



PREPARED REMARKS OF JAMES H. FREIS, JR.

DIRECTOR, FINANCIAL CRIMES ENFORCEMENT NETWORK

**10TH ANTI-MONEY LAUNDERING AND FINANCING TERRORISM INTERNATIONAL
SEMINAR**

**PROMOTING INFORMATION SHARING IN OUR GLOBAL ANTI-MONEY
LAUNDERING/COUNTERTERRORISM FINANCE EFFORTS**

ACAPULCO, MEXICO

OCTOBER 9, 2008

Good morning. It is a pleasure to join you all today for the Mexico Bankers Association's 10th Anti-Money Laundering and Financing Terrorism International Seminar. It is an honor to be back in Mexico following my visit in February of this year when the Financial Crimes Enforcement Network (FinCEN) and the Unidad de Inteligencia Financiera (UIF), the Mexican financial intelligence unit, co-hosted a training seminar for Central American Egmont financial intelligence unit (FIU) members in Mexico City.

As the FIU for the United States, FinCEN values the strong relationships we have developed with our counterparts, and Mexico has been no exception. FinCEN's work with Mexico in co-sponsoring the training event in February is but one example of the mutual commitment and deep level of cooperation between our two countries.

Beyond our shared border, our countries share many common interests. The financial regulatory issues we face in the United States are similar in many ways to the experiences of our Mexican counterparts. Our respective governments both recognize the importance of a strong partnership among the public and private sectors to achieve our common goal of countering criminal abuse of the financial system, including terrorist financing. Our countries also both understand the importance of leveraging commercial incentives as a part of a strong public-private partnership, from which both the government and the financial industry benefit.

In these times of volatility in the financial market, it is important that we not lose sight of our anti-money laundering/counterterrorist financing (AML/CFT) responsibilities. Recent events have only underscored the relevance of the AML/CFT framework common to our countries. First, traditional distinctions between different financial industry sectors such as banking and securities markets have become increasingly blurred. Second, the global interconnections of the financial markets are beyond dispute. Third, there is a renewed focus on knowing one's customer for assessing creditworthiness and risks of fraud. These commercial incentives can and should be leveraged to carry out AML/CFT responsibilities.

Criminals and terrorists do not respect the law; they certainly do not respect national borders. They will seek to exploit the weakest link to move and launder money through any means of financial intermediation. Our joint efforts to root out illicit financial activity increase confidence in and promote the integrity and stability of the financial system. These are critical contributions to helping the banking system return to what it does best, i.e. promoting legitimate economic activity and growth.

When I was last in Mexico in February, I had the opportunity to meet with members of the Mexican Bankers Association where we discussed several issues of mutual interest and concern, including the sharing of reports of suspicious activity across borders. We have been working in the United States on this issue and I'd like to focus my remarks today on some of the efforts we have under way to improve the efficiency and effectiveness of our suspicious transaction reporting regime in support of our global counterterrorism and anti-money laundering efforts. The Mexican banking industry is in significant part affiliated with global entities. The issues I will be addressing today are directly relevant to globally active banks.

Specifically, I would like to outline two proposals that FinCEN is currently finalizing that are intended to clarify further the confidentiality provisions applicable within the United States to suspicious activity reporting under the Bank Secrecy Act (BSA). I will discuss some efforts we are undertaking globally to learn more from our partner countries about limitations or possible impediments to sharing of information. In closing, I will address the benefits of sharing information among financial institutions, which is a program we have in place in the United States and which is also nearing a reality in Mexico, as well as ongoing collaborative efforts between our two countries.

Suspicious Activity Reporting Initiatives

Turning first to the Suspicious Activity Report ("SAR") issues that we are working on in the United States, we will soon be taking two steps to clarify the confidentiality of SARs and at the same time permit certain sharing of SARs within a corporate organizational structure to promote greater enterprise-wide risk management. The first step entails issuing a proposed rule to update our regulations on SAR confidentiality. When finalized, these updates will clarify, among other things, the scope of the statutory prohibition against the disclosure by a financial institution or by a government agency of a SAR or any information that would reveal the existence of a

SAR. The second step entails proposing guidance to accompany the new rule change. This guidance will clarify that for certain financial institutions the sharing of a SAR with a domestic affiliate is consistent with the purposes of the BSA (including the confidentially provisions) and will therefore be permitted. Before going into more specifics about these proposals, let me provide some background.

In the United States, FinCEN was established in 1990 as an office within the Department of the Treasury.¹ It was under the USA PATRIOT Act of 2001, however, that its functions were statutorily formalized as a bureau within the Treasury Department.² FinCEN's responsibilities to receive, analyze, disseminate, and safeguard financial intelligence for the purposes of anti-money laundering and combating the financing of terrorism ("AML/CFT") and to coordinate with foreign FIUs were codified into law.³

In our role as the FIU for the United States, FinCEN, through BSA authority delegated by the Secretary of the Treasury, may require financial institutions to keep records and file reports that FinCEN determines to have a high degree of usefulness in criminal, tax, regulatory, and counter-terrorism investigations or proceedings.⁴ Within this framework, FinCEN may require financial institutions to file SARs, and has issued rules implementing that specific authority.

¹ Treasury Order 105-08, "Establishment of the Financial Crimes Enforcement Network," (April 25, 1990).

² See Treasury Order 180-01, "Financial Crimes Enforcement Network," (September 26, 2002), art. 1 ("By virtue of the USA PATRIOT Act of 2001 (Pub. L. No. 107-56, Title III, Subtitle B, Section 361(a)(2), 115 Stat. 272, 329-332), and by the authority vested in me as Secretary of the Treasury, it is hereby ordered that the Financial Crimes Enforcement Network ("FinCEN" or the "Bureau") is re-established as a bureau within the Department.").

³ See 31 U.S.C. § 310(b) Director.—

(1) Appointment.— The head of FinCEN shall be the Director, who shall be appointed by the Secretary of the Treasury.

(2) Duties and powers.— The duties and powers of the Director are as follows:

(B) Maintain a government-wide data access service, with access, in accordance with applicable legal requirements, to the following:

(i) Information collected by the Department of the Treasury, including report information filed under subchapter II of chapter 53 of this title (such as reports on cash transactions, foreign financial agency transactions and relationships, foreign currency transactions, exporting and importing monetary instruments, and suspicious activities)

(C) Analyze and disseminate the available data . . . to—

(i) identify possible criminal activity to appropriate Federal, State, local, and foreign law enforcement agencies;

(v) determine emerging trends and methods in money laundering and other financial crimes;

(vi) support the conduct of intelligence or counterintelligence activities, including analysis, to protect against international terrorism; and

(vii) support government initiatives against money laundering.

(H) Coordinate with financial intelligence units in other countries on anti-terrorism and anti-money laundering initiatives, and similar efforts.

⁴See 31 U.S.C. § 5311

The Importance of SAR Confidentiality

Under our regulations in the United States, the filing of SARs has always been considered confidential.⁵ Similarly, any information that would reveal the existence of a SAR is also confidential.⁶ Unauthorized disclosure of a SAR filing is a federal criminal offense.⁷ However, despite the widespread treatment of SARs as highly confidential documents, FinCEN's current regulations only expressly reference the prohibited disclosure of a SAR to "any person involved in the transaction." At times, this language in our rules has led to some confusion. Nevertheless, U.S. courts have upheld the general confidentiality of SARs, noting that disclosure to any outside party may make it likely that SAR information would be disclosed to a person involved in the transaction. In the context of discovery in civil lawsuits, these courts have concluded that financial institutions are prohibited from disclosing a SAR or information that would reveal the existence of a SAR.⁸ Our proposed rule will clarify this absolute confidentiality of SARs. It will also include updated language reflecting recent statutory provisions prohibiting disclosure by government agencies.

I want to emphasize that confidentiality is a crucial component to the open sharing of information from banks to the government. It is also important to note that SAR reports are not evidence. Rather, they are lead information, which in some cases can be the first tip that starts an investigation. A financial institution employee's good instincts can, and do, result in the contribution of critical information that serves to set investigatory wheels in motion to track down suspected criminal activity. Our forthcoming proposal will reaffirm our commitment to the financial industry to protect this sensitive commercial and personal information.

Allowing SAR Sharing Among Affiliates

FinCEN and its U.S. regulatory colleagues have long recognized that in order to discharge their oversight responsibilities for enterprise-wide risk management, financial institutions required to file SARs may need to share the SARs, or information about the SARs, within their corporate structure. For example, head offices, controlling entities or parties, or parent entities, may have a valid need to review an internal unit's compliance with legal requirements to identify and report suspicious activity.

Although the sharing of information underlying the filing of a SAR generally has never been prohibited under the BSA, it is understood that the sharing of a SAR itself may entail greater efficiency. Industry has repeatedly told us of the impracticality of being able to share only the underlying information regarding a report of suspicious activity. FinCEN currently affords "safe harbor" for the sharing of such information between institutions, as it relates to money laundering or terrorist financing, under its

⁵ See 31 U.S.C. § 103.18 (e)

⁶ See 31 U.S.C. § 5318 (g) (2)

⁷ See 31 U.S.C. § 5318 (g) (3)

⁸ See, e.g., Whitney Nat'l Bank v. Karam, 306 F. Supp. 2d 678, 682 (S.D. Tex. 2004); Cotton v. Private Bank and Trust Co., 235 F.Supp. 2d 809, 815 (N.D. Ill. 2002).

314(b) voluntary sharing provisions.⁹ We recognize the importance of institutions communicating with each other with respect to illicit activity, which by its very nature will rarely impact only a single institution. In order to facilitate greater efficiency in this and other industry best practices, FinCEN desires to open the door to such sharing in every way possible that would not ultimately compromise the confidentiality afforded SARs.

As a result, FinCEN and the Federal Banking Agencies in 2006 issued joint guidance specifying that, subject to certain exceptions or qualifications, a U.S. branch or agency of a foreign bank may share a SAR with its head office outside the United States and a U.S. bank or savings association may disclose a SAR to its controlling company, no matter where the entity or party is located.¹⁰ At that time, we deferred taking a position on whether a depository institution is permitted to share a SAR with affiliates and directed institutions NOT to share with such affiliates. Of course, such unilateral acts to allow banking operations in the United States to share with a foreign headquarters have limited effect so long as there is a lack of reciprocity from other countries.

In 2006, FinCEN also issued guidance in consultation with the staffs of the Securities and Exchange Commission (“SEC”) and the Commodity Futures Trading Commission determining that, subject to certain exceptions or qualifications, a securities broker-dealer, futures commission merchant, or introducing broker in commodities may share a SAR with parent entities, both domestic and foreign.¹¹ Guidance issued by FinCEN in consultation with the SEC in October 2006 further specified that a U.S. mutual fund may share a SAR with the investment adviser that controls the fund, whether domestic or foreign, so that the investment adviser can implement enterprise-wide risk management and compliance functions over all of the mutual funds that it controls and to better identify and report suspicious activity.¹²

It is a significant step to allow sensitive financial information to leave a jurisdiction. These pieces of guidance expressly noted that “the sharing of a Suspicious Activity Report with a non-U.S. entity raises additional concerns about the ability of the foreign entity to protect the Suspicious Activity Report in light of possible requests for disclosure abroad that may be subject to foreign law. . . .” In addition, FinCEN and the Federal regulators recognized the need for further guidance regarding whether financial institutions may share SARs with affiliates other than a controlling company, head office, or parent entity. Those are among the issues addressed by the two new proposals.

The SAR confidentiality rule proposal, discussed above, in strengthening the current non-disclosure provisions found in the SAR regulations for all covered industries, will also clarify that a financial institution may share a SAR, and information about a SAR, within its corporate organizational structure for purposes consistent with Title II of

⁹ See 31 CFR § 103.110 (b)

¹⁰ http://www.fincen.gov/statutes_regs/guidance/pdf/sarsharingguidance01122006.pdf

¹¹ http://www.fincen.gov/statutes_regs/guidance/pdf/sarsharingguidance01202006.pdf

¹² http://www.fincen.gov/statutes_regs/guidance/pdf/guidance_faqs_sar_10042006.pdf

the BSA, provided that no person involved in any reported suspicious transaction is notified that the transaction has been reported.

The issues surrounding SAR sharing are challenging. This point has been reiterated by banks and government officials around the world. FinCEN has been engaging in dialogue with some of our largest financial institutions in the United States, and it is clear that this remains a significant issue for which additional guidance is needed.

Therefore, our second proposal, the proposed interpretive guidance on SAR sharing with affiliates, clarifies instances where sharing within a corporate organizational structure is consistent with the purposes of the BSA. The proposal clarifies that affiliates, as defined in the guidance, are within the corporate organizational structure.¹³ It also outlines the circumstances under which a SAR filed by one institution may be shared with an affiliate institution that is also subject to BSA SAR requirements.

Based on the two primary goals of the BSA – promoting depository institutions’ efforts to detect and report money laundering and terrorist financing, as well as ensuring the confidentiality of a SAR or any information that would reveal the existence of a SAR – the guidance will specify that a financial institution may share a SAR, or information that would reveal the existence of the SAR, with an affiliate *provided* the affiliate is subject to a SAR regulation issued by FinCEN or the Federal Banking Agencies. The proposed guidance will apply only to depository institutions and regulated entities in the securities and futures sector, but FinCEN will be seeking comment on whether the guidance should be applied to other types of financial institutions subject to a SAR rule.

We believe that a financial institution’s ability to share a SAR, or information that would reveal the existence of a SAR, with affiliates as specified in the proposed guidance, will help depository institutions better facilitate compliance with the applicable requirements of the BSA and more effectively execute enterprise-wide diligence. SAR sharing will also help affiliates assess risks based on information regarding suspicious transactions taking place through other affiliates or lines of business within the corporate organizational structure. Further, enabling a filing institution to share the SAR under these circumstances would eliminate the present need for an institution that wants to provide information to an affiliate to create a separate summary document, which has to be crafted carefully to avoid revealing the existence of the SAR itself.

At the same time, the limitation on sharing only with those affiliates with SAR obligations, including SAR confidentiality requirements, will help protect SARs and information that would reveal the existence of a SAR from improper disclosure. In addition, because the guidance will apply only to the sharing of a SAR by the financial institution that has filed the SAR, the guidance will clarify that it is not permissible for an affiliate that has received such a SAR to share it with another affiliate. This ensures that the filing depository institution will only be sharing with those affiliates it expressly

¹³ The guidance will include a definition of an affiliate that focuses on companies under common control with, or controlled by, a depository institution.

selects. In addition, there is an expectation that the filing institution will put in place appropriate written confidentiality agreements ensuring that affiliates protect the confidentiality of the SAR, or any information that would reveal the existence of a SAR, through appropriate internal controls.

By limiting sharing to those affiliates with SAR obligations pursuant to regulations issued by FinCEN or the Federal Banking Agencies, FinCEN also intends to prevent SARs, or any information that would reveal the existence of a SAR, shared under this proposed guidance from being subjected to the laws of another jurisdiction.¹⁴ This is based on our present understanding that the confidentiality and safe harbor underpinnings of SAR reporting in the United States are not recognized in foreign jurisdictions. FinCEN acknowledges that there may be circumstances in the future that would enable the broadening of the parameters for SAR sharing to include sharing with foreign affiliates in the event FinCEN is satisfied that appropriate safeguards apply to U.S. SARs shared in such jurisdictions. As we develop a better understanding of how laws in foreign jurisdictions may presently or in the future ensure the confidentiality of U.S. SARs, our proposed rule on confidentiality will enable us to consider further circumstances under which sharing within a corporate organizational structure is consistent with the purposes of the BSA. In proposing our guidance on sharing, we are specifically seeking comment from industry that may be helpful in this regard.

I've detailed for you guidance we are working on in the United States. But why is this relevant to Mexican and international banks? The reason is that the global community is confronting some of these same challenges regarding information sharing within and across jurisdictions.

Next Steps: Surveying the Global Community

An ever-growing majority of countries in the world apply the same AML/CFT principles of the FATF 40+9 Recommendations.¹⁵ Implementation, however, remains subject to the laws of each individual jurisdiction. Many financial institutions operating in multiple jurisdictions seek to implement to the extent possible an enterprise-wide AML/CFT policy. This is often consistent with the way a financial institution manages other types of risks on an enterprise-wide basis. An enterprise-wide AML/CFT policy can help a financial institution avoid duplication and/or lower costs, and in theory, better allocate resources to the greatest AML/CFT risks.

Individual financial institutions play an important role in combating money laundering and terrorist financing, both (i) in their diligence to avoid being abused to facilitate illegal activity and (ii) in reporting transactions including suspicious

¹⁴ For example, for purposes of the BSA, foreign branches of U.S. banks are regarded as foreign banks. Under the proposed guidance, they would be “affiliates” that are not subject to a SAR regulation. Accordingly, a U.S. bank that has filed a SAR would not be able to share the SAR, or any information that would reveal the existence of the SAR, with its foreign branches.

¹⁵ http://www.fatf-gafi.org/document/28/0,3343,en_32250379_32236930_33658140_1_1_1_1,00.html

transactions to FIUs for the investigation of and ultimate government action to counter illegal activity. If a financial institution can fully share information within its corporate structure across jurisdictions, this would maximize the financial institution's ability to further both of the above functions. Such sharing of information across jurisdictions must be balanced with other policy considerations, especially ensuring the appropriate protection of the information— which is fundamental to ensuring the continued reporting from financial institutions to FIUs. Such protection will include maintaining the confidentiality of suspicious transaction reports (STRs, the equivalent to SARs in the United States) as well as broader issues of data and privacy protection.

Lengthy discussions took place on these sharing issues at the Egmont plenary meeting of Financial Intelligence Units (FIUs) held in May 2008 in Seoul, Korea. At the plenary, it was agreed that further examination of limitations or possible impediments to the sharing of information was needed. Therefore, FinCEN issued a survey for Egmont to gather information from FIUs to learn more about their rules for allowing financial institutions to share suspicious activity reports with affiliates outside their borders.

The focus of the survey was not on the sharing of information *between* FIUs or other government authorities. Rather, the primary focus is the sharing of information *within a private financial institution* that operates in multiple jurisdictions—whether through branches in different locations, or separate corporate entities including subsidiaries and affiliates under a common ownership structure.

Various FIUs confirmed during the discussion at the Seoul Plenary that the issue of impediments to sharing of information across jurisdictions has been raised by some reporting entities. It was apparent that even where certain FIUs or supervisors had addressed the issue to some extent, the allowable sharing of information may vary considerably across jurisdictions.

For example, within the European Union, the Third Money Laundering Directive would allow for sharing across jurisdictions within a financial conglomerate. Other countries similarly allow, for example, a branch of a foreign-based institution to share information back to the headquarters. Only if the law is consistent in all jurisdictions in which a financial institution operates, however, will the financial institution be able to share information on an enterprise-wide basis.

The consensus of the Egmont plenary was that it would be useful to gather further information about the laws and policies in the jurisdictions of member FIUs to better understand the challenges of financial institutions to sharing information across jurisdictions. Some of these impediments might be direct legal prohibitions such as a prohibition on the export of STR information (or possibly even a prohibition on the export from the jurisdiction of customer information more generally, such as due to bank secrecy laws).

Other practical limitations might arise from a perception of financial institutions of a lack of clarity on the applicability of the law, for example whether STR information originating in one jurisdiction would be subject to equivalent protections in another jurisdiction (in which case the financial information might choose not to share at all rather than risk a loss of protection). Obviously, in any jurisdiction a combination of the foregoing factors might lead to the practical result of less information sharing.

In another example, a financial institution operating globally can have transactions processed through multiple offices in different jurisdictions. As an illustration, a customer in Madrid orders a payment via funds transfer to a customer in Mexico City, denominated in the currency of the United States where the transaction clears in New York City. That transaction could be processed across three offices (such as branches or affiliates) of a single corporate group. If one of the offices suspected money laundering, this should be of interest to all three offices which might have different levels of information regarding the transaction. In practice, there might be impediments to the financial institution sharing information related to the transaction or its reasons for suspicion among offices in different jurisdictions.

Furthermore, the FIUs of each of the three jurisdictions would have an interest in learning about the suspicion of money laundering. While it is possible that an FIU in one of the three jurisdictions receiving a report could make a spontaneous disclosure to the FIUs of the other two jurisdictions, it would be much more practical, timely, and ultimately effective if the financial institution were able to report directly to FIUs in all jurisdictions in which the financial institution has some involvement and awareness of the suspicious transaction.

Moreover, a further vulnerability remains to the extent that one office of the financial institution could close an account or otherwise decline to engage in transactions for which there is suspicion of money laundering. The same customer might nonetheless be able to open another account with the same financial institution at another branch or affiliate to conduct the same suspicious activity, because of impediments to the financial institution managing its AML/CFT risks on an enterprise-wide basis.

The process of surveying the jurisdictions of all 108 Egmont member FIUs remains ongoing at this time. An initial review of the results will take place during the Egmont meetings to be held in Toronto, Canada the week of October 20, 2008. The information should help identify impediments and how to address them to better promote information sharing. The Egmont Group FIUs will seek to engage other international standard-setters going forward. This initiative will likely lead to some clarification, as well as proposals, to amend the laws of some jurisdictions to provide explicitly for mutual recognition.

Another area that is important to explore today is the valuable information exchange that can take place *among* financial institutions.

Information Sharing Among Unrelated Financial Institutions

I understand the Government of Mexico is currently working to establish draft procedures that would establish a mechanism for information exchange among Mexican financial institutions.

In the United States, a program has been established where financial institutions can share information with one another in order to help in the identification and reporting to the federal government activities that may involve money laundering or terrorist activity. Section 314(b) of the USA PATRIOT Act stipulates the conditions for this sharing in more detail and requires financial institutions to provide notice to FinCEN in order to share information with other institutions.¹⁶

To participate in this voluntary program, a financial institution must file a notice with FinCEN of its intent to share information. Financial institutions may file a notice electronically through FinCEN's web site, or manually by sending a paper form through standard mail. A notice to share information is effective for a period of one year. The list of participating financial institutions is not publicly available; FinCEN only provides the list to information-sharing participants.

Registered institutions include: Banks, Thrifts, Credit Unions, Broker Dealers, Mutual Fund Associations, Insurance Companies, Holding Companies, Commodity Trading Advisors, Operators of Credit Card Systems, Registered Investment Advisors, Real Estate Closers/Settlers, Trust Companies, and Money Services Businesses. As of today, there are over 4,000 financial institutions participating in this voluntary information sharing program, a number we hope will continue to grow as more institutions learn of the benefits of information sharing.

We know institutions are actively sharing information through this process in the areas of money laundering and terrorist financing, and we've received extremely positive feedback from financial institutions that participate. Promoting greater use of this type of information sharing is an area where I feel we should be ever vigilant in order to achieve the full potential of this valuable tool. FinCEN is currently exploring ways to encourage further usage, so you will hear more soon about this 314(b) authority in the United States.

I am very encouraged that our Mexican counterparts are in the process of developing procedures for a similar information sharing program as well. This type of information sharing is another area in which both of our countries recognize the value of a strong public-private partnership.

Ongoing Collaboration with Mexico

It is important to recognize the contributions of the Mexican banks in the fight against money laundering and terrorism financing. Your vigilance in reporting threshold and suspicious transactions enable FinCEN and the UIF to track illicit activity. FinCEN

¹⁶ See 31 CFR § 103.110: Voluntary information sharing among financial institutions.

and the UIF enjoy a strong partnership in this regard and have had the opportunity to engage in many tactical and strategic projects resulting in great success. We are continuing to explore new ways in which our two countries can continue to foster our dynamic relationship. By facilitating sharing of information among banks, both within a corporate structure and among unrelated entities, we help, first, to protect the banks from criminal abuse, and, second, to provide the government with the information it needs to track down the criminals and thereby protect all citizens.

It has been a great pleasure for me to be here today in Mexico to announce these very important U.S. and global initiatives. I hope that the Mexican banks and the Mexican government will support these efforts as part of our ongoing close collaboration and common goals of combating money laundering, terrorism, and other criminal activity

I would be happy to answer any questions you may have in the time remaining.

###