PREPARED REMARKS OF BESS MICHAEL
ASSOCIATE DIRECTOR, INTERNATIONAL PROGRAMS DIVISION
FINANCIAL CRIMES ENFORCEMENT NETWORK
U.S. DEPARTMENT OF THE TREASURY

DELIVERED AT THE
INSTITUTE OF INTERNATIONAL BANKERS
ANNUAL ANTI-MONEY LAUNDERING SEMINAR
MAY 23, 2011

Introduction

Today I would like to speak about two distinct issues, both involving international information exchange, and analogies that one may draw between the two issues. First, I will describe some ongoing developments in FinCEN's work with its direct foreign counterparts, known as financial intelligence units (FIUs) and the Egmont Group of FIUs. I hope that this will give you a better sense of how governments around the world use the information that your institutions report to FinCEN to counter financial crime.

Second, I will say a few words about the enterprise-wide sharing of suspicious transaction reports (STRs), and in particular highlight some work done by the Egmont Group on this issue. Finally, I would like to look at the two issues side by side to see how the sharing of STRs and other information *among FIUs* compares with similar sharing done by *a single enterprise* operating across jurisdictions.

Information Exchange among Financial Intelligence Units

Last year, during his address to this conference, FinCEN Director Freis spoke about FinCEN's tripartite mission and its three business lines. He identified international cooperation as one of FinCEN's three main mission areas. The bulk of that cooperation occurs in the context of FinCEN's function as the U.S. financial intelligence unit, or FIU.

FinCEN collaborates with a broad international network of FIUs comprising the Egmont Group. FIUs and the Egmont Group have evolved over the past decade. When FinCEN was created in 1990 through an order of Secretary of the Treasury Nicholas Brady, only two other countries (Australia and the United Kingdom) had FIUs. In 1995, a group of like-minded government agencies and international organizations met at the Egmont-Arenberg Palace in Brussels, Belgium, to discuss operational issues that they had in common, and the Egmont Group of FIUs was born.

Today many jurisdictions around the globe have established an FIU as a core component of an AML/CFT regime. The expansion of FIUs has been promoted through the incorporation of the FIU concept into the standards of the Financial Action Task Force and the Egmont Group. As a reflection of the growing importance of FIUs, consider that the Egmont Group's membership has expanded from just 15 FIUs in 1995 to 53 in 2000 to 120 in 2011.

During the past sixteen years, the Egmont Group has developed mechanisms for the rapid exchange between FIUs of sensitive information across borders. Over the years, Egmont Group members have agreed upon a common framework for information exchange. This framework begins with a shared vision – an internationally accepted definition – of an FIU that serves as a national, central authority that receives, analyzes, and disseminates disclosures of financial information, particularly STRs to combat money laundering and terrorist financing.[1] FIUs share sensitive information with other FIUs in accordance with two key Egmont documents, "Principles of Information Exchange" and "Best Practices for the Exchange of Information." These documents promote the confidentiality of FIU-related information.

On a technical level, Egmont Group FIUs exchange information between themselves via a secure system known as the Egmont Secure Web, which is managed by FinCEN on behalf of the Egmont Group. FIUs use the Egmont channel for information sharing in support of thousands of law enforcement cases per year. In fiscal year 2010, FinCEN alone closed 1,100 incoming cases from FIUs and referred almost 590 requests to 84 FIUs on behalf of U.S. law enforcement and regulatory agencies.[2]

Just as the Egmont Group has expanded in terms of its global reach, so have its constituent FIUs been growing in sophistication. Established FIUs assist newly formed FIUs, both through a rigorous process of sponsorship for admission to the Egmont Group, through the efforts of an active Egmont working group focused on FIU-specific training and on a bilateral basis. At the same time, all FIUs have been building on their experiences to refine their analysis of the financial information that they receive from reporting entities like those that you represent. FIUs match the suspicious transaction reports and other reports such as cash transaction reports that reporting entities provide with commercial, administrative, and law enforcement information to determine potential financial criminal activity for law enforcement to investigate at a tactical level.

In addition to their traditional role in supporting existing law enforcement investigations on a reactive basis, FIUs are increasingly proactively sharing information with each other and developing strategic analyses to identify trends and patterns of money laundering/terrorist financing based on the information that FIUs possess or have access to. But in how many cases

---

[1] For the exact text of the Egmont Group's definition of an FIU as well as a detailed discussion, see "Interpretive Note Concerning the Egmont Definition of a Financial Intelligence Unit," available at http://www.egmontgroup.org/library/download/8.

[2] "FinCEN Annual Report," Fiscal Year 2010, p. 52, available at http://www.fincen.gov/news_room/rp/files/annual_report_fy2010.pdf

do multiple FIUs hold different pieces of a puzzle and not know it? Proactive cooperation among FIUs on both the tactical and strategic levels seeks to explore overlap in FIUs' data sets.

FinCEN and the global FIU community have evolved over time. Just last year, FinCEN celebrated its twentieth anniversary. While I think we'd all agree personally that twenty years is quite a long time, FinCEN and the rest of the world's FIUs are still relatively young when considered as functional elements of governments. We are seeing a tendency of more and more jurisdictions to transform police FIUs into administrative units to enhance collaboration with the financial sector. More and more FIUs are taking on regulatory functions for AML/CFT purposes over sectors not already supervised. With all of the changes in the international community of FIUs to date, I am certain that this system of information sharing and collaboration will continue to evolve.

Enterprise-wide STR Sharing

Let us turn our attention from information exchange among the governments of multiple jurisdictions – that is, among FIUs – to an issue of information exchange among the parts of an individual financial enterprise operating in multiple jurisdictions. Specifically, I would like to talk about the issue of enterprise-wide STR sharing. This term, as you undoubtedly know, refers to the sharing of STRs among the components of a financial enterprise or financial group operating in multiple jurisdictions.

I suspect that you are also aware of FinCEN's November 2010 guidance documents regarding the sharing of suspicious activity reports, particularly the document focused on depository institutions. That document reiterated FinCEN's view that,

> [T]he sharing of a SAR or, more broadly, any information that would reveal the existence of a SAR, with a head office or controlling company (including overseas) promotes compliance with the applicable requirements of the BSA by enabling the head office or controlling company to discharge its oversight responsibilities with respect to enterprise-wide risk management, including oversight of a depository institution's compliance with applicable laws and regulations.[3]

However, it is important to emphasize that a depository institution sharing with its head office or controlling company must have written confidentiality agreements or arrangements in place specifying that the head office or controlling company must protect the confidentiality of Suspicious Activity Reports through appropriate internal controls.[4]

---

[3] "Sharing Suspicious Activity Reports by Depository Institutions with Certain U.S. Affiliates," November 23, 2010, p. 2, available at http://www.fincen.gov/statutes_regs/guidance/pdf/fin-2010-g006.pdf.

[4] "Interagency Guidance on Sharing Suspicious Activity Reports with Head Offices and Controlling Companies," January 20, 2006, p. 2, available at http://www.fincen.gov/statutes_regs/guidance/pdf/sarsharingguidance01122006.pdf.

With respect to sharing SARs with domestic affiliates, the guidance limits sharing to circumstances where the receiving affiliate is subject to a SAR regulation. As FinCEN noted in issuing the November 2010 guidance, "the need to prevent a SAR from becoming subject to the laws of a foreign jurisdiction significantly outweighs any limited need for a foreign affiliate to obtain SAR information."[5]

In the context of international cooperation on the issue of enterprise-wide STR sharing, I would draw your attention to the Egmont Group's February 2011 paper "Enterprise-wide STR Sharing: Issues and Approaches."[6] This paper was the result of the collaboration of a small group of FIUs, led by FinCEN. Naturally, the paper approaches the issue from the perspective of FIUs, which are primarily operational rather than policy-making bodies. FIUs have an inherent interest that STRs are kept confidential by reporting entities while fully incorporating all information available to those entities.

The paper begins with the results of a 2008 Egmont Group-wide survey of approximately 60 FIUs regarding the treatment of enterprise-wide STR sharing in their jurisdictions. The paper then discusses both the risks and potential benefits of sharing. Finally, the paper presents a series of alternative approaches jurisdictions could consider in seeking to facilitate the sharing of STRs across borders. If you are not familiar with the Egmont paper, I would encourage you to take a look at it.

While it is impossible to talk about all aspects of the paper here, perhaps I can give you a flavor for the paper by highlighting two questions raised in its conclusion. First, as jurisdictions begin to adjust their AML/CFT regimes to allow sharing of STRs across borders, is it possible that different jurisdictions could adopt different approaches to STR sharing, thereby undermining any potential gains in efficiency associated with enterprise-wide sharing? Second, how are institutions likely to engage in sharing of STRs and what are the implications? Specifically, will institutions more likely engage in occasional sharing of individual STRs on a case-by-case basis or wholesale transfers of entire databases or data sets? What is the impact of the method used to share STRs across borders on the risks and benefits of sharing?

Comparing FIU-to-FIU Information Exchange with Enterprise-wide STR Sharing

I now want to focus on information sharing in these two situations – first, among FIUs, and second, among a single enterprise in numerous jurisdictions. These scenarios are, to be sure, different circumstances. But perhaps thinking through the similarities and differences will highlight particular issues with respect to enterprise-wide STR sharing and allow us to think about it in a different way.

The most obvious place to start is that both FIU-to-FIU information exchange and enterprise-wide STR sharing involve the sharing of highly sensitive information for analytical purposes in an effort to detect potential financial crime. As you know, the confidentiality of

[5] 75 FR 75609 (Dec. 3, 2010), available at http://edocket.access.gpo.gov/2010/pdf/2010-29884.pdf.
[6] Egmont Group, "Enterprise-wide STR Sharing: Issues and Approaches," available at http://www.egmontgroup.org/library/egmont-documents

STRs is critical in protecting the subject of the report, the financial institution and its staff, and the integrity of law enforcement investigations. The analysis that results from sharing information, whether a financial institution's STR or an FIU's intelligence report, becomes an input for another actor in the broader AML/CFT system.

Both situations involve information crossing international borders. To be more precise, both situations involve the transfer of information from the control of an entity operating under the laws of one jurisdiction to an entity operating under or subject to the laws of one or more jurisdictions. As such, both situations raise important challenges of international cooperation, though in somewhat different ways.

In both cases, the need to share information across borders arises from the fact that the individual entities, while working toward the common goal of fighting financial crime, directly receive only incomplete information about potential financial crime involving different jurisdictions. Those engaged in financial crime are not limited by international borders, and surely in some cases they use international borders to their advantage, knowing the challenges that can arise in international cooperation.

In the absence of sharing, elements of a financial group have no knowledge that particular activities or transactions have been judged suspicious by co-workers in other jurisdictions. Similarly, while the FIU is, by design, able to consolidate information from many domestic sources, including all reporting entities and many government agencies, it does not automatically receive STRs from other jurisdictions. Both FIUs and the individual components of a financial group or enterprise are at a disadvantage when cut off from the full spectrum of available and relevant information.

What, then, are the differences between the two situations and what can that tell us about enterprise-wide STR sharing?

First, for the purposes of information sharing, the global network of FIUs is vast but in many ways simpler in structure than a global financial group. The international definition of an FIU specifically allows only one FIU per jurisdiction. For example, FinCEN's point of contact within a given jurisdiction for information exchange is always a single entity.[7] From the perspective of an FIU, most information exchange within the FIU network occurs through a series of bilateral relationships. A global financial group, by contrast, could consist of an interlocking web of corporate structures; defining the extent of the organization for the purposes of enterprise-wide AML/CFT compliance may be a complex exercise. As a result of this difference, it seems reasonable to conclude that the FIU-to-FIU channel may be in some ways more easily controlled and possibly more centralized.

Second, within the context of the Egmont Group, the decision to exchange information about a particular individual or transaction is generally made on a case-by-case basis. An FIU

[7] In a few cases, an FIU might exist in a jurisdiction that is in some way part of a larger jurisdiction. For example, the Isle of Man has an FIU different from that of the United Kingdom, even though the Isle of Man is a British crown dependency.

does not simply upload its STRs and other information to a common database for all other FIUs to query as they see fit. Rather, an FIU considers each exchange separately, with an individual actively determining what to share with the counterpart FIU. While it is not entirely clear, it is possible to imagine enterprise-wide STR sharing occurring in a far more automatic fashion, for example through the use of a shared database.

A final difference is that there is an existing international framework governing the exchange of information among FIUs, while such a system does not currently exist in the context of financial groups operating in multiple jurisdictions. With respect to FIU-to-FIU exchange, the Egmont Group's "Principles of Information Exchange" provides a framework to address the challenges of international cooperation that arise. Indeed, facilitating this type of information exchange is one of the primary goals of the Egmont Group.

The Egmont Group's "Principles of Information Exchange" consists of thirteen points that scarcely fill both sides of a single sheet of paper.[8] Nonetheless, they have proven to be a powerful tool for FIUs. Key among these points is the notion that information exchange be based on a foundation of mutual trust, reciprocity and confidentiality. The text also addresses quite specifically how FIUs must protect information that has been received from other FIUs. Allow me to quote in full just two of the thirteen principles:

> 12. 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.
> 13. All information exchanged by FIUs must be subjected to strict controls and safeguards to ensure that the information is used only in an authorized manner, consistent with national provisions on privacy and data protection. 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.[9]

FIUs, therefore, must subject foreign STRs or information derived from those STRs to the same confidentiality requirements that hold for domestic STRs. What is the mechanism for enforcement of this requirement? Essentially, it is a matter of trust, reciprocity, and a commitment to shared standards. FIUs that provide information, meanwhile, inevitably have either the formal responsibility or simply an interest in ensuring that their own information is protected, particularly with respect to STRs.

When we speak of enterprise-wide STR sharing, however, there is no analogous common international framework to protect STRs from disclosure when they have been transferred to a foreign jurisdiction. FATF Recommendation 14 indicates, in part, that financial institutions, their

---

[8] Egmont Group, "Principles of Information Exchange," available at http://www.egmontgroup.org/library/download/5.
[9] Egmont Group, "Principles of Information Exchange," available at http://www.egmontgroup.org/library/download/5.

directors, officers and employees should be "…[p]rohibited by law from disclosing the fact that a suspicious transaction report or related information is being reported to the FIU."

However, it is not at all clear that all individual jurisdictions' laws and regulations implementing Recommendation 14 apply to "foreign" STRs or related information, that is, STRs that have been filed in one jurisdiction and shared with an entity in another. Indeed, the research conducted in the context of the Egmont Group paper I spoke of earlier indicates that such STRs in some cases would not be protected from disclosure,[10] a troubling development.

Conclusion

Let me conclude with some comments on how the Egmont Group experience may have some relevance for enterprise-wide STR sharing. In the Egmont context written rules have proven to be a necessary but not sufficient condition for ensuring the appropriate handling of sensitive information. Notwithstanding the application of the Egmont "Principles of Information Exchange" to our interactions with other FIUs, FinCEN has bilateral relationships with all FIUs grounded in reciprocity, trust, and confidentiality. That trust includes not simply a promise by the FIU to ensure that it protects the information, but also that it will ensure that authorized recipients protect the information.

Earlier I referred to FIU-to-FIU exchange and enterprise-wide STR sharing as "challenges for international cooperation." I would like to return to that point. Government-to-government cooperation underpins the Egmont Group, but it is also critical to the success of enterprise-wide STR sharing. In the end, it is governments that bear the ultimate responsibility for enforcing rules on the confidentiality of STRs. Therefore, any successful arrangement that allows an STR and related information to leave one jurisdiction for another necessarily involves government-to-government cooperation, whether explicit, implicit, or both.

Similarly, government-private sector collaboration is crucial to any FIU and an enterprise-wide STR sharing regime. In a globalized financial world, I would suggest that the usual term "public-private partnership" may understate the case, in that it does not place enough emphasis on the cross-border nature of efforts to fight financial crime. What we are really talking about is the cooperation of a collection of governments and, at least with respect to internationally active banks, private sector entities that operate across jurisdictional lines. We count on you and your colleagues to continue working with us to protect the integrity of the international financial system from abuse by money launderers and terrorists.

###

[10] Egmont Group, "Enterprise-wide STR Sharing: Issues and Approaches," p. 14, available at http://www.egmontgroup.org/news-and-events/news/2011/02/03/str-sharing-white-paper.