REMARKS OF JENNIFER SHASKY CALVERY
DIRECTOR
FINANCIAL CRIMES ENFORCEMENT NETWORK

2014 MID-ATLANTIC AML CONFERENCE
WASHINGTON, DC
AUGUST 12, 2014

Good morning. I am honored to be a part of this year's conference, which brings together law enforcement, the regulatory community, and the financial industry. I would like to thank everyone on the planning committee who worked to pull together such a compelling agenda for this event. I know I am the first of several FinCEN speakers you will be hearing from today, and we are looking forward to engaging with all of you. While each agency or institution represented here may approach anti-money laundering (AML) issues from a different perspective, and have its own unique challenges, an event such as this shows us that we all have the same ultimate goal in mind.

As you likely already know, the Bank Secrecy Act, or "BSA," is the common name for a series of statutes and regulations that form this country's anti-money laundering and countering the financing of terrorism laws. Nearly every country around the world has similar laws in place at this point. These laws are meant to protect the integrity of the financial system by leveraging the assistance of financial institutions to make it more transparent and resilient to crime and security threats, and to provide information useful to law enforcement and others to combat such threats.

Indeed, the threats that we face in the United States are quite serious and provide the context for why we must work together effectively. The information financial institutions provide is used to confront terrorist organizations, rogue nations, WMD proliferators, foreign grand corruption, and increasingly serious cyber threats, as well as transnational criminal

organizations, including those involved in drug trafficking, and massive fraud schemes targeting the U.S. government, our businesses, and our people.

Against this backdrop, I would like to discuss some of the challenges we need to address together as we work to combat these threats. While we might not leave here today with all of the answers, sometimes the hardest part is just starting the dialogue. And that is what I hope to do today.

First, I would like to address the challenge of implementing a risk-based approach to money laundering. Our AML regime is risk-based, because each and every financial institution – from its products, to its customers, to its internal procedures – is different. And because of these differences, it would be impossible to have a one-size-fits-all approach. I can appreciate that a prescriptive yes-or-no/check-the-box exercise may seem easier. I can also appreciate that a risk-based approach can create some uncertainty.

However, to be truly effective, every financial institution needs to consider its own products and practices, assess its own risks, and develop a program that works best for the particular financial institution to mitigate its unique risks.

Recently, we have been hearing about instances of "de-risking," where money services businesses (MSBs) are losing access to banking services because of perceived risks with this category of customer and concerns about regulatory scrutiny. Some financial institutions also state that the costs associated with maintaining these accounts outweigh the benefits. But just because a particular customer may be considered high risk does not mean that it is "unbankable" and it certainly does not make an entire category of customer unbankable. Banks and other financial institutions have the ability to manage high risk customer relationships.

It is not the intention of the AML regulations to shut legitimate business out of the financial system. I think we can all agree that it is not possible for financial institutions to eliminate all risk. Rather, the goal is to provide banking services to legitimate businesses by understanding the applicable risks and managing them appropriately.

MSBs play a vital role in our economy and provide valuable financial services, especially to individuals who may not have easy access to the formal banking sector. In fact, FinCEN and our regulatory partners first addressed this issue in 2005 when we learned that MSBs were having difficulty maintaining bank account relationships. In response, FinCEN and the Federal Banking Agencies issued joint guidance to assist banking organizations assess and minimize risks posed by providing banking services to MSBs. This guidance, which I would like to emphasize still remains in effect today, states:

> "While recognizing the importance and diversity of services provided by money services businesses, the guidance to banking organizations specifies that FinCEN and the Federal Banking Agencies expect banking organizations that open and

> maintain accounts for money services businesses to apply the requirements of the Bank Secrecy Act, as they do with all accountholders, on a risk-assessed basis… Through the interpretive guidance, FinCEN and the Federal Banking Agencies confirm that banking organizations have the flexibility to provide banking services to a wide range of money services businesses while remaining in compliance with the Bank Secrecy Act."

FinCEN is joined by the Federal Banking Agencies in continuing to support the applicability of this guidance. Recently, officials from both the Federal Reserve Board and Office of the Comptroller of the Currency underscored in Congressional testimony that the joint guidance issued in 2005 remains in effect today. Scott Alvarez, the Federal Reserve Board's General Counsel, stated: "That [the] guidance confirms that banking organizations may provide banking services to MSBs that operate lawfully. The guidance is intended to assist banks in the decision to open and maintain accounts for legitimate businesses by identifying the programs and procedures they should have in place to perform customer due diligence and monitoring of these customers for suspicious activity."

It is worth noting that with limited exceptions, MSBs are subject to the full range of BSA regulatory controls, including the anti-money laundering program rule, suspicious activity and currency transaction reporting rules, and various other identification and recordkeeping rules. Additionally, existing FinCEN regulations require certain money services business principals to register with FinCEN. As a result, MSBs play an important role in implementing procedures to thwart serious illicit activity that, left unchecked, could jeopardize the U.S. financial system. MSBs also play an important role in providing crucial reporting used to combat a wide range of criminal and security threats.

In fact, MSBs submit to FinCEN a significant number of Suspicious Activity Reports (SARs). In 2013 alone, MSBs filed more than 490,000 SARs, compared to 713,000 filed by depository institutions. And while I am not able to discuss specifics, I can say that the BSA reporting provided by MSBs contains some of the most valuable counterterrorism information we receive.

As with all of our regulated financial institutions, where particular MSBs fail to meet their BSA responsibilities, the organization and its individual partners, directors, officers, and employees are subject to possible civil and criminal penalties. FinCEN has the authority to bring civil actions in such circumstances and will continue to do so where we see pervasive and systemic, or egregious, failures. In fact, just last month, FinCEN assessed a civil money penalty against an MSB in Georgia in response to repeated violations of the BSA that persisted even after notification of the violations by examiners. As financial institutions, MSBs cannot ignore either their AML responsibilities or their examiners. They should also realize that banks will be more willing to do business with those MSBs that take their BSA obligations seriously.

While we are hearing reports of de-risking, we do not yet know how widespread it is, and we are still working to gauge the impact. FinCEN continues to meet informally with industry representatives and other experts to explore additional ways to gather feedback on the issue. We are also hearing that some within the financial industry are working independently to study and scope the problem. One idea that has been discussed is the possibility of MSBs, depository institutions, and their respective trade associations coming together and developing a set of industry best practices, which if adopted by an MSB, could provide a depository institution with more comfort in offering banking services. We are also considering the merits of updating the 2005 guidance to banks on providing services to MSBs. And we are looking forward to exploring how the Money Remittances Improvement Act of 2014, which was signed into law by the President last week and authorizes FinCEN to rely on examinations of financial institutions conducted by State supervisory agencies, can positively impact this issue.

All this is to say that a risk-based approach is not black and white. A key aspect of FinCEN's mission is to collect reporting from financial institutions and get this information into the hands of our law enforcement and regulatory partners. The only way we can do our job is if businesses actually have bank accounts and their transactions are monitored and reported to FinCEN, as appropriate. This is critical to what we do, because of the indisputable value the BSA reporting provides to investigations. And for those of you who are not sure that the value BSA reporting provides to investigations is indisputable, hold that thought, because I will be returning to that topic in a moment.

While we need financial institutions to provide us with transparency, we also ask financial institutions to help us keep dirty money from contaminating not only their institutions, but our financial system as a whole. I can appreciate that these two messages are at odds with each other, but we need to find a balance between the two; a balance where we receive valuable BSA reporting, but where a financial institution also feels it has effectively managed its risk in making decisions about maintaining a relationship with its customers.

Nothing illustrates this point better than FinCEN's recent guidance on the provision of financial services to marijuana-related businesses in states where such business is legal under state law. Our overarching goal in issuing this guidance was to promote financial transparency, ensuring law enforcement receives the reporting from financial institutions that it needs to police this activity and making it less likely that the financial operations move underground and become more difficult to track.

Since FinCEN's guidance went into effect in February of this year, we have received more than 1,000 SARs that indicate banks are using our guidance and providing much needed transparency into their dealings with marijuana-related businesses. And based on a review of SARs filed between February 14 and August 8, 2014, there are currently 105 individual financial institutions from states in more than one third of the country engaged in banking relationships with marijuana-related businesses.

FinCEN's guidance assists financial institutions in determining when and how to file a SAR based on eight law enforcement priorities identified by the U.S. Department of Justice. Financial institutions providing financial services to a marijuana-related business that it reasonably believes, based on its customer due diligence, does not implicate one of the eight priorities or violate state law should file a SAR using the phrase "Marijuana Limited" in the narrative. Since issuing the guidance, FinCEN has received 502 SARs marked as "Marijuana Limited." A financial institution filing a SAR on a marijuana-related business that it reasonably believes, based on its customer due diligence, implicates one of the eight priorities or violates state law should file a SAR with the phrase "Marijuana Priority" in the narrative. To date, FinCEN has received 123 SARs indicating "Marijuana Priority." Lastly, if a financial institution deems it necessary to terminate a relationship with a marijuana-related business in order to maintain an effective anti-money laundering compliance program, it should file a SAR and note in the narrative the basis for the termination, using the term "Marijuana Termination" in the narrative. Just over 475 SARs filed to date reflect "Marijuana Termination."

So, from our perspective the guidance is having the intended effect. It is facilitating access to financial services, while ensuring that this activity is transparent and the funds are going into regulated financial institutions responsible for implementing appropriate AML safeguards.

It is in this vein of transparency that I want to discuss in more detail the value of BSA reporting. As noted earlier, the reporting and transparency required of financial institutions under the BSA provide some of the most important information available to law enforcement and other agencies safeguarding the United States.

BSA reporting – particularly SARs – continues to play an integral role in law enforcement investigations at both the federal and state levels. Generally speaking, law enforcement uses the reporting in four key ways.

First, law enforcement uses the reporting as tips to initiate investigations. The BSA reporting contributes critical information that is routinely analyzed, resulting in the identification of suspected criminal activity and the initiation of investigations. For instance, more than 100 SAR review teams and financial crimes task forces across the country bring together investigators and prosecutors from different agencies to review reporting related to their geographic area of responsibility and initiate investigations. In the second quarter of FY 2014 alone, these teams reviewed a total of over 180,000 SARs of the more than 290,000 SARs filed during that same period, which is a rate of approximately 62 percent.

Second, law enforcement uses the reporting to expand existing investigations. The reporting aids in expanding the scope of ongoing investigations by pointing to the identities of previously unknown subjects, exposing accounts and hidden financial relationships, or revealing other information such as common addresses or phone numbers that connect seemingly unrelated

participants in a criminal or terrorist organization and, in some cases, even confirming the location of suspects.

In the first six months of 2014 alone, over 350 unique agencies, representing a broad cross section of federal, state, and local law enforcement and regulators operating nationwide, accessed BSA reporting via FinCEN Query. Thousands of agents, analysts, and investigative personnel from each of these agencies have conducted in excess of 1 million queries against the database during that period. In fact, reviewing our numbers, it appears that more reports are likely reviewed by law enforcement and other users, on any given day, than are filed by financial institutions.

The Federal Bureau of Investigation (FBI), which is a very active user of BSA information, reports that in the past month alone, approximately 2,500 new BSA reports are directly relevant to over 1,100 of their ongoing investigations. Between March 2013 and April 2014, 34% of the FBI's cases on organized crime and drug trafficking organizations were found in BSA filings. The same can be said for 28% of the Bureau's transnational organized crime cases, as well as 15% of their international terrorism cases. And while we talk a great deal about the value of SARs, it should also be noted that over this same time period, the Bureau tells us that 73% of the BSA reports related to their investigations were actually Currency Transaction Reports.

Third, law enforcement uses the reporting to facilitate international information exchange and conduct enforcement in a globally connected world. The Egmont Group has developed mechanisms for the rapid exchange of sensitive information between 146 financial intelligence units (FIUs), like FinCEN, around the world. In FY 2014, based on current trends, it is estimated that FinCEN will receive approximately 1,300 incoming Egmont requests from foreign FIUs seeking information derived from BSA reporting and will make approximately 700 outgoing Egmont requests on behalf of U.S. law enforcement agencies seeking similar information from foreign FIUs.

Fourth, law enforcement uses the reporting to identify significant relationships, patterns and trends. The reporting unmasks the relationships between illicit actors and their financing networks enabling law enforcement to target the underlying conduct of concern, and to use forfeiture and sanctions to disrupt their ability to operate and finance their illicit conduct. The same information can also help an institution protect itself and aid law enforcement in protecting the institution from bad actors, including insider threats, frauds, and cyber-related threats such as spear phishing, account takeovers, and distributed denial of service attacks.

For example, in November 2012, a regional bank in northern Florida had nearly $7 million fraudulently wired out of one of its accounts. The bank maintained an account at a larger correspondent bank – a bank that provides services to other banks rather than to businesses or individuals. A single wire for the nearly $7 million was initiated from the correspondent bank

account to an account in Switzerland. Although the correspondent bank's records show that the wire was initiated by an employee of the Florida bank, that employee denied initiating or authorizing the wire transfer. Subsequent FBI investigation confirmed that a computer at the Florida bank was infected with the "GameOver Zeus" (GOZ) virus, and that the infected computer was used to steal the credentials that were used to initiate the fraudulent transfer.

SARs filed by several different financial institutions played a vital role in furthering the investigation. The SARs helped the FBI identify several wire transfers related to one co-conspirator involved in a large scale money laundering organization acting on behalf of GameOver Zeus, which, in turn, led to further significant investigative gains.

The total losses associated with this GOZ botnet are believed to exceed $100 million in the United States alone. The group responsible is based in Russia and Ukraine, and deliberately targeted their malicious software at U.S. individuals and companies.

So, as you can see, BSA reporting does not go into a "Black Hole" as suggested by some in the financial industry, but rather is used extensively by law enforcement and other government agencies. Indeed, part of instituting a culture of compliance at a financial institution is ensuring that personnel at all levels understand the purpose and usefulness of BSA reporting.

Looking at BSA filing statistics as a whole also provides helpful insight. Last month, FinCEN released the first edition of *SAR Stats*, a successor publication of *The SAR Activity Review – By the Numbers*, which provides statistical information following the adoption of the unified SAR form and the implementation of E-filing. More than 1.3 million SARs filed between March 1, 2012 and December 31, 2013 were analyzed as a part of this effort, and the reporting provides a new baseline for financial sector reporting on suspicious activity. In the first few weeks of the publication being posted to FinCEN's website, it was viewed over 130,000 times, which is yet another statistic that tells us that this kind of information is of interest and valuable.

Not only do we think that the *SAR Stats* format is easier to navigate for our stakeholders, it also includes richer information based on the new SAR format. Here's an example of that richness. In the past, it was more difficult for us to focus specifically on structuring, and in particular the amount of structuring that related to other suspicious activity versus so-called "idiosyncratic structuring," where people may be breaking up transactions simply because they feel that the government has no business knowing anything about their transactions. Structuring is illegal either way, as we have made clear in a brochure that is available for financial institutions to share with their customers. But clearly, it is important for us to recognize the distinctions here, and it is something that we now feel will be easier to understand.

So when we talk about the value of the BSA reporting to law enforcement, the statistics and success stories speak for themselves. But these same stats and stories also illustrate the tension we are facing when we discuss de-risking. If banks cut businesses off from the financial

system, we lose the financial intelligence that is so crucial to combating a wide range of criminal and national security threats. How do we balance this tension between maintaining valuable reporting while also keeping bad actors out of the U.S. financial system so that they cannot exploit it to further their nefarious ends? Clearly, there are no easy answers here but the stakes are high and we need to continue engaging in an open and honest dialogue to get that balance right.

The information that financial institutions provide, the resiliency that they establish with respect to illicit actors, and the value of the reporting, brings me right back to the importance of transparency. Over the last month, FinCEN has taken several significant actions aimed at increasing transparency in the financial system and assisting law enforcement in its efforts to confront criminal and national security threats.

A few weeks ago, FinCEN issued a Notice of Proposed Rulemaking (NPRM) that would clarify and strengthen Customer Due Diligence (CDD) obligations for financial institutions, including a requirement that they identify the individuals who ultimately own or control accounts held in the name of legal entities. The proposed rule will enhance financial transparency in multiple ways. It will increase the availability of beneficial ownership information to law enforcement and thereby assist law enforcement investigations. It will increase the ability of financial institutions and law enforcement to identify the assets of illicit actors, and further help financial institutions better assess and mitigate risk. The proposed CDD rule will also strengthen consistency in the application of FinCEN's regulations across industry sectors.

The proposed rule builds on substantial industry outreach, including five hearings around the country. It follows the issuance in 2010 of guidance on a risk-based approach to the collection and retention of beneficial ownership information by FinCEN, the Securities and Exchange Commission (SEC), and the Federal Banking Agencies, as well as subsequent industry calls for codification of a clear and practicable rule on beneficial ownership.

Additionally, just last week, FinCEN announced two measures to address ongoing concerns about the lack of transparency in the movement of cash across the U.S./Mexico border by armored car services and other common carriers of currency. Authorities have long suspected that some cross border carriers abuse both the spirit and letter of a limited CMIR filing exemption to avoid submitting reporting to FinCEN about the cross border movement of cash. Whether witting or not, flaunting the exemption requirements degrades transparency and has assisted transnational criminal organizations to launder their illicit proceeds.

The first measure we took at FinCEN to promote greater transparency was to issue guidance clarifying the circumstances under which common carriers of currency, including armored car services, can take advantage of the narrow exemption to the CMIR filing requirements. FinCEN's regulations state that a CMIR must be used to report the physical transportation of currency or other monetary instruments in an aggregate amount exceeding

$10,000 at one time when they are moved across the border into or out of the United States. Common carriers of currency enjoy a narrow exemption from the requirement to file a CMIR, under certain limited circumstances, when delivering their currency shipments to U.S. depository institutions or securities broker/dealers. However, this exemption has routinely been misapplied, resulting in under-reporting of CMIRs. FinCEN's guidance clarifies the responsibilities of a common carrier of currency with respect to CMIR completion and filing.

The second measure we took at FinCEN to promote greater transparency was to issue a Geographic Targeting Order (GTO), requiring enhanced BSA reporting at two ports of entry along the U.S./Mexico border. The GTO requires common carriers of currency, including armored car services, to file CMIRs upon crossing the land border between Mexico and the United States (regardless of any existing exemption) and identify the originator of the currency and the name and phone number of the currency recipient. Information gathered pursuant to the GTO will provide U.S. law enforcement unprecedented ability to identify precisely who is moving money into and out of the United States. FinCEN has worked in close coordination with law enforcement on this GTO, including Homeland Security Investigations (HSI) and U.S. Customs and Border Protection (CBP).

FinCEN also continues to look at the armored car services industry as a whole and contemplate further guidance on how certain aspects of its evolving business models fall within the scope of our requirements for money transmitters including the accompanying reporting and recordkeeping requirements, among others.

Taken together, these measures will significantly increase the transparency into the movement of currency across the U.S./Mexico border.

Finally, last month, FinCEN took action against FBME Bank, which openly promoted itself to a vast array of bad actors on the basis of its weak AML controls that undermined transparency. FBME changed its country of incorporation numerous times, partly due to its inability to adhere to regulatory requirements. It established itself with a nominal headquarters in Tanzania. However, FBME transacted over 90 percent of its global banking business through branches in Cyprus. FBME was used by its customers to facilitate money laundering, terrorist financing, transnational organized crime, fraud, sanctions evasion, and other illicit activity, internationally, and through the U.S. financial system. Through our issuance of a 311 action, FinCEN found the bank to be a foreign financial institution of primary money laundering concern, and proposed shutting off FBME from the U.S. financial system.

Our message is clear: FinCEN will not turn a blind eye to foreign financial institutions seeking to operate in the U.S. financial system while taking active steps to evade oversight by their regulatory authorities and facilitate illicit activity, globally.

You have heard me and many others talking for several months now about creating a culture of compliance. For an audience like this, which includes AML professionals in the

public and private space, the concept is not novel. You are the people that we rely on to live and breathe BSA/AML and its importance. But how easy is it for the private sector to take that message to its board rooms? And how easy is it for the owner of a small MSB or brokerage house to understand it?

With that difficulty in mind, FinCEN has put down in writing what we mean by a culture of compliance in terms that you can take to your organization's leadership. The Advisory that FinCEN issued yesterday does not say anything that you have not heard before, but we view it as another tool that you can use to influence your organization's leadership, to make it easier for them to live and breathe BSA/AML the same way that you do. It discusses not only the importance of compliance, but also stresses the value that we derive from your compliance efforts and reporting, along the lines that I mentioned earlier.

Based on the enforcement cases I have seen time and time again, both during my time as a prosecutor at the U.S. Department of Justice and now as Director of FinCEN, I can say without a doubt that a strong culture of compliance could have made all the difference. If I were to find myself responsible for BSA/AML compliance within any financial institution, my first order of business would be to pay attention to these core, fundamental concepts. Because once you have a strong culture in place, including the support of your institution's leadership, you have a firm foundation on which to build an effective program.

We recognize that financial institutions spend a significant amount of time and money to do their part to balance risks and ensure businesses are operating with transparency in the U.S. financial system. We will continue to do our part to help financial institutions navigate these waters, and to ultimately find a way forward in maintaining and managing categories of higher-risk accounts for the sake of transparency while at the same time helping you identify those actors that need to be kept out of the U.S. financial system.

###