PREPARED REMARKS OF JAMES H. FREIS, JR.
DIRECTOR, FINANCIAL CRIMES ENFORCEMENT NETWORK
U.S. DEPARTMENT OF THE TREASURY

DELIVERED AT THE ABA/ABA MONEY LAUNDERING ENFORCEMENT CONFERENCE

WASHINGTON, D.C.
OCTOBER 13, 2009

A *strong* partnership is needed between the financial industry and our government to fight money laundering, terrorist financing, fraud and other financial crimes. An *effective* partnership requires an open and ongoing *dialogue* among the partners. Meeting with you today presents another opportunity for us to continue this important dialogue. Specifically, I'd like to share some of the insights that the Financial Crimes Enforcement Network (FinCEN) has gleaned from recent efforts to hold candid conversations with individual financial institutions to better understand the practical implications of FinCEN's regulatory requirements and ways that, working together with the financial industry, we can better achieve our common goals in protecting the financial system from the abuses of financial crime. I would also like to highlight some examples of how we have tried to be responsive to constructive suggestions from members of the financial industry as to how we can be more efficient and effective.

Among the remarks I made at this conference two years ago, I spoke about a range of FinCEN efforts to provide feedback to financial institutions on the value of their anti-money laundering / counter-terrorist financing (AML/CFT) efforts.[1] In particular, I reviewed the multiple ways we use the information reported by financial institutions, and how we continuously publish examples of case successes while balancing the needs to protect the sensitivities of law enforcement operations. Many of you are familiar with FinCEN's analytical reports and guidance provided to help financial institutions better focus their compliance efforts to address underlying risks and provide FinCEN and law enforcement with the information we need to fight crime.

The type of dialogue on which I will focus today is FinCEN's role as administrator of the Bank Secrecy Act (BSA) and thus as a regulator of financial institutions. FinCEN's responsibilities in this area have grown tremendously over the past decade with the extension of BSA regulations to new industry sectors as well as specific requirements for certain types of financial activity. One thing that any regulator must understand is how its rules affect the day-to-day business and related compliance decisions of regulated institutions. Both the financial industry and the government continue to learn from one another as the partnership evolves over

[1] See http://www.fincen.gov/news_room/speech/pdf/20071022.pdf

time. Even those at FinCEN with professional experience in the financial industry or as financial supervisors (including myself) must constantly seek to understand the implications of our rules in a dynamic world.

Last year at this conference, I spoke about the objectives and conduct of BSA enforcement.[2] FinCEN works closely with the agencies to which we have delegated authority to examine for compliance, and is committed to coordinating closely with other agencies on BSA enforcement actions. As I previously explained, FinCEN benefits from leveraging the resources and knowledge of the supervisory agencies.

One aspect of this framework is that in the absence of having compliance examiners of its own, FinCEN does not have the same type of day-to-day interactive relationship with the industry common to other regulators. Nevertheless, we have worked hard to establish better and more efficient channels of communication like: our modernized Web site, our dedicated outreach staff who have attended hundreds of conferences and answered thousands of questions that come into our BSA Resource Center and Regulatory Helpline; and, as most of you are familiar with, the Bank Secrecy Act Advisory Group that we administer. But, we know we can do more. It is in this context that FinCEN decided to undertake a concerted effort to reach out to financial institutions.

FinCEN's Outreach Initiative

For the past two years, FinCEN has been engaged in an outreach initiative with the nation's largest banks and money services businesses as part of our broader effort to ensure that our mission as BSA administrator is carried out in the most efficient and effective manner possible.

In January 2008, FinCEN reached out to some of the largest banks in the nation to invite them to volunteer to participate in our outreach initiative, with the intent of broadening our understanding of financial industry practices, and of what information institutions need in order to effectively implement their AML programs.

From April 2008 through January 2009, FinCEN teams individually visited eight large depository institutions in conjunction with this outreach effort. The teams were a cross-section of FinCEN: Our analysts who are working with the BSA data on a daily basis in support of law enforcement, our outreach and policy specialists who craft BSA guidance and regulations, and those within our IT office involved with our BSA E-filing and other technology initiatives.

All of the FinCEN team members felt the meetings provided a very helpful snapshot into the industry. But what was particularly helpful to us was having an opportunity to simply sit face to face and hear from the different banks. Not only did we gain an understanding of how different banks integrate AML into their business plans, we also had frank discussions about some of their challenges. And it can only benefit the financial industry, the law enforcement community, and our regulatory partners if we share our observations from this outreach initiative more broadly.

[2] See http://www.fincen.gov/news_room/speech/pdf/20081020.pdf

So, today, FinCEN is releasing a public report that summarizes the information we gathered during the course of our outreach.[3] I would also like to spend my time today talking about our findings, as well as looking forward in this ongoing initiative. Let me emphasize that these findings with respect to these largest banks are merely that – facts that help FinCEN better understand the way in which these institutions are working in practice, which I am pleased to be able to share publicly. This does not mean that FinCEN endorses or requires any institutions to follow these examples, nor do these findings alone change our regulations and guidance.

During our outreach meetings, FinCEN received briefings on each bank's AML program, comprised of corporate-wide, risk-based procedures tailored to their various lines of business. In our discussions with the banks, we also received information in several key areas that are discussed in more detail in the report, but that I'd also like to focus on today: account closure policies surrounding suspicious activity report (SAR) filings; how banks identify and report fraud-related activity; the value of bank referrals in the identification of suspicious transactions; and the role of financial intelligence units (FIUs) within the banks.

Account Closure Policies

Among our key findings, FinCEN learned that many larger depository institutions have internal account closure policies in place relating to SAR filings; however, the policies differ among the various banks.

For some banks, one egregious SAR filing could lead to an account closure; however, a number of banks stated that once a bank files a second SAR on a customer's activity, the account is monitored and may be closed, depending on law enforcement interest. All banks stated that they will keep an account open for investigative purposes if they receive a request from law enforcement to do so.[4]

Some banks also noted that the $5,000 *de minimis* threshold is not a significant consideration when filing a SAR; if the activity is deemed to be suspicious by the bank, they will file regardless of the dollar amount involved. In addition, the banks indicated that they are very careful and serious in their SAR filing decisions. The banks were emphatic that after careful review they were filing SARs that were required and may merit law enforcement investigation.

Several banks also indicated that if a customer were structuring transactions, a brochure, letter, or other educational materials would be sent to the customer to explain BSA reporting requirements. If activity continues after this outreach, account closure procedures are initiated. Since the conclusion of our outreach, we have since heard that banks are also providing FinCEN's educational pamphlet released in February of this year entitled, "Notice to Customers: A CTR Reference Guide," which is another resource available to address customers' questions about BSA reporting requirements.[5]

---

[3] See http://www.fincen.gov/news_room/rp/reports/pdf/Bank_Report.pdf
[4] See http://www.fincen.gov/statutes_regs/guidance/pdf/Maintaining_Accounts_Guidance.pdf
[5] See http://www.fincen.gov/whatsnew/pdf/CTRPamphletBW.pdf

Fraud vs. Money Laundering

Turning now to the issue of fraud, FinCEN found during the course of our outreach that generally speaking, the money laundering-related SAR process is managed within a bank's AML or BSA compliance group, while the fraud-related SAR process is typically handled by other business lines within the bank, including corporate security, fraud prevention, loan risk and recovery, consumer lending operations, and credit card operations.

FinCEN's work in this area illustrates that while fraud and money laundering are often viewed as separate criminal enterprises, acts of fraud and acts of money laundering are often quite interconnected. The financial gain of the fraudulent activity ultimately needs to be integrated into the financial system, so money laundering is often a product of fraud.

Therefore, it was of interest to FinCEN that many banks' AML programs are run entirely separately from their fraud detection programs. Several banks noted the challenge that a successful AML program does not recoup losses like anti-fraud programs – with pure money laundering, there typically is not a loss for the bank, meaning there are no funds to recoup.

From a due diligence perspective, however, information financial institutions have available and collect to comply with their anti-money laundering program requirements in many ways mirrors the information they would already be gathering for anti-fraud purposes; customer and transactional information used for AML purposes is often the same customer and transactional information needed for fraud investigations. As a result, the resources being spent on fraud detection and prevention within financial institutions may well support the AML program, and vice versa.

In fact, one bank also observed that, historically, as AML programs and fraudulent activity became more sophisticated over time, efforts to combat fraud and money laundering diverged. This bank noted that they are now starting to see fraud and AML programs at their institution, as well as others, merge back together because there is an increasing recognition of the similarity of the data being collected to investigate fraud and money laundering. It was also noted that with the increasing convergence of fraud and AML investigations taking place within the bank, there is yet another benefit to merging anti-fraud and anti-money laundering resources and tools.

Several banks also commented they are witnessing an increase in fraud-related SARs, specifically in the areas of mortgage loan fraud, home equity loan fraud, credit card fraud, and general account misrepresentations and false statements. It was noted that FinCEN's *SAR Activity Reviews* and mortgage loan fraud studies are helpful tools to assist in identifying this type of activity.

FinCEN further discussed the interconnectedness of criminal activity in an analytical study that was released in March 2009, which looks at the relationship between mortgage fraud and other financial crime, and identifies how financial crime runs through the different financial sectors.[6]

[6] See http://www.fincen.gov/news_room/rp/files/mortgage_fraud.pdf

Some banks also noted that they changed some of their processes related to risks of fraud in mortgages following their review of FinCEN's analytical products in the mortgage fraud area.

I've touched on the issue of account closure policies related to SARs, as well as how banks manage the fraud-related SAR process, and now I would like to turn to what all the banks unanimously viewed as their most valuable resource for spotting suspicious activity: alert employees within the bank itself.

Automated Monitoring vs. Referrals

While banks indicated that automated transaction monitoring systems to generate "alerts" for further investigation provided added value to their efforts to identify suspicious activity, every bank indicated that they believe their best source of information on possible suspicious activity comes from referrals by front-line bank personnel.

One bank estimated that over 80 percent of its suspicious activity referrals are generated from bank personnel, while the rest are the result of alerts generated by the transaction monitoring systems and reports. Another bank noted that 25 percent of its investigations originate from staff referrals and 45 percent of its AML SARs that are ultimately filed originated from these referrals.

These statistics speak to the importance of the training provided to bank personnel to spot suspicious activity, as well as the important role of bank employees dedicated to reviewing the referrals and alerts generated by automated systems. No one knows better what is normal business for a bank's customers, and hence what anomalous activity is suspicious, then the bank's employees who serve those customers every day.

Financial Intelligence Units (FIUs)

The vast majority of banks that were visited during our outreach had established stand-alone "financial intelligence units" (FIUs) to support their efforts to comply with reporting requirements under the BSA. Although the name is the same, this should not be confused with FinCEN's role as the financial intelligence unit of the United States, which is defined as:

> A central, national agency responsible for receiving, (and as permitted, requesting), analyzing and disseminating to the competent authorities, disclosures of financial information:
>
> (i) concerning suspected proceeds of crime and potential financing of terrorism, or
>
> (ii) required by national legislation or regulation, in order to combat money laundering and terrorism financing.[7]

Naturally, the FIUs within the banks varied greatly in size and organizational structure depending upon the size of the bank and its risk profile.

[7] See Interpretive Note Concerning the Egmont Definition of a Financial Intelligence Unit, available at http://www.egmontgroup.org/files/library_egmont_docs/egmont_final_interpretive.pdf.

It was of interest to note that the FIUs are structured, and in many ways operate, like FinCEN's own analytical function. While visiting with the banks, FinCEN received several demonstrations that provided additional insight into how the banks' AML programs operate and how their FIUs function to include: account opening; wire transfer monitoring; the 314(a) process; transaction monitoring; alert processing; case management; and SAR filing.

In every instance, the banks spoke of maintaining active, engaged relationships with Federal, State, and local law enforcement officials. Several banks noted their investigators are active with the SAR Review Teams that have been established within their banks' regions and the interactions with these Teams were characterized as very beneficial.

Some banks noted that they draw on the SAR Review Teams to assist in training bank employees within their FIU. One bank also commented that they engage closely with their law enforcement contacts: to gather feedback on the usefulness of the SARs that are filed; during the process of producing underlying SAR documentation in response to subpoenas received on SAR suspects; and in cases where the bank notified law enforcement prior to, or concurrent with, SAR filing.

While it was very helpful to learn about the banks' various AML processes and procedures, we also wanted to hear their honest feedback on the value of FinCEN's products to help us determine what is useful to our financial industry partners or where additional guidance might be helpful. In these discussions, the banks expressed positive reactions to FinCEN's new Web site design, as well as FinCEN's Regulatory Helpline, which provides a forum for financial institutions to ask FinCEN questions relating to BSA requirements.

Issues Raised by the Banks

I'd like to spend a moment discussing a few of the specific issues the banks raised where they felt additional guidance would be helpful in fulfilling their AML program requirements, including: SAR sharing, the 30-day clock, and SAR acknowledgements. As a direct result of this feedback, FinCEN has already worked to respond in many areas. This shows FinCEN's commitment to being responsive to questions raised by the industry in trying to comply with our regulations.

SAR Sharing

One bank emphasized its strong feelings that geography should not be an inhibitor to SAR sharing with affiliates and that the ability to share the SAR should be dependent on the need to know the information, not one's geographical location. Another bank brought up the difficulties in the current domestic SAR sharing process and its frustrations with having to utilize the 314(b) process to share with affiliates.

In March 2009, FinCEN proposed amendments to our SAR regulations to expand the confidentiality of SAR information, along with a parallel proposed guidance document on "SAR sharing," to ensure that the appropriate parties, but only those parties, have access to SARs.[8]

[8] See http://www.fincen.gov/news_room/nr/pdf/20090303.pdf.

Among other things, these proposals would clarify the responsibilities of both government employees and financial institutions to protect this information. As a result, law enforcement investigators should receive higher caliber information from SARs, and corporate affiliates can share information with each other about dangerous customers who could harm the institution's bottom line or reputation.

In June 2009, FinCEN also issued a statement following the annual plenary meeting of the Egmont Group, held in Doha, Qatar,[9] noting the guidance that FinCEN has proposed to facilitate SAR sharing among domestic affiliates is but a first step to raise awareness and remove some of the impediments that are preventing nations across the globe from fulfilling some of the Financial Action Task Force principles designed to protect corporations, institutions, and financial markets. The G-20 leaders have also noted the need to promote greater sharing of AML-CFT information across jurisdictions.[10]

30-Day SAR Filing Clock

During our visits, a few of the banks expressed their views regarding the 30-day SAR filing period. The banks maintained that there is no definitive judicial or regulatory decision that provides clear guidance as to when the statutory 30-day SAR filing period begins to run, nor was it clarified in the most recent exam manual when a transaction should be determined to be suspicious.

For example, the banks felt that the regulations require a SAR to be filed "no later than 30 calendar days after the date of initial detection by the bank of facts that may constitute a basis for filing the SAR" and view this as a completely subjective approach to risk assessment. Moreover, they maintain that most of the transactions, events, or referrals that are or can be investigated for purposes of possible suspicious activity prove to be unworthy of investigation or filing.

The banks suggested a more practical approach for regulating the SAR filing that recognizes the need to manage events and review cases in order to determine whether a SAR should be filed, and then a 30-day period to prepare and file the SAR. Another suggestion they offer is to implement a 60-day or even 90-day time frame from receipt of a referral or generation of an alert to the date the SAR should be filed.

FinCEN explained in the meetings that the 30-day period was meant to balance appropriate review within a bank with getting timely information to law enforcement to carry out fuller investigations where appropriate. Building upon the feedback from banks, FinCEN issued guidance on the 30-day filing requirement in its October 2008 issue of the *SAR Activity Review: Trends, Tips and Issues*.[11]

[9] The Egmont Group is an international network of financial intelligence units from more than 100 jurisdictions.
[10] See http://www.g20.org/Documents/g20_wg2_010409.pdf, Key Message #38
[11] See http://www.fincen.gov/news_room/rp/files/sar_tti_14.pdf

SAR Acknowledgements

Another bank requested the addition of acknowledgements to its SAR BSA E-filings. The ability to receive an acknowledgement file allows the bank to verify their submissions were loaded properly into the FinCEN internal database and also provides their regulators with additional verification of their submissions.

On September 12, 2009, FinCEN implemented a system to provide an acknowledgement to financial institutions when they file a SAR electronically through the BSA E-filing system.[12] Specifically, the SAR acknowledgement will provide financial institutions with receipt of submission by providing acknowledgement files containing Document Control Numbers (DCNs) generated by the current system of record, WebCBRS.

To allow time to modify their own systems and processes to accept the DCNs, BSA E-Filing users will be able to self-enroll to receive acknowledgements by form type when they are ready to receive and process the acknowledgement files. The acknowledgement files will also be available to filers in both the legacy flat file and as an XML file. When self-enrolling, the user can select to receive one or both types of acknowledgement files. In December 2009, FinCEN will implement SAR Validations, which will allow the BSA E-Filing system to validate SAR documents and provide filers with feedback on the technical quality of their submissions.

Banks also raised a variety of issues where additional guidance was requested, specifically emerging trends and patterns, and transaction monitoring more focused on larger institutions and certain geographic areas. FinCEN will continue to work to address remaining areas of concern brought to our attention by the banks during the outreach meetings as appropriate.

Looking Forward

Throughout 2009, FinCEN has been conducting similar outreach to some of the largest money services businesses, and we have found these meetings to be equally beneficial to improving our understanding of some of the issues unique to MSBs in complying with FinCEN regulations.

Looking forward into 2010, FinCEN is announcing today its interest in conducting similar meetings with representatives from the nation's depository institutions with assets under $5 billion to hear about how these institutions implement their anti-money laundering programs, including unique challenges faced by institutions across this asset class and where additional guidance from FinCEN could be helpful.[13]

Due to the large number of financial institutions within this asset class, FinCEN is inviting depository institutions to express their interest by applying to participate in this voluntary outreach. An e-mail address has been established for this purpose: outreach@fincen.gov. Interested depository institutions with assets under $5 billion are

[12] See http://www.fincen.gov/whatsnew/html/20090826.html
[13] See http://www.fincen.gov/news_room/nr/20091013a.pdf

requested to send an e-mail by November 30, 2009 to outreach@fincen.gov with the following information:

- Name of their institution;
- Point of contact;
- The institution's asset size;
- Geographic location;
- Type of charter; and
- Preference of either an on-site visit by FinCEN or a visit to FinCEN's office.

Based on the number of financial institutions responding, FinCEN will then select a cross-section of no less than fifteen (15) financial institutions to ensure our outreach takes place with a diverse representation of depository institutions with assets under $5 billion. More information may be found on FinCEN's Web site at www.fincen.gov.

As with the previous outreach we've conducted, FinCEN would appreciate learning how these institutions comply with each of the four pillars of the BSA regulatory regime: program requirements; designation of a compliance officer; training; and independent audit, with a focus on how the institution complies with the program requirements.

Conclusion

Once again, FinCEN would like to express its appreciation to all the banks, MSBs, and their staff that devoted their time and effort to participate in our outreach initiative. FinCEN team members have found the meetings to be very informative and valuable toward furthering FinCEN's broader mission of enhancing U.S. national security, deterring and detecting criminal activity, and safeguarding financial systems from abuse by promoting transparency in the U.S. and international financial systems.

We are looking forward to our next round of meetings with representatives from depository institutions with assets under $5 billion, and I encourage those of you here today from banks within this asset class to contact outreach@fincen.gov, as we seek to expand upon what has already been a very positive initiative.

We appreciate the partnership in fighting financial crime. As your regulator, I want financial institutions to know that FinCEN is open to constructive suggestions as to how we can strive towards this objective in more efficient and effective ways.

###