REMARKS OF JENNIFER SHASKY CALVERY
DIRECTOR
FINANCIAL CRIMES ENFORCEMENT NETWORK

MORTGAGE BANKERS ASSOCIATION
FRAUD ISSUES CONFERENCE

APRIL 15, 2013
HOLLYWOOD, FL

Good morning. I want to start by thanking our hosts, **THE MORTGAGE BANKERS ASSOCIATION,** for the opportunity to join you at this year's conference.

Strong public-private partnerships are critical for us to achieve success, particularly on an issue such as mortgage fraud. I cannot emphasize this fact enough. Our nation's financial institutions play a vital role in our efforts to safeguard the financial system from illicit use, combat money laundering, and promote national security. And we do this through the collection, analysis, and dissemination of financial intelligence and strategic use of our financial authorities.

FinCEN depends on the information financial institutions provide to us, and today I'd like to update you on how we are using this information to help our law enforcement partners combat mortgage fraud. FinCEN is a leader in the analysis of Bank Secrecy Act (or "BSA") data and financial intelligence. Our advanced analytic tools and highly skilled analysts play a unique role in analyzing and integrating BSA data and other information to accomplish three ends: (1) map illicit finance networks; (2) identify compromised financial institutions and jurisdictions; and (3) understand the current methods and schemes for illicit finance. These three key pieces of analysis are critical to enable our stakeholders – law enforcement, regulators, foreign partners, and industry – to take action against money laundering and the various types of illegal activity underpinning it -- such as mortgage fraud.

Suspicious activity reports ("SARs") on mortgage fraud filed by financial institutions continue to provide a wealth of information to law enforcement investigators all over the country.

Last October, the Financial Fraud Enforcement Task Force announced the results of their year-long initiative to target fraud schemes that preyed upon distressed homeowners. The initiative, launched by the FBI, resulted in 530 criminal defendants charged, including 172 executives. The cases involved more than 73,000 homeowner victims, with total losses by those victims estimated at more than $1 billion.

The Distressed Homeowner Initiative focused on fraud targeting homeowners, such as foreclosure rescue schemes that take advantage of homeowners who have fallen behind on their mortgage payments. Typically, the con-artist in such a scheme promises the homeowner that he can prevent foreclosure for a substantial fee, for example, by having so-called investors purchase the mortgage, or transferring title in the home to persons in league with the scammer. In the end, the homeowner can lose everything.

Other targets of the Distressed Homeowner Initiative include perpetrators of loan modification schemes who obtained advance fees from homeowners after falsely promising that they would negotiate more favorable mortgage terms on behalf of the homeowners.

The FBI generated new investigations by gathering victim complaint data from FTC databases and other sources, analyzing the data, and distributing information of lead value to field offices from coast-to-coast.

Another key tool for law enforcement: The SARs filed by alert financial institutions. Critical to the investigation were 4,395 SARs reporting “foreclosure rescue fraud.” These SARs were crucial to the law enforcement officials conducting these investigations. I’m sure many of these SARs were filed by the institutions represented in this room today, so I hope you know that they are making a real difference in the work being done by our law enforcement and regulatory partners.

Perhaps this would be a good time to touch on some preliminary mortgage loan fraud Suspicious Activity Report statistics for 2012. FinCEN received approximately 69,000 Mortgage Loan Fraud (or "MLF") SARs last year. This figure is a 25 percent decrease from the roughly 92,000 MLF SARs FinCEN received in 2011.

We attribute much of the decline to the relative dearth of “repurchase” related SARs addressing loans originated during the housing bubble. “Repurchase” SARs drove 2011’s spike in SAR filings, as opposed to reports about new occurrences of mortgage fraud. The number of mortgage loan fraud SARs with the term “repurchase” in the narrative spiked in 2011 to nearly 41,000 SARs. This figure was up significantly from the roughly 8,600 SARs filed in 2010. In 2012, “repurchase” SARs decreased to about 13,000.

In contrast, during 2011 and 2012, FinCEN continued to see dramatic growth in the number of SARs discussing “foreclosure rescue” scams in the narrative. In 2011, nearly 2,800 SARs indicated this activity, and in 2012, over 4,400 SARs reported this activity. Our analysis reflects that this could be partly a function of scammers finding opportunity in the distressed part of the mortgage market, as opposed to new loan origination. And it may also be the result of increased awareness of foreclosure rescue scams, given the focus on this issue during the past several years.

Third Party Payment Processors

FinCEN also continues to be an active member of the Financial Fraud Enforcement Task Force's Consumer Protection Working Group. And a focus of our fraud efforts this past year has been to highlight the fraud risks associated with third party payment processors.

While many third party payment processors provide legitimate payment transactions for reputable clients, we have also seen recent increases in criminal activity in this area. In addition to fraud, this activity includes money laundering, identity theft, and other illicit transactions.

Unfortunately, complicit Payment Processors provide fraudsters with access to the legitimate financial system by facilitating the movement of funds from the victim to the fraudulent merchant.

Of course, the risks will vary significantly depending on the makeup of the customer base. For example, Payment Processors providing consumer transactions on behalf of telemarketing and Internet merchants may present a higher risk profile to a financial institution than would other businesses. Telemarketing and Internet sales and transactions involving remotely created checks also tend to have a higher occurrence of consumer fraud. These customer relationships can pose increased risk to institutions and may require careful due diligence and monitoring.

FinCEN issued an Advisory last October to alert financial institutions of possible indicators of suspicious activity involving Payment Processors. This information was pulled together with the help of our federal, state, and local law enforcement partners. Some of the red flags we identified include:

High numbers of consumer complaints about Payment Processors and/or merchant clients, and particularly high numbers of returns or chargebacks (aggregate or otherwise), suggest that the originating merchant may be engaged in unfair or deceptive practices or **fraud**. This fraud includes using consumers' account information to create unauthorized remotely created checks or ACH debits.

Payment Processors engaged in suspicious activity often maintain **accounts at more than one financial institution**. Similarly, they may move from one financial institution to another within a short period. Such Payment Processors also may use multiple financial institutions and maintain redundant banking relationships in recognition of the risk to the Payment Processor and merchant that a financial institution may recognize the suspicious activity and terminate the Payment Processor and/or merchant accounts. In addition, regulators and law enforcement have recognized an increased use of "check consolidation accounts" by some Payment Processors. Consolidation accounts can be used by Payment Processors to conceal high return or chargeback rates from originating financial institutions and regulators.

Criminals are continually looking for ways to **launder illicit proceeds**, including the proceeds of consumer fraud. Payment Processors can be used by criminals to mask illegal or suspicious transactions and to launder proceeds of crime. In addition, Payment Processors have been used to place illegal funds directly into a financial institution using ACH credit transactions originating from foreign sources.

Payment Processors engaged in suspicious activity have also been known to solicit business relationships with **distressed financial institutions** in need of revenue and capital. Such Payment Processors may consider troubled financial institutions to be more willing to engage in higher-risk transactions. In some cases, Payment Processors also have committed to purchasing stock in these financial institutions to further induce the financial institution to provide banking services to high risk merchants. Often, the targeted financial institutions are smaller community banks that lack the infrastructure to properly manage or control a high-risk Payment Processor relationship. Fraudulent merchants also have been known to possess accounts through Payment Processors at large financial institutions.

Lastly, Payment Processors engaged in or complicit in suspicious activities may also reflect an **elevated rate of return** of debit transactions due to unauthorized transactions substantially higher than the average.

We will continue to work closely with our law enforcement and regulatory partners on this issue and we appreciate your help in spotting this activity.

Advanced Analysis

FinCEN's ability to conduct analysis on mortgage loan fraud and other crimes would be impossible without the BSA data financial institutions provide. In the very recent past, our analysts often needed to develop ad hoc tools to help analyze the data because our technical backbone was unable to sufficiently support the layers of tasks required to query, download, integrate, sort, connect, and chart the data.

Last fall, FinCEN began rolling out a key component in our IT Modernization Program to improve upon our ability to conduct analysis and make the BSA data available to a large number of federal and state agencies, including law enforcement and regulators. FinCEN Query allows users to easily access, query, and analyze 11 years of BSA data; apply filters to narrow search results; and utilize enhanced data capabilities. Our users are now able to look at the information more comprehensively, and we are excited to work with them in making sure that your filings become more valuable than ever before in this new system.

To give you an idea of the value of the information your institutions provide, in the months since FinCEN Query went live last September, there have been over 1.3 million queries of the BSA data by more than 7,000 users. This past Thursday alone, there were over 16,000 queries of the BSA data through FinCEN Query.

With our technology advancements, we are now getting closer to being able to leverage predictive analytics to take our work even further. This will provide us with the ability to work with our law enforcement partners, review their top completed investigations, understand the money laundering indicators present in our data, parse through the existing BSA forms, and then develop automated business rules that will allow us to provide agencies with new leads indicative of similar illicit activity elsewhere.

For example, FinCEN is working towards developing business rules based on information provided by our law enforcement and regulatory partners. Our goal is to dive deeper into aggregated regional and state level data to extract underlying drivers and trends between and among regions. We are doing this by automating the detection of regions and industries with significant changes, reviewing BSA records, and drilling down to understand which financial institutions are on the front lines of seeing changes in trends and patterns.

Moving forward, we expect to use the strategic application of business rules on the data industry provides to not only detect, but to "predict" where certain types of money laundering, such as the placement of dollars in connection with trade-based money laundering activities, might be manifested.

This type of predictive analysis will significantly improve our intelligence and enforcement efforts by allowing us to focus on those vulnerable regions or financial sectors where money laundering or financial crimes are most prevalent. Furthermore, it will allow us to provide new leads to law enforcement, alert our regulatory partners, and develop "red flags" for industry so we can provide feedback on the kind of information that would be helpful in their SAR reporting. It will also help us to target our own regulatory enforcement efforts. For example, I referenced our concerns about complicit Payment Processors earlier. Right now, a team of FinCEN analysts is using our new tools to identify SAR reporting trends with respect to this activity. Their efforts will help us better identify not just the complicit Payment Processors, but also the banks that may have "looked the other way" when facilitating their transactions. In December, we took joint action with the FDIC and the Department of Justice with respect to such an institution. We hope that there aren't many others in similar situations, but with our data and with continued inter-agency cooperation, we will work to identify them and take appropriate measures.

Universal SAR

In another aspect of our modernization, financial institutions were required to utilize the new FinCEN reports, including CTRs and SARs, starting April 1, 2013. The new FinCEN reports were specifically developed to work with the new FinCEN Query system that we just rolled out, and these new FinCEN reports allow us, law enforcement, and regulators to slice and dice the information submitted in a much more advanced way.

In developing the new "universal" FinCEN SAR form, we sought input from the regulators as well as law enforcement to obtain suggestions on additional categories of suspicious activity for inclusion. On the new FinCEN SAR, the suspicious activity information options have been expanded from 21 to more than 70, allowing the financial industry to provide more detailed information on the type of suspicious activity they are seeing.

In particular, with respect to possible mortgage fraud, several new categories have been added, allowing industry to report on the types of frauds of most interest to law enforcement. Instead of simply checking "mortgage fraud," financial institutions can now be more specific in terms of the type of fraud they suspect. For instance, the new form now includes boxes for:

- Reverse mortgage fraud;
- Loan modification fraud;
- Appraisal fraud; and
- Foreclosure rescue fraud.

While financial institutions were not required to begin using the reports until just a few weeks ago, it is encouraging to note that FinCEN received approximately 2,600 mortgage loan fraud SARs in 2012 using the new SAR form. With respect to the new forms, I want to point out in particular the guidance that we issued last March regarding the new fields.

The new FinCEN Currency Transaction Report (or "CTR") and FinCEN SAR do not create any new obligations or otherwise change existing statutory and regulatory expectations. Financial institutions must provide the most complete and accurate information known to them. They are not under an obligation to collect non-mandatory information simply because there is now a field for it. However, just as has always been the case, if financial institutions have information that is pertinent to a report, they need to be able to include it in the report, so that the CTR, SAR, or other FinCEN report is complete and accurate.

FinCEN has and will continue to provide additional guidance and training materials in support of the new reports through Webinars, FAQs, and other publications and materials.

The new reports are simply that – new. There will certainly continue to be some growing pains. But as a result of all the work that is being done within the industry, at FinCEN, and in collaboration with regulatory and law enforcement partners, the adoption of the new reports will prove extremely valuable to our shared fight against money laundering, terrorist financing, and other financial crimes -- such as mortgage fraud.

It also remains crucial that we continue to work to get the reports being filed into the right hands. FinCEN is currently working to provide direct BSA access to the Federal Housing Finance Agency (or "FHFA"), as well as the state insurance regulatory agencies. And as I mentioned earlier, FinCEN provides members of the Financial Fraud Enforcement Task Force and other law enforcement direct access to mortgage fraud SARs and analysis of the SARs to assist and support criminal investigations nationwide. When we can get the SAR data into the hands of more good users, it is certainly a step in the right direction.

Regulatory Update

I want to quickly update you on the regulatory side. As you know, last February, FinCEN finalized regulations requiring anti-money laundering program and SAR regulations for a specific subset of loan and finance companies: non-bank residential mortgage lenders and originators ("RMLOs"). The Final Rule went into effect almost exactly one year ago – on April 16, 2012 – and the compliance deadline was August 13, 2012. The SAR regulation requires reporting of suspicious activity, including but not limited to fraudulent attempts to obtain a mortgage or launder money by use of the proceeds of other crimes to purchase residential real estate.

While we typically wait 18 months after a rule is implemented to assess the impact, I wanted to provide you with a very preliminary snapshot on the filings we have seen since the compliance deadline last August. As I noted earlier, while MLF SAR counts are down about 25 percent from the record 2011 levels, we had more MLF SAR filers.

Specifically, we had 1,100 uniquely named filers of MLF SARs in 2012, up from 975 in 2011. That's a 13 percent increase in filers. The bulk of mortgage fraud SARs continue to be filed by the leading banks in the U.S. However, this data also suggests some of the smaller institutions, including RMLOs, are stepping up to report mortgage fraud. So we are making progress in bringing RMLOs into the SAR reporting system, and expect more as the industry gains experience with the rule.

In addition, in November 2011, FinCEN proposed regulations that would require government-sponsored enterprises (or "GSEs") Fannie Mae, Freddie Mac, and the Federal Home Loan Banks to develop anti-money laundering programs and file SARs with FinCEN. The GSEs currently file fraud reports with their regulator, the FHFA, which then files SARs with FinCEN when the facts in a particular fraud report warrant a SAR under FinCEN's reporting standards.

As proposed, the regulations would require that the GSEs file SARs directly with FinCEN, which will help streamline the reporting process, provide law enforcement with quicker access to data about potential fraud and other financial crimes, and result in the reporting of a wider range of suspected financial crimes. FinCEN is in the last stages of crafting final regulations for the GSEs.

Conclusion

As I mentioned at the outset, FinCEN can't do its work alone. Your financial institutions are the eyes and ears in the fight against terrorists, fraudsters, and other bad guys. The BSA data starts with you. It is the key to our defenses and we are depending on you. I am committed to maximizing our ability to be effective partners and colleagues.

FinCEN is a critical partner in the fight against money laundering and terrorist financing. Our talented and dedicated team is committed to that mission. We have an incredible opportunity to serve the American public and to contribute to the safety of this country and the world. FinCEN will meet the challenges ahead working together with you, law enforcement, and our regulatory partners. Thank you once again for inviting me here to speak with you today.

###