REMARKS OF JENNIFER SHASKY CALVERY
DIRECTOR
FINANCIAL CRIMES ENFORCEMENT NETWORK

NATIONAL CYBER-FORENSICS TRAINING ALLIANCE
CYFIN 2013 CONFERENCE

APRIL 16, 2013
PITTSBURGH, PA

Good morning. I want to start by thanking our hosts, **THE NCFTA,** for the opportunity to join you at this year's **CyFin Conference**.

For those of you that might not be familiar with the work being done at the Financial Crimes Enforcement Network, known as FinCEN, I wanted to spend just these first few minutes giving you a broad overview of our agency, as well as the information that we use to do our work.

FinCEN is a part of the Treasury Department, and reports to the Office of Terrorism and Financial Intelligence. With approximately 300 employees, we are relatively small considering our broad responsibilities. FinCEN's mission is to safeguard the financial system from illicit use and combat money laundering and promote national security through the collection, analysis, and dissemination of financial intelligence and strategic use of financial authorities.

FinCEN carries out this mission by receiving and maintaining certain financial transactions data; analyzing and disseminating those data for law enforcement purposes; and building global cooperation with counterpart organizations in other countries.

So, where does FinCEN get its data? Another key aspect of FinCEN's mission is to administer and issue regulations pursuant to the Bank Secrecy Act (BSA). The BSA requires a broad range of U.S. financial institutions, which includes traditional depository institutions, money services business, such as Western Union, Money Gram, and PayPal, casinos and some card clubs, insurance companies, securities and futures brokers, precious metals/jewelry industry, and some trades or business, like car dealerships, to assist U.S. government agencies in the detection and prevention of money laundering. Financial institutions do this by maintaining records and filing reports with FinCEN.

The two primary reports FinCEN collects from financial institutions are Currency Transaction Reports (CTRs) and Suspicious Activity Reports (SARs). CTRs must be filed on all

cash transactions exceeding $10,000. In 2012, there were over 14 million CTRs filed by financial institutions around the country.

SARs are reports of suspicious transactions. While the dollar thresholds differ slightly by industry, generally speaking, if a financial institution "knows, suspects, or has reason to suspect" that any transaction or attempted transaction is suspicious, and the transaction or attempted transaction involves or aggregates to funds of $5,000 or more, a SAR is required. Last year, 1.4 million SARs were filed with FinCEN.

Overall, FinCEN's BSA data includes nearly 190 million records with approximately 16 million records added each year. Without the financial institutions that report this information, FinCEN literally could not do its job. Their role is vital in our efforts to safeguard the financial system from illicit use, combat money laundering, and promote national security.

FinCEN is a leader in the analysis of 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 ultimately 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, terrorist financing, and cyber threats.

FinCEN's analysis depends primarily on the excellent information financial institutions provide – it is the baseline from which our analysts work. What our analysts do now – and do very well – is look across those data to find interconnections to support ongoing law enforcement cases, to find trends and patterns within those data, and to understand the overall changes and shifts within them. They also combine those findings with other information sources, such as law enforcement data or publicly available data, and enhance the picture.

Where our analysts are going – and we're not there yet, but we are on the cusp of these capabilities – is to take our analysis to a whole new level. Currently, we are capable of dissecting law enforcement and BSA information to identify a specific methodology for illicit finance in a particular segment of the financial industry related to a particular type of crime. We are also capable of using such information to identify entirely new and unknown bad actors engaged in similar activity in other parts of the country.

However, right now this is long and arduous work as analysts sift through hundreds and sometimes thousands of reports. Very soon, new capacities made possible by our internal technology modernization will allow our analysts to deal with such data sets to find leads in a fraction of the time previously necessary. Very soon, we will be able to point law enforcement and other stakeholders precisely to where they should be looking. Our analysts, working hand-in-hand with our superb technology team, are now putting these new capacities into place.

Having seen the initial results from our new capabilities, I am excited about where we are headed. I am committed to making this a central role for FinCEN in the 21st Century. So today, I'd like to talk to you about some of the work we are doing, and where our cutting-edge

analytical efforts are taking us, as we seek to remain out in front of emerging payment systems and use our advanced analytical capabilities to combat cyber threats.

Emerging Payment Systems

I'd like to begin today by discussing how FinCEN's analysts are working hard to stay ahead of the curve in understanding emerging payment systems and related financial flows and vulnerabilities and to put that information into the hands of those customers who need it most.

As we all know, during the past decade, the development of new market space and new types of payment systems have emerged as alternatives to traditional mechanisms for conducting financial transactions, allowing developing countries to reach beyond underdeveloped infrastructure and reach those populations who previously had no access to banking services. For consumers and businesses alike, the development and proliferation of these systems are a significant continuing source of positive impact on global commerce.

These new systems have also expanded the boundaries of "money transmission" as more sophisticated payment systems have become available. And the inherent added complexity of these systems opens them to potential misuse by criminals.

FinCEN's analysts are continually working to understand the schemes and methods used to exploit emerging payment methods for money laundering and terrorist financing, and to develop related guidance for law enforcement. This guidance provides law enforcement with information on key sectors' operations, recordkeeping practices, and efforts to identify and counter vulnerabilities.

Partnership is crucial. As our analysts develop their understanding of these new systems, they are significantly aided by working directly with the financial industry. This partnership enables them to better follow financial trails and realistically understand financial mechanisms.

Crypto-Currencies

For instance, FinCEN's analysts just recently finalized a bulletin that explores the relatively new payment technology of digital currency systems. FinCEN's bulletin helps "de-mystify" the digital currency realm by explaining to the broader law enforcement community how these systems work. The bulletin also addresses the role of traditional financial institutions as intermediaries for these new payment methods.

We're viewing our analytic work in this space as an important part of an ongoing conversation between industry and law enforcement. While probably most of today's audience understands what these emerging payments systems are and how they work, many line analysts, investigators, and prosecutors in law enforcement may not, and part of FinCEN's role is to help be the bridge to explain these new systems. FinCEN is dedicated to learning more about digital currency systems, along with other emerging mechanisms, to protect those systems from abuse and to aid law enforcement in ensuring that they are getting the leads and information they need to prosecute the criminal actors. As our knowledge base develops, in concert with you, we will

look to leverage our new capabilities to identify trends and patterns among the interconnection points of the traditional financial sector and these new payment systems.

In addition to developing products to help law enforcement follow the financial trails of emerging payments methods, FinCEN also develops guidance for the financial industry to clarify their regulatory responsibilities as they relate to emerging areas.

Virtual Currencies

In fact, just last month, FinCEN issued interpretive guidance to clarify the applicability of BSA regulations to virtual currencies, such as Bitcoin, which has in recent weeks gained significant attention. The guidance responds to questions raised by financial institutions, law enforcement, and regulators concerning the regulatory treatment of persons who use virtual currencies or make a business of exchanging, accepting, and transmitting them.

FinCEN's rules define certain businesses or individuals as money services businesses (MSBs) depending on the nature of their financial activities. MSBs have registration requirements and a range of anti-money laundering, recordkeeping, and reporting responsibilities under FinCEN's regulations. The guidance considers the use of virtual currencies from the perspective of several categories within FinCEN's definition of MSBs.

The guidance explains how FinCEN's "money transmitter" definition applies to certain exchangers and system administrators of virtual currencies depending on the facts and circumstances of that activity. Those who use virtual currencies exclusively for common personal transactions like receiving payments for services or buying goods online are not affected by this guidance.

Those who are intermediaries in the transfer of virtual currencies from one person to another person, or to another location, are money transmitters that must register with FinCEN as MSBs unless an exception applies. Some virtual currency exchangers have already registered with FinCEN as MSBs, though they have not necessarily identified themselves as money transmitters. The guidance clarifies definitions and expectations to ensure that businesses engaged in similar activities are aware of their regulatory responsibilities and that all who need to, register appropriately.

Uncovering Cyber Trends and Patterns

FinCEN depends on the information financial institutions provide to us, and today I'd like to focus on what our analysts do with that information. In addition to providing case support, some of you may know that FinCEN has, for many years, carried out trends and pattern analyses of the information contained in the millions of SARs and CTRs that financial institutions send to FinCEN annually.

Account Takeovers

For instance, as an example of our tactical case support, a FinCEN analyst recently provided analytical case support to a federal law enforcement agency on an international cybercrime investigation. The investigation involved the use of computer intrusion techniques and malware to facilitate the unauthorized transfer of funds from legitimate small business accounts to "temporary accounts" created solely for this purpose and subsequently closed or abandoned after the illicit activity was conducted. There were more than 50 attempted transfers over a four month period, including more than two dozen successful transfers resulting in the theft of almost $850,000. The suspects used multiple banks and accounts and targeted several small businesses ranging from a law firm to a landscaping company. Financial institutions filed more than 40 SARs and 20 CTRs detailing the illicit activity and movement of funds. Based on this information, the analyst was able to identify what appeared to be a network of individuals with connections to Russia and Eastern Europe involved in the cybercrime scheme.

We all know that account takeovers via Zeus or other malware have been plaguing victims and financial institutions for years. This is an area where I know there are opportunities for FinCEN to contribute and for us all to work together. While FinCEN issued an advisory on this issue in 2011, we must continue to head in a direction analytically where we will be able to identify trends and indicators, as well as actual targets, within the BSA data. What is exciting about this is that there is a real opportunity to harness our analytical capabilities to undermine account takeovers. In addition, we recognize that our data, though a key piece of the puzzle, are not the whole of the picture – we are looking forward to working with partners in law enforcement and industry to tackle the increasing costs of cyberfraud.

Third Party Payment Processors

FinCEN has also been working to identify and address the risks associated with third-party payment processors (TPPPs). While many third party payment processors provide legitimate payment transactions for reputable clients, we have also seen significant criminal activity involving TPPPs. This includes fraud, money laundering, identity theft, and other illicit transactions, including in particular schemes to facilitate spam-based marketing schemes, for example for pharmaceuticals. TPPPs deserve scrutiny because cybercriminals rely on them to get paid, making them a crucial node in the cybercrime business model, and because they may be more amenable to regulatory and enforcement efforts than other segments of that model, for example individual cybercriminals, corporations, and suppliers of goods or services. Targeting TPPPs also can lead us to the banks that are complicit in cybercrime, and such institutions are highly vulnerable and deserving of enforcement action.

Of course, the risks associated with individual TPPPs vary significantly depending on the make-up 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 (RCC) 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 the roles certain unscrupulous processors continue to play to commit or facilitate a range of criminal activities. Our review of a small group of BSA filings since the October Advisory shows these illicit activities, which often also involved the participation of banks, money services businesses, shell corporations, and a wide-range of Web site-hosting and/or support entities located in the United States and about 27 other countries.

Many of the errant TPPPs reportedly stole funds directly from consumer financial accounts through their initiation of unauthorized ACH debits or RCCs, often made possible through computer intrusion and identity theft. Others facilitated the collection and/or layering of illicit funds generated on Web sites touting Internet gambling, child pornography, pharmaceuticals, and investment scams. Some filers also reported smaller, mainly foreign-based, TPPPs that used larger independent exchange providers to clear payments to individuals and merchants who offered products and services on the Internet.

Many of these merchants failed to receive payment and were left with the difficult task of trying to determine which processor actually stole their funds. Within the group of BSA filings read, we identified millions of dollars in wire transfers to or from Internet-based companies in the United States and countries known for child exploitation, human trafficking, illicit pornography, illegal diamond trading, and tax avoidance.

We will continue to work in close partnership with our financial industry and law enforcement partners to raise awareness of this ongoing activity.

Advanced Analytics

While FinCEN has had much success in the analytical area, we do face our share of technical challenges to produce timely, cogent, and actionable intelligence products, useful to both our policy leaders and to field personnel. Filing protocols and the data within FinCEN reports vary from form to form, particularly with respect to those forms filed by individuals, as opposed to financial institutions.

Because of these variances, FinCEN analysts must find innovative solutions to match and fuse data as part of their mapping of illicit finance networks, identification of compromised financial institutions and jurisdictions, and understanding of schemes and methods for illicit finance.

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 – more than 180 million reports.

The system allows users to 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 filings become more valuable than ever before in this new system.

To give you an idea of the value of the information financial 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 also to "predict" where certain types of cyber crime, may be taking place and to cut off this activity before if begins.

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.

We are beginning to touch the very early parts of this capability; we are very excited to be heading in this direction and I greatly look forward to seeing the products when we are able to reach full implementation.

Without strong public-private partnerships, none of the work we are doing would be possible. So, I'd like to close-out my remarks today discussing our efforts in this area.

Public-Private Partnerships

The NCFTA clearly recognizes that to combat an issue as complex as cyber fraud, you must engage with partners on all fronts. The CyFin Initiative, which brings industry, law

enforcement, and academia together to share information addressing cyber threats aimed at the financial services industry, is key. I could not agree more strongly with this approach, and have made fostering strong public-private partnerships a cornerstone of my efforts as Director of FinCEN.

The Delta Team

One of my first initiatives upon arriving at FinCEN last fall was to being looking at how we could form stronger partnerships with our industry, regulatory, and law enforcement partners. We know financial institutions spend a great deal of time and money to comply with the BSA. And while I know it is worth it, we need to ask ourselves if the money is being spent in the right ways and ask ourselves hard questions. How does compliance risk compare with the actual illicit financing risk? What is the delta between the two?

Fortunately, FinCEN has a productive forum in which to have these discussions. The Bank Secrecy Act Advisory Group, or BSAAG, is comprised of high-level representatives from financial institutions, federal law enforcement agencies, regulatory authorities, and others from the private and public sectors. We meet twice a year to discuss issues relating to the administration of the BSA and to make policy recommendations to the Secretary of the Treasury.

The purpose of the Delta Team is for industry, regulators, and law enforcement to come together and examine the space between compliance risks and illicit financing risks. The goal is to reduce the variance between the two. To the extent we are successful, we will be building a smarter, more effective, and more cost efficient system. If we are successful we will have our eyes squarely on the ball, protecting our financial system from illicit finance and combating serious criminal and national security threats.

The Delta Team held its first meeting in February in FinCEN's Washington, D.C. offices. We had a very productive first meeting, with an exchange of views on risks and the beginning of discussions on practical steps that address these risks.

As part of this meeting, which consisted of a broad cross-section of industry, regulators, and law enforcement agencies, we facilitated discussions among smaller breakout groups aligned by industry sector. One thing in particular that I found striking was that although these industry breakout sessions provided a forum to raise and discuss industry-specific concerns and ideas, there was a lot of consistency in the themes raised by the different financial industry components.

A common theme from participants was that additional information on money laundering trends, including more specifics on schemes and methods for illicit finance and red flags, would be helpful in aligning industry efforts with law enforcement priorities. For those of you who are not aware, FinCEN puts out advisories to financial institutions that contain information on different schemes and methods for illicit finance and red flags for which financial institutions should be on the lookout. When done well, these advisories drive reporting, which in turn enables FinCEN to use its advanced analytics to provide additional and, hopefully, even better analysis for law enforcement and other stakeholders.

Another common theme that arose from the Delta Team meetings -- and something at which I believe the NCFTA is already quite good -- is the need to find ways for more dynamic, real-time information sharing by and between financial institutions, and also with FinCEN and law enforcement. The Patriot Act provides certain safe harbors for financial institutions to engage in such sharing of information, but I believe the prevalent view is that the current mechanisms for doing so are overly clunky and bureaucratic. Through the Delta Team we are considering ways to achieve the dynamic, real-time sharing that we all see is necessary to combat today's criminal and national security threats.

I look forward to continuing these valuable discussions in order to identify meaningful actions for FinCEN and other agencies to consider over the coming months.

International Partnerships

In the intelligence area, FinCEN also plays a role in fostering strong public/private partnerships. Here too, FinCEN serves as global experts on illicit finance, providing data-driven tactical and strategic perspectives and engaging our international partners to disrupt threats to the U.S. financial system. FinCEN serves as the Financial Intelligence Unit, or FIU, for the United States. But the United States is just one member of the Egmont Group of Intelligence Units, a group of 131 FIUs located around the world.

These 130 FIUs are important partners to FinCEN. While each FIU is a bit different in terms of organization and responsibilities, all Egmont-member FIUs commit to serve as a national, central authority that receives and analyzes disclosures of financial information, particularly suspicious transaction reports, and disseminates the results of the analysis to combat money laundering and terrorist financing.

The unique role that FinCEN plays in this space is that we serve as a conduit for information flow between U.S. law enforcement and each of these 130 jurisdictions. And when it comes to the cyber area, our ability to open the door to information that law enforcement could otherwise not access, can pay great dividends. Just as FinCEN receives a large amount of valuable reporting from the private sector, each FIU receives analogous reporting from its own domestic reporting entities. Only by working collaboratively with our FIU counterparts can we find commonalities across these datasets.

Just in the past few weeks, we've been working with a U.S. law enforcement agency and one of our foreign counterparts to help seize approximately $1.4M USD which had been fraudulently transferred from the bank accounts of two U.S. companies as a result of computer intrusion. FinCEN passed information allowing our foreign counterpart to keep the money frozen while U.S. law enforcement begins the legal process of getting the funds repatriated to the victims. While this work remains ongoing, to date, nearly $1 million has been returned to one of the victimized businesses.

These are just a few ways that FinCEN works to build strong partnerships – in concert with you we could more fully understand the current methods and schemes for illicit finance in

the cyber realm and more strongly combat shadowy illicit actors. Our combined expertise could also inform the development of predictive models to exploit the data for previously unidentified networks of illicit activity associated with cybercrime. So we hope this is just the first step in what will be an ongoing relationship.

Conclusion

My remarks today have focused extensively on the work being done by FinCEN's analytical team – not only their ongoing efforts, but where we are heading in the future. From the time I arrived at FinCEN, I have been continually impressed by the fascinating work our analysts are doing, and even more so, by their dedication each and every day to FinCEN's mission, and their desire to make a real difference as public servants.

As the escalation of transnational criminal threats to the U.S. financial system has increased, so too has the imperative to ensure that FinCEN is fully maximizing its potential to disrupt this activity. I am hopeful that my remarks today have given you new insight into the team at FinCEN working to respond to these threats.

But we can't do it alone. Strong public-private partnerships are vital. That is why being here today, having the opportunity to hopefully meet with many of you throughout the day, and learn how we could better work together, is so important. Keeping this dialogue going will benefit all of us. And I am certainly committed to maximizing our ability to be effective partners and colleagues.

Thank you once again for inviting me here to speak with you today.

###