroad risks the release of those STRs to the public.

The cross-border element of enterprise-wide STR sharing necessitates that jurisdictions coordinate their actions in this field. This paper puts forward five approaches for sharing, with the observation that a jurisdiction may be able to combine elements of the approaches into a "hybrid" approach. The paper does not endorse one approach over another, as it seems unlikely that a single approach will be most appropriate for all jurisdictions, given the diversity of AML/CFT regimes across the world. However, further study is needed to understand whether the implementation of different approaches by different jurisdictions would lead to an optimal result. Would the benefits to sharing be negated by a financial group's inability to navigate jurisdictions' varying and possibly conflicting mechanisms for permitting sharing?

Another key question for the future relates to the way financial group might share STRs. On one hand, financial groups might share STRs in a broad, passive way by allowing access by the head office, subsidiaries, branches, and affiliates to a common, shared database. With this method, a given subsidiary, branch, or affiliate might be aware of relevant STRs from another subsidiary, branch, or affiliate only if it sought them out. Alternatively, a financial group's mechanism for sharing might require a subsidiary, branch, or affiliate to actively direct an STR to another subsidiary, branch, or affiliate, such as through a secure e-mail system. The risks and benefits of STR sharing may depend on whether the sharing is primarily active or passive.

The present paper points to the need for a greater understanding of jurisdictions' policies regarding the protection of foreign STRs. Based on the results of the 2008 survey, it appears that in many jurisdictions, foreign STRs would not have the same protection from disclosure as domestic STRs.

The Egmont Group addressed the protection of foreign STRs in the context of FIU-to-FIU information exchange in 2001. The Egmont Group's "Principles for Information Exchange" indicate that "At a

minimum, exchanged information must be treated as protected by the same confidentiality provisions as apply to similar information from domestic sources obtained by the receiving FIU." Furthermore, the Principles also enshrine the concept of third-party dissemination requirements: "The requesting FIU may not transfer information shared by a disclosing FIU to a third party, nor make use of the information in an administrative, investigative, prosecutorial, or judicial purpose without the prior consent of the FIU that disclosed the information."[16]

Certainly, the Egmont Group's Principles for Information Exchange would not apply to the sharing of STRs within a financial group. Nonetheless, the two principles quoted above protect the confidentiality of foreign STRs and information revealing their existence, among other types of information. Analogous protections would likely be necessary in some form for enterprise-wide STR sharing to be successful.

FIUs have clear stakes in the issue of STR sharing, whether or not they possess regulatory powers themselves. By their very nature, FIUs cannot operate without a properly functioning suspicious transaction reporting system. A key concern is that of "territoriality," i.e., the idea that banks in any given jurisdiction must report STRs only to their domestic FIU. More broadly, FIUs will want to be certain that however their jurisdictions choose to handle STR sharing, any processes that are created do not interfere with existing, well-defined channels for the sharing of STRs, both between the FIU and private sector, as well as in the context of the Egmont Group.

[16] "Principles for Information Exchange Between Financial Intelligence Units for Money Laundering and Terrorism Financing Cases." Egmont Group, 13 June 2001, available at p. 2, http://www.egmontgroup.org/library/download/5.

Appendix: Egmont STR Sharing Survey

The text of the Egmont STR Sharing Survey is below, followed by a table summarizing the results of the survey.

Questions:

Enterprise-wide sharing (Please explain answers with relevant citations)

1. Does your jurisdiction allow for the sharing of STRs among different offices of a single corporate entity, domestically (for example, can a bank have one single compliance office maintaining all STRs for all domestic branches of the bank)?

   Yes _____ No_____

   Relevant Citations:_____

   1.a. If the above question referred to the information related to or underlying the STR and not the STR itself, would your answer be any different?

   Yes _____ No_____

If yes, please explain:
_____
_____
_____

   1.b. If the above example in parenthesis did not refer to banks, but rather to one or more different types of reporting entities, would your answer be any different?

   Yes _____ No_____

If yes, please explain:
_____
_____
_____

2. Does your jurisdiction allow for the sharing of STRs among different offices of different corporate entities under common ownership or control, domestically (for example, if a bank holding company owns multiple banks with separate legal personality, can the holding company have one single compliance office maintaining all STRs for all domestic branches of the different banks)?

   Yes _____ No_____

   Relevant Citations:_____

   2.a. If the above example in parenthesis did not refer to banks, but rather to one or more different types of reporting entities, would your answer be any different?

Yes _____ No_____

If yes, please explain:

_____
_____
_____

3. Does your jurisdiction allow for the sharing of STRs with a related corporate entity across jurisdictions (for example, (i) can a foreign bank with a branch in your jurisdiction share STRs with its headquarters or branches in other jurisdictions; (ii) can a bank headquartered in your jurisdiction share STRs with branches in other jurisdictions?[17]

Yes _____ No_____

Relevant Citations:_____

3.a. If the above question referred to the information related to or underlying the STR and not the STR itself, would your answer be any different?

Yes _____ No_____

If yes, please explain:

_____
_____
_____

3.b. If the above example in parenthesis did not refer to banks, but rather to one or more different types of reporting entities, would your answer be any different?

Yes _____ No_____

If yes, please explain:

_____
_____
_____

4. Does your jurisdiction allow for the sharing of STRs among different offices of different corporate entities under common ownership or control, across jurisdictions (for example, (i) can a foreign bank with a subsidiary in your jurisdiction share STRs among that subsidiary and its headquarters or affiliates in other jurisdictions; (ii) can a bank headquartered in your jurisdiction share STRs among that headquarters and subsidiaries in other jurisdictions)?

[17] Due to a typographical error, some FIUs received a version of the survey in which the word "related" in question 3 had been replaced by the word "unrelated." Therefore, the results related to question 3 should be interpreted with great caution.

Yes _____ No_____

Relevant Citations:_____

4.a. If the above question referred to the information related to or underlying the STR and not the STR itself, would your answer be any different?

Yes _____ No_____

If yes, please explain:

_____
_____
_____

4.b. If the above example in parenthesis did not refer to banks, but rather to one or more different types of reporting entities, would your answer be any different?

Yes _____ No_____

If yes, please explain:

_____
_____
_____

5. Does your jurisdiction allow for significant amounts of STRs originating in your jurisdiction to be moved for processing or storage in other jurisdictions (for example, can a depository institution store their STRs at a separate office in a foreign jurisdiction)?

Yes _____ No_____

Relevant Citations:_____

5.a. If the above question referred to the information related to or underlying the STR and not the STR itself, would your answer be any different?

Yes _____ No_____

If yes, please explain:

_____
_____
_____

5.b. If the above example in parenthesis did not refer to banks, but rather to one or more different types of reporting entities, would your answer be any different?

Yes _____ No_____

If yes, please explain:

_____
_____
_____

6. Are there any distinctions between allowable initial sharing of STRs and restrictions on further dissemination by the receiving entity?

Yes _____ No_____

Relevant Citations:_____

If yes, please explain:

_____
_____
_____

6.a. If the above question referred to the information related to or underlying the STR and not the STR itself, would your answer be any different?

Yes _____ No_____

If yes, please explain:

_____
_____
_____

Sharing among Unrelated Entities (Please explain answers with relevant citations)

7. Does your jurisdiction allow for the sharing of STRs among unrelated corporate entities, <u>domestically</u> (for example, if one bank detects a suspicious transaction, can it inform the other bank within the same jurisdiction involved in the transaction)?

Yes _____ No_____

Relevant Citations:_____

7.a. If the above question referred to the information related to or underlying the STR and not the STR itself, would your answer be any different?

Yes _____ No_____

If yes, please explain:

_____
_____
_____

8. Does your jurisdiction allow for the sharing of STRs among unrelated corporate entities, across jurisdictions (for example, if one bank detects a suspicious transaction, can it inform the other bank involved in the transaction, even if the other bank is in a different jurisdiction)?

Yes _____ No_____

Relevant Citations:_____

8.a. If the above question referred to the information related to or underlying the STR and not the STR itself, would your answer be any different?

Yes _____ No_____

If yes, please explain:

_____
_____
_____

9. Does your jurisdiction allow for any group to share of STRs (for example, the sharing of STR subjects among all members of a banking association)?

Yes _____ No_____

Relevant Citations:_____

9.a. If the above question referred to the information related to or underlying the STR and not the STR itself, would your answer be any different?

Yes _____ No_____

If yes, please explain:

_____
_____
_____

10. If the above examples in parentheses in the preceding three questions did not refer to banks, but rather to one or more different types of reporting entities, would your answers be any different?

Yes _____ No_____

Relevant Citations:_____

If yes, please explain:

_____
_____
_____

Sharing with Foreign Government Authorities

For the purposes of questions 11-13, please assume that STRs that originated in a foreign jurisdiction are brought by a financial institution into your jurisdiction, such as through sharing across jurisdictions among related corporate entities. (To clarify, these are NOT STRs that are subject to the reporting requirements of the FIU in your jurisdiction. They also have NOT been shared with your FIU by a counterpart FIU.)

11. Can a financial institution in your jurisdiction directly share STRs or related information with foreign government authorities other than an FIU, such as supervisors from a different jurisdiction (for example, can a branch or subsidiary in your jurisdiction share information with the supervisor of the jurisdiction of the headquarters of the corporate entity or holding company)?

    Yes _____ No_____

    11.a. Are the protections or prohibitions a matter of settled law in your jurisdiction?

    Yes _____ No_____

Please explain:

_____
_____
_____

12. Do the protections for STRs and prohibitions against disclosure in your jurisdiction depend upon or otherwise assume that they apply only with respect to required reporting entities in your jurisdiction, or to reports originated or filed there?

    Yes _____ No_____

13. Are there any differences with respect to the protections and prohibitions that might apply to foreign source STRs in judicial or administrative proceedings?

    Yes _____ No_____

If yes, please explain:

_____
_____
_____

14. Can a financial institution in your jurisdiction directly share STRs with an FIU of a different jurisdiction (for example, if your jurisdiction has suspicion regarding a transaction involving a foreign jurisdiction, in addition to reporting to your FIU, can that financial institution report to the FIU of the involved foreign jurisdiction)?

    Yes _____ No_____

Relevant Citations:_____

Privacy and Data Protection

15. Please briefly describe any other laws or policies in your jurisdiction relevant to the sharing of STRs, including with respect to privacy, data protection, and/or bank secrecy laws. Please provide relevant citations where applicable.

_____
_____
_____

16. Please describe any relevant exceptions to the application of such laws or policies allowing for the sharing of STRs, particularly with other jurisdictions. Please provide relevant citations where applicable.

_____
_____
_____

17. Are there any other options or authorities available, notwithstanding the limitations of such laws or policies, that would allow for the sharing or STRs in order to advance AML/CFT laws and policies?

Yes _____ No_____

If yes, please explain:

_____
_____
_____

General Questions:

18. Please provide any further comments on limitations of which you are aware in the sharing of a) STRs, and b) information underlying STRs in specific circumstances and/or with specific jurisdictions.

_____
_____
_____

19. Please provide comments on any related concerns of which you are aware from financial institutions that may limit their ability to operate an AML/CFT program on an enterprise-wide basis.

Results of Egmont STR Sharing Survey	Yes (%)	No (%)	Total FIUs Responding
Enterprise-wide Sharing			
1. Does your jurisdiction allow for the sharing of STRs among different offices of a single corporate entity, domestically (for example, can a bank have one single compliance office maintaining all STRs for all domestic branches of the bank)?	93%	7%	59
1.a. If the above question referred to the information related to or underlying the STR and not the STR itself, would your answer be any different?	8%	92%	59
1.b. If the above example in parenthesis did not refer to banks, but rather to one or more different types of reporting entities, would your answer be any different?	5%	95%	58
2. Does your jurisdiction allow for the sharing of STRs among different offices of different corporate entities under common ownership or control, domestically (for example, if a bank holding company owns multiple banks with separate legal personality, can the holding company have one single compliance office maintaining all STRs for all domestic branches of the different banks)?	42%	58%	57
2.a. If the above example in parenthesis did not refer to banks, but rather to one or more different types of reporting entities, would your answer be any different?	8%	92%	59
3. Does your jurisdiction allow for the sharing of STRs with a related[18] corporate entity across jurisdictions (for example, (i) can a foreign bank with a branch in your jurisdiction share STRs with its headquarters or branches in other jurisdictions; (ii) can a bank headquartered in your jurisdiction share STRs with branches in other jurisdictions?	44%	56%	59
3.a. If the above question referred to the information related to or underlying the STR and not the STR itself, would your answer be any different?	25%	75%	60
3.b. If the above example in parenthesis did not refer to banks, but rather to one or more different types of reporting entities, would your answer be any different?	5%	95%	59
4. Does your jurisdiction allow for the sharing of STRs among different offices of different corporate entities under common ownership or control, across jurisdictions (for example, (i) can a foreign bank with a subsidiary in your jurisdiction share STRs among	40%	60%	55

[18] Due to a typographical error, some FIUs received a version of the survey in which the word "related" in question 3 had been replaced by the word "unrelated." Therefore, the results related to question 3 should be interpreted with great caution. The results from question 3 were not used in section 3 or any other part of this paper.

	that subsidiary and its headquarters or affiliates in other jurisdictions; (ii) can a bank headquartered in your jurisdiction share STRs among that headquarters and subsidiaries in other jurisdictions)?			
4.a.	If the above question referred to the information related to or underlying the STR and not the STR itself, would your answer be any different?	14%	86%	58
4.b.	If the above example in parenthesis did not refer to banks, but rather to one or more different types of reporting entities, would your answer be any different?	5%	95%	58
5.	Does your jurisdiction allow for significant amounts of STRs originating in your jurisdiction to be moved for processing or storage in other jurisdictions (for example, can a depository institution store their STRs at a separate office in a foreign jurisdiction)?	27%	73%	56
5.a.	If the above question referred to the information related to or underlying the STR and not the STR itself, would your answer be any different?	7%	93%	55
5.b.	If the above example in parenthesis did not refer to banks, but rather to one or more different types of reporting entities, would your answer be any different?	2%	98%	54
6.	Are there any distinctions between allowable initial sharing of STRs and restrictions on further dissemination by the receiving entity?	15%	85%	53
6.a.	If the above question referred to the information related to or underlying the STR and not the STR itself, would your answer be any different?	2%	98%	53
Sharing among Unrelated Entities				
7.	Does your jurisdiction allow for the sharing of STRs among unrelated corporate entities, domestically (for example, if one bank detects a suspicious transaction, can it inform the other bank within the same jurisdiction involved in the transaction)?	25%	75%	59
7.a.	If the above question referred to the information related to or underlying the STR and not the STR itself, would your answer be any different?	11%	89%	57
8.	Does your jurisdiction allow for the sharing of STRs among unrelated corporate entities, across jurisdictions (for example, if one bank detects a suspicious transaction, can it inform the other bank involved in the transaction, even if the other bank is in a different jurisdiction)?	24%	76%	59
8.a.	If the above question referred to the information related to or underlying the STR and not the STR itself, would your answer be any different?	9%	91%	58
9.	Does your jurisdiction allow for any group to share of STRs (for example, the sharing of STR subjects among all members of a banking association)?	10%	90%	59

9.a.	If the above question referred to the information related to or underlying the STR and not the STR itself, would your answer be any different?	7%	93%	57
10.	If the above examples in parentheses in the preceding three questions did not refer to banks, but rather to one or more different types of reporting entities, would your answers be any different?	7%	93%	57
Sharing with Foreign Government Authorities[19]				
11.	Can a financial institution in your jurisdiction directly share STRs or related information with foreign government authorities other than an FIU, such as supervisors from a different jurisdiction (for example, can a branch or subsidiary in your jurisdiction share information with the supervisor of the jurisdiction of the headquarters of the corporate entity or holding company)?	22%	78%	59
11.a.	Are the protections or prohibitions a matter of settled law in your jurisdiction?	71%	29%	56
12.	Do the protections for STRs and prohibitions against disclosure in your jurisdiction depend upon or otherwise assume that they apply only with respect to required reporting entities in your jurisdiction, or to reports originated or filed there?	56%	44%	54
13.	Are there any differences with respect to the protections and prohibitions that might apply to foreign source STRs in judicial or administrative proceedings?	12%	88%	52
14.	Can a financial institution in your jurisdiction directly share STRs with an FIU of a different jurisdiction (for example, if your jurisdiction has suspicion regarding a transaction involving a foreign jurisdiction, in addition to reporting to your FIU, can that financial institution report to the FIU of the involved foreign jurisdiction)?	8%	92%	59
Privacy and Data Protection				
15.	Please briefly describe any other laws or policies in your jurisdiction relevant to the sharing of STRs, including with respect to privacy, data protection, and/or bank secrecy	n/a		

[19] The survey included the following note with respect to questions 11-13: "For the purposes of questions 11-13, please assume that STRs that originated in a foreign jurisdiction are brought by a financial institution into your jurisdiction, such as through sharing across jurisdictions among related corporate entities. (To clarify, these are NOT STRs that are subject to the reporting requirements of the FIU in your jurisdiction. They also have NOT been shared with your FIU by a counterpart FIU.)"

	laws. Please provide relevant citations where applicable.			
16.	Please describe any relevant exceptions to the application of such laws or policies allowing for the sharing of STRs, particularly with other jurisdictions. Please provide relevant citations where applicable.	n/a		
17.	Are there any other options or authorities available, notwithstanding the limitations of such laws or policies, that would allow for the sharing or STRs in order to advance AML/CFT laws and policies?	15%	85%	52
General Questions				
18.	Please provide any further comments on limitations of which you are aware in the sharing of a) STRs, and b) information underlying STRs in specific circumstances and/or with specific jurisdictions.	n/a		
19.	Please provide comments on any related concerns of which you are aware from financial institutions that may limit their ability to operate an AML/CFT program on an enterprise-wide basis.	n/a		