PREPARED REMARKS OF JAMES H. FREIS, JR.

DIRECTOR, FINANCIAL CRIMES ENFORCEMENT NETWORK

ASSOCIATION OF CERTIFIED FRAUD EXAMINERS

20TH ANNUAL FRAUD CONFERENCE

LAS VEGAS, NV

JULY 13, 2009

Good afternoon. I'd like to spend my time today sharing with you some of the Financial Crimes Enforcement Network's (FinCEN's) most recent work to combat fraud, particularly as it relates to the areas of loan modification fraud and identity theft, and the important role you play as fraud examiners in detecting and investigating fraudulent activity.

Whether you are an internal auditor within a health care company, a fraud investigator for a law enforcement agency, or a CPA working to guard against fraud within a not-for-profit organization, you all have one thing in common: as fraud detection and prevention professionals, you are the eyes and ears of your organization. You know your business and what are considered normal and regular business practices in your industry. Who better to identify suspicious activity when extraordinary activities occur, particularly when you know how your organization operates as well as your customers' business, habits, and routines?

Your interests in deterring, detecting, holding accountable, and seeking restitution from those who perpetrate fraud are directly aligned with FinCEN's mission. And in FinCEN's case, our success in pursuing our mission of fighting money laundering, terrorist financing, and financial fraud depends on the dedicated men and women of FinCEN and our ability to listen to our law enforcement customers and our industry partners. But, we could not wholly perform our mission without strong partnerships with the industries that fall under the Bank Secrecy Act regulations as well as our colleagues in the Federal and State financial regulatory agencies, and our international, Federal, State, and local law enforcement partners.

For those of you who may not be familiar with FinCEN, our mission is to enhance U.S. national security, deter and detect criminal activity, and safeguard financial systems from abuse by promoting transparency in the U.S. and international financial systems.

FinCEN works to achieve its mission in the following ways:

- ***Administering the Bank Secrecy Act (BSA)***, which is the principal anti-money laundering and counter-terrorist financing regulatory regime in the United States;
- ***Supporting law enforcement, intelligence, and regulatory agencies*** through the sharing and analysis of financial intelligence;
- ***Building global cooperation*** with our counterpart financial intelligence units; and
- ***Promoting*** the appropriate use of Bank Secrecy Act information.

The BSA plays an important role in increasing the transparency of the U.S. financial system so that, working together with industry, regulatory and law enforcement partners, we can deter, detect, investigate, and prosecute money laundering, terrorist financing, and other financial crimes.

As the administrators of the BSA, we strive to fulfill our mission in a way that ensures that financial institutions have appropriate controls in place to protect themselves from those seeking to abuse the financial system. FinCEN's regulations requiring financial institutions to implement anti-money laundering and counter-terrorist financing programs are primarily about ***prevention –*** a critical component of any effort to combat fraud. But it's also our job to work with the financial industry as it strives to comply with its responsibility to report certain financial information and suspicious activities so that we can make that useful information available to law enforcement. I'd like to take a moment to provide you with some feedback on what we've seen recently as it relates to suspected fraud, which financial institutions report to us through Suspicious Activity Reports, known more commonly as SARs.

Increase in Reporting of Suspected Fraud

In our most recent *SAR Activity Review, By the Numbers* - issued about a week ago on July 7, 2009 - we've seen a continued increase in SAR filings related to all areas of suspected fraud.[1] Of the 20 different violation types reportable on the SAR-DI, which is the SAR form used by depository institutions, 7 of the categories relate specifically to fraud. These categories are: check fraud, mortgage loan fraud, consumer loan fraud, wire transfer fraud, commercial loan fraud, credit card fraud, and debit card fraud.

While these 7 categories only represent 1/3 of the possible violation types, they account for nearly half of the increase in total SAR filings from 2007-2008. In fact, all 7 fraud categories saw double-digit increases in percentage of filings between 2007-2008.

---

[1] *See* http://www.fincen.gov/news_room/rp/files/sar_by_numb_12.pdf

Check fraud – Overall, check fraud accounts for about 489,000 SARs, or about 10 percent of all SAR-DIs filed with FinCEN between April 1996 and December 2008. During this 12-year period, the number of check fraud SARs filed with FinCEN has increased every year, with a third of all reports being filed in 2007 and 2008. Reported instances of check fraud (in whole or in part) continue to rise, increasing 17 percent in the last year.

Commercial Loan Fraud – While commercial loan fraud reports account for less than 1 percent of the total SAR database, steady increases in reporting have been observed in this area as well. Reports of suspected fraud have risen 14 percent from 2007-2008. We have also seen a number of commercial loan frauds reported under other categories such as "mortgage loan fraud."

Consumer Loan Fraud – Since January 2006, 56,555 SAR-DIs have been filed indicating consumer loan fraud as the summary characterization of suspicious activity. This 3-year period accounts for 59 percent of all such reports filed since April 1996. Additionally, since 2007, consumer loan fraud filings have increased 34 percent.

Credit Card Fraud – SARs indicating credit card fraud neared the 40,000 mark in 2008, a 22 percent increase over the filings from the previous year. Credit card fraud also continues to be the most prevalent criminal activity facilitated by identity theft. Identity theft is committed to facilitate all of these types of fraud, not vice versa. Approximately 36 percent of the SAR filings involved credit card fraud in combination with identity theft, by itself or with other listed violation(s). In addition to these explicitly noted credit card fraud reports, we see many instances of credit card fraud reported under other activities, including securities fraud.

Debit Card Fraud – Like commercial loan fraud, reports of debit card fraud comprise less than 1 percent of the SAR database; however, we continue to see steady increases in this reporting as well. The 17,000 reports reflecting suspected debit card fraud filed in the past 4 years (2005-2008) account for more than 55 percent of all such reports filed since April 1996.

Wire Transfer Fraud – Since April 1996, 53,590 SAR-DIs have been filed identifying wire transfer fraud as the summary characterization of suspicious activity. Of these reports, nearly half (45 percent) were filed in the last two years. Reported instances continue to rise, increasing 69 percent in 2007 and 58 percent in 2008.

In 2008, SARs filed by the securities industry that characterized the suspicious activity type as "Significant Wire" or "Other Transactions without Economic Purpose" increased 28percent, as compared to the previous year, which saw a similar increase from the prior year's end.

Mortgage Loan Fraud – Like the previous year, 2008 saw a continued trend upward for SAR-DIs reporting mortgage loan fraud. In 2007, this summary characterization was ranked 5th by depository institutions, and rose to 3rd by the end of 2008.

One reason for these increased volumes of mortgage loan fraud SAR filings is that financial institutions that file SARs are getting much better at spotting potential fraud and are more aware today of the types of mortgage fraud being perpetrated. On the other hand, the

Federal government, through the combined efforts of local, State and Federal law enforcement, is cracking down on scammers, which makes it harder for criminal elements to successfully commit fraud. Criminals look for opportunity and increased vigilance reduces those opportunities.

There also was an increase in the percentage of SARs where the filer reported detecting the suspicious activity prior to granting the loan – 34 percent compared with 31 percent in the prior 1-year period. FinCEN's April 2008 mortgage fraud report showed the increase was 21 percent over the preceding decade. [2] Once again, this reaffirmed the trends we had been seeing since 2003 when we began providing feedback to industry on this issue: institutions – and fraud examiners like you – are becoming more adept at spotting fraud before the money goes out the door.

While these increases in reporting of suspected fraudulent activity could mean that there is an increase in fraud activity, it also reflects an increase in awareness within financial institutions detecting such activity. Fraud examiners play a vital role in working to help businesses of all kinds in their efforts to root out fraud. Particularly in challenging economic times, with fraud impacting the bottom line, these statistics show that the skills of fraud examiners are more valuable than ever. The demand for your services and expertise will only continue to grow.

How SARs are Used

Primarily with respect to SARs, but also sometimes with the other reporting forms filed with FinCEN, the information financial institutions provide can be the ***tip-off*** that starts an investigation. An 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.

When an investigation is already underway, BSA information can add significant value by pointing to the ***identities*** of previously unknown subjects, exposing accounts and other hidden financial relationships, or unveiling items of identifying information like common addresses or phone numbers that connect seemingly unrelated individuals and, in some cases, even confirming locations of suspects at certain times. Law enforcement, again and again, confirms the reliability of the information in BSA reports, which is a direct reflection of the diligence and training within financial institutions.

FinCEN analysts can use technology to examine the entire BSA information base more broadly. When expertly queried, the data unmasks ***trends and patterns*** that hold signs of criminal or terrorist networks and emerging threats. Hidden in the wealth of information, but easily revealed by skilled analysts with the right tools, are very reliable and credible reports of mortgage fraud, check fraud, identity theft, and other suspected crimes. This information can also be overlaid on a map to make apparent the geographic range of suspicious activity and allow law enforcement agencies to better allocate their limited resources for maximum effectiveness.

---

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

The existence of BSA regulations also has a ***deterrent effect*** on those who would abuse the financial system. The near certainty of a CTR filing and the mere possibility of a SAR filing force criminals to behave in risky ways that expose them to scrutiny and capture. In addition to the increased likelihood of discovery, it's a success of its own that our collective efforts make it more expensive, difficult and time-consuming for illicit actors to realize the proceeds of crime or to raise funds for terrorist attacks.

Loan Modification Fraud

One of the greatest obstacles FinCEN faces is that there is always a new scam, a new angle, or new opportunities for criminal actors. Mortgage loan fraud and loan modification fraud are prime examples of fraud opportunities in all economic conditions. When times are good, mortgage loan fraud emerges as an issue because there is lot of money changing hands and it may be easier to get a mortgage with minimal documentation requirements. When times turn bad, fraudsters can use loan modification and foreclosure rescue scams to prey upon innocent homeowners who are doing everything they can just to keep their homes.

On April 6, 2009, Treasury Secretary Geithner announced a new coordinated effort, led by FinCEN, to combat fraudulent loan modification schemes and coordinate ongoing efforts across a range of Federal, State, civil, and criminal enforcement agencies to investigate fraud and assist with enforcement and prosecutions.[3]

FinCEN's targeting effort is producing leads that have helped various agencies halt the illegal practices of those attempting to perpetrate loan modification or foreclosure rescue scams. To date, FinCEN has identified approximately 600 SARs filed related to loan modification or foreclosure rescue fraud, from which reports have been developed and referred to Federal and State law enforcement agencies. The initial feedback FinCEN has received on these referrals has been positive.

FinCEN is also marshaling information about possible fraud criminals – drawing upon a variety of data available to law enforcement, regulatory agencies, and the consumer protection community – for the purpose of identifying and proactively referring potential criminal targets to participating law enforcement authorities. FinCEN has developed several analytical reports based on the subject leads and coordinated the dissemination of these reports through its High Intensity Financial Crime Area (HIFCA) representatives.

FinCEN also issued an advisory on April 6, 2009 to alert financial institutions to the risks of emerging schemes related to loan modifications.[4] The advisory identifies red flags that may indicate a loan modification or foreclosure rescue scam and warrant the filing of a SAR by a financial institution. A key request in the advisory is that financial institutions include the term "foreclosure rescue scam" in the narrative sections of all relevant SARs. Including this term will allow law enforcement to more easily search for and identify fraudulent activity when reviewing SAR information, which in turn assists in focusing their investigative resources.

---

[3] *See* http://www.treas.gov/press/releases/tg83.htm
[4] *See* http://www.fincen.gov/statutes_regs/guidance/pdf/fin-2009-a001.pdf

Our work in this area is but one example of broader FinCEN efforts underway to support the Term Asset-Backed Securities Loan Facility (TALF) task force program to deter, detect, and investigate instances of fraud in the financial stability plan programs.

Identity Theft

Reports of identity theft are also on the increase. From 2007 – 2008, there was a 28 percent increase in SAR-DI filings, compared with only an 8 percent increase in filings from 2006 – 2007. Identity theft had the third highest percentage increase behind reports of wire transfer fraud and consumer loan fraud.

The crime of identity theft is obviously not a new one. In October 1998, the Congress passed the *Identity Theft and Assumption Deterrence Act of 1998* to address this problem and specifically make it a Federal crime to: "knowingly [transfer] or [use], without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law."[5]

FinCEN first highlighted the issue of identity theft in an analysis of SAR filings published in June 2001, noting that the increase of technology, specifically the internet, was proving to be a powerful facilitator for this crime.[6] Many of the SAR narratives reviewed indicated that loss or theft of a wallet or purse, mail theft, and fraudulent address change were the most common ways to become a victim of identity theft. This early analysis also noted instances of insider involvement by persons with easy access to the victim's personal information. Many narratives also described the fraudulent use of another individual's Social Security number to obtain car loans to purchase or lease high-end automobiles.

Over the years, FinCEN has continued to provide feedback on the filing activity we have been seeing related to identity theft, providing an update in the October 2001 *SAR Activity Review*.[7] In more recent issues, we've highlighted feedback received from law enforcement where BSA information played a key role in the successful investigation of criminal activity involving identity theft.[8]

In July 2003, an "Identity Theft" box, along with a box for "Terrorist Financing," was added to the SAR-DI form, and in May 2004 to the SAR-SF form, so institutions could more easily highlight their suspicions of this activity when filing SARs.

In FinCEN's most recent issue of the *SAR Activity Review, Trends, Tips and Issues* – published in May 2009 – our Office of Regulatory Policy included guidance on the importance of SAR form completion when reporting instances of identity theft.[9] A SAR that includes a

---

[5] *See* 18 USC § 1028
[6] *See* http://www.fincen.gov/news_room/rp/files/sar_tti_02.pdf
[7] *See* http://www.fincen.gov/news_room/rp/files/sar_tti_03.pdf
[8] *See* http://www.fincen.gov/news_room/rp/files/reg_sar_index.html#Identity%20Theft
[9] *See* http://www.fincen.gov/news_room/rp/files/sar_tti_15.pdf (p. 41)

chronological and complete narrative of the suspicious activity involved paints a full picture that is extremely useful to law enforcement.

The Relevance of Fraud and Money Laundering

FinCEN's work in the fraud area illustrates that while fraud and money laundering are often viewed as separate criminal enterprises, acts of fraud and acts of money laundering are quite often interconnected: the financial gain of the fraudulent activity ultimately needs to be integrated into the financial system. Therefore, money laundering is often a malignant and pernicious product of fraud. By fighting fraud, you are fighting money laundering. And in turn, by identifying money laundering, you could be alerting law enforcement to activity intended to obscure the illicit source of the proceeds of fraudulent activity committed against innocent victims.

This ***interconnectedness*** of criminal activity was discussed in an analytical study that FinCEN 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.[10]

FinCEN's expert analysis of the BSA data has played a valuable role in significant fraud investigations. As examples, the Commodity Futures Trading Commission (CFTC) recently cited FinCEN's assistance in breaking up two different multi-million dollar fraud schemes.[11] I mention these as further evidence of how broadly financial crime can spread and how sophisticated our criminal adversaries can be.

It is important to appreciate that the information financial institutions 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. Therefore, the resources being spent on fraud detection and prevention within financial institutions can often be harnessed for anti-money laundering (AML) purposes, and vice versa.

In the case of fraud, financial institutions have a clear interest in expending significant resources – including, for example, hiring highly skilled employees with a CFE credential – to combat crime taking place within their businesses. This obviously makes selling the business case for fighting fraud within financial institutions easier, because there is a tangible impact on the institution's bottom line.

For the financial institution, the business case for fighting fraud is a much easier argument to make if every investigation not only works to recover the proceeds of fraud, but also aims to detect and prevent fraud from taking place so that there is no loss to begin with. I want to emphasize that financial institutions can benefit by leveraging their fraud resources with their AML efforts and by taking advantage of the significant efficiencies available through this leverage.

---

[10] *See* http://www.fincen.gov/news_room/rp/files/mortgage_fraud.pdf
[11] *See* http://www.cftc.gov/PressRoom/PressReleases/pr5616-09.html and http://www.cftc.gov/PressRoom/PressReleases/pr5610-09.html

Sharing Information Related to Fraud

Fraud generates dirty money. In order to be used by a criminal, the illicit source of that money needs to be cleaned and integrated into the legitimate financial system. The more information financial institutions can share with each other, the more the integrity of our financial system will be protected and law enforcement can gain additional sources of valuable information.

FinCEN has a unique authority under Section 314 of the USA PATRIOT Act to allow regulated financial institutions to share information with each other for the purpose of identifying and, where appropriate, reporting ***possible money laundering*** or ***terrorist activity***.[12]

We understand that some banks were hesitant to share information under the 314(b) program as it related to ***suspected fraud***. On June 16, 2009, FinCEN issued guidance to clarify the scope of permissible sharing covered by the section 314(b) safe harbor. The guidance clarifies that financial institutions, upon providing notice to FinCEN and using procedures designed to safeguard the information, are permitted to share information with one another. Sharing of information is permitted to identify and report activities, such as suspected fraud - or other specified unlawful activities (SUAs) - if they suspect there is a nexus between the suspected fraud or other SUA and possible money laundering or terrorist financing activity.[13] We expect this guidance to result in further exchange of information among financial institutions for the purpose of fighting fraud.

Ongoing FinCEN Outreach

FinCEN's holistic approach to fighting fraud involves not only the front-line people who work in financial institutions and have day-to-day contact with their customers, but also the leadership of an organization. In furtherance of these goals, FinCEN has an increased emphasis on industry outreach. We've taken steps to reach out to the various industries that must comply with the BSA. We've held and attended meetings around the country and visited many depository institutions and money services businesses to better understand their business models and concerns and needs as they work to ensure that legitimate business flourishes, while not inadvertently facilitating financial crime and terrorist financing. FinCEN then seeks to take this detailed knowledge and step back to look at the issues that transcend individual institutions and even industry sectors.

On the international front, FinCEN serves as the financial intelligence unit (FIU) of the United States and plays an active role within the Egmont Group, which is composed of 116 FIUs from around the world that work together to intensify international anti-money laundering collaboration and combat terrorist financing. FinCEN cooperates closely with its Egmont partners to provide analytical support in response to their case requests, as well as in broader strategic studies. FinCEN also works with FIUs to refer information requests on behalf of U.S. law enforcement agencies hoping to obtain additional information from abroad in support of their ongoing financial crime cases and investigations.

---

[12] *See* 31 CFR § 103.110

[13] *See* http://www.fincen.gov/news_room/nr/pdf/20090616.pdf

FinCEN is a member of a Department of Justice-led working group to address international mass marketing fraud. We are currently exploring ways in which we can help facilitate the sharing of information on fraud targets transnationally, and have requested information from our international partners within the Egmont Group to gain a better understanding of the type(s), and extent of, mass marketing fraud. FinCEN is also querying key terms within the SAR narrative to conduct a statistical analysis of those SARs that may involve suspected mass marketing fraud.

Our efforts in close cooperation with criminal investigators and prosecutors hold accountable those persons engaged in criminal activity. On an interagency basis, FinCEN is actively involved with a number of initiatives that focus on combating fraud: the Bank Fraud Working Group and the Mortgage Fraud Working Group, jointly sponsored by the Departments of the Treasury and Justice, respectively, and the President's Corporate Fraud Task Force, which is run out of the Department of Justice. FinCEN staff regularly brief the Mortgage Fraud Working Group on our latest mortgage fraud trends and patterns, and we have hosted the Bank Fraud Working Group for discussions on the issue. FinCEN also provides technical advice and analytical support to prosecutors at the Federal and State levels.

At every outreach opportunity, FinCEN works with our partners to communicate the importance of BSA requirements in fighting fraud and financial crime and keeping the nation secure. FinCEN participates in more than 100 conferences and events per year. Our Regulatory Helpline responds to thousands of requests every year from financial institutions seeking information and clarification on their BSA/AML responsibilities. FinCEN also works closely with our regulatory colleagues and relies on the existing expertise and examination functions of the regulators who know their industries best, and regularly participates in Federal Financial Institutions Examination Council workshops.

Conclusion

In concluding today, I want to emphasize that meaningful cooperation between the public and private sectors is a vital component in our collective efforts to guard against fraud and ensure the strength, safety, and integrity of the global financial system.

Again, what brought us all here today is that we all have a mutual concern about combating fraud, and I want to assure you that we at FinCEN are harnessing all of our authorities in this fight. We view this as a specific – and very important - part of our mandate to promote market integrity and help financial institutions protect themselves from fraud. Fighting fraud is also a key part of our efforts to build public confidence and promote economic growth.

Criminal methods to commit fraud are constantly evolving; our defenses against fraud must evolve as well, and those defenses are strongest when law enforcement and the private sector are working in concert. Your role, and the skills Certified Fraud Examiners bring to this fight, has never been more important. Thank you.

###