PREPARED REMARKS OF JENNIFER SHASKY CALVERY
DIRECTOR
FINANCIAL CRIMES ENFORCEMENT NETWORK

ASSOCIATION OF CERTIFIED ANTI-MONEY LAUNDERING SPECIALISTS (ACAMS)
19TH ANNUAL INTERNATIONAL AML AND FINANCIAL CRIME CONFERENCE

MARCH 18, 2014
HOLLYWOOD, FL

Good afternoon. It is a pleasure to be joining you all again this year. I would like to spend my time today updating all of you on some of the high profile and sensitive issues FinCEN has been working on this past year. It has been a busy time for not only FinCEN, but for all of us in the anti-money laundering (AML) area.

I would like to first discuss FinCEN's efforts to promote greater financial transparency in the marijuana industry. Last month, FinCEN, in coordination with the U.S. Department of Justice, issued guidance clarifying reporting and customer due diligence expectations for financial institutions seeking to provide services to marijuana businesses.

The guidance clarifies that financial institutions can provide services to marijuana-related businesses consistent with their Bank Secrecy Act (BSA) obligations.

Providing clarity in this context should enhance the availability of financial services for marijuana businesses and mitigate the dangers associated with conducting an all-cash business. The guidance also helps financial institutions file reports that contain information important to law enforcement. Law enforcement will now have greater insight into marijuana business activity generally, and will be able to focus on activity that presents high-priority concerns.

This is a unique and complex issue, and only legislative change can fully and completely address it. We believe that FinCEN's approach best balances the multiple competing interests currently at play. We are encouraged by Suspicious Activity Reports (SARs) we have received so far indicating that certain financial institutions are providing banking services to marijuana-related businesses. In fact, since the guidance was issued last month, FinCEN has received dozens of SARs filed by financial institutions that are banking marijuana businesses. So, from

our perspective the guidance is having the intended effect. It is facilitating access to financial services for marijuana-related businesses, while ensuring that their activity is transparent and that appropriate AML safeguards are in place.

We realize, however, that it is one thing to issue guidance from Washington. The hard part is making sure the guidance is implemented on the ground. So we are working closely with our regulatory partners both directly and through forums such as the Bank Secrecy Act Advisory Group (BSAAG), as well as the Federal Financial Institutions Examination Council (FFIEC), to address the practical issues that may arise as financial institutions provide services to state authorized marijuana businesses. We also encourage financial institutions to contact FinCEN's Resource Center with any questions about the guidance.

It would be ironic if financial institutions that choose not to provide services to state authorized marijuana businesses feel like they are being asked to devote significantly more BSA compliance attention in this space than they were before the guidance was issued. Not only would it be ironic, but it would also be counterproductive as that was not the intent of the guidance. FinCEN will work with industry and our government stakeholders to help avoid what arguably would be the type of gap (or delta) between regulatory risk and actual risk that we are trying to reduce more broadly.

In a similar vein, FinCEN's guidance included the explicit statement that FinCEN's enforcement priorities in connection with this guidance will focus on matters of systemic or significant failures, and not isolated lapses in technical compliance. While not a novel view, we specifically highlighted this common sense position in the guidance to clarify regulatory risk and focus industry resources on priority areas. This is consistent with themes we have heard through Delta Team discussions, which I will touch more on later, and fundamental to the entire premise of the guidance itself.

Virtual currency issues have also been at the forefront this year. Because any financial institution, payment system, or medium of exchange has the potential to be exploited for money laundering, fighting such illicit use requires consistent regulation across the financial system. Virtual currency is not different from other financial products and services in this regard. What is important is that financial institutions that deal in virtual currency put effective anti-money laundering and counter terrorist financing (AML/CFT) controls in place to harden themselves from becoming the targets of illicit actors that would exploit any identified vulnerabilities.

Indeed, the idea that illicit actors might exploit the vulnerabilities of virtual currency to launder money is not merely theoretical. We have seen both centralized and decentralized virtual currencies exploited by illicit actors. With money laundering activity already valued in the billions of dollars, virtual currency is certainly worthy of FinCEN's attention.

Just this morning, David Cohen, the Under Secretary for Terrorism and Financial Intelligence at the U.S. Department of the Treasury – and my boss – delivered remarks on virtual currency at an event in New York City, where he made a compelling case for transparency and regulation in the virtual currency space. I encourage all of you to visit Treasury's website and

review his speech in its entirety, as the Under Secretary's remarks highlight how Treasury as a whole is approaching this issue.

On the regulatory side, Under Secretary Cohen noted that our current regulatory framework for decentralized virtual currencies, which guards the entryways and exits into the virtual world, provides sufficient oversight. However, if levels of adoption increase more significantly, and if it appears that daily financial life can be conducted for long stretches completely within a virtual currency environment, we may need to consider whether to apply a more "cash-like" regulation to the virtual currency space**.**

That being said, let me step back for a moment and put virtual currency in perspective as a payment system. The U.S. government indictment and proposed special measures issued last May against Liberty Reserve allege it was involved in laundering more than $6 billion over several years. Administrators of other major centralized virtual currencies report processing similar transaction volumes to what Liberty Reserve did.

In the case of Bitcoin, it has been publicly reported that its users processed transactions worth approximately $8 billion over the twelve-month period preceding October 2013; however, this measure may be artificially high due to the extensive use of automated layering in many Bitcoin transactions.

By way of comparison, according to information reported publicly, in 2012 Western Union made remittances totaling approximately $81 billion; PayPal processed approximately $145 billion in online payments; the Automated Clearing House Network processed $36.9 trillion in transactions; and Bank of America processed $244.4 trillion in wire transfers.

This relative volume of transactions becomes important when you consider that, according to the United Nations Office on Drugs and Crime, the best estimate for the amount of all global criminal proceeds available for laundering through the financial system in 2009 was $1.6 trillion.

While of growing concern, to date, virtual currencies have yet to overtake more traditional methods to move funds internationally, whether for legitimate or criminal purposes.

Exactly one year ago today, FinCEN issued interpretive guidance to bring clarity and regulatory certainty for businesses and individuals engaged in money transmitting services and offering virtual currencies.

In the simplest of terms, FinCEN's guidance explains that administrators or exchangers of virtual currencies must register with FinCEN, and institute certain recordkeeping, reporting, and AML program control measures, unless an exception to these requirements applies. The guidance also explains that those who use virtual currencies exclusively for common personal transactions – like buying goods or services online – are users, and not subject to regulatory requirements under the BSA.

In all cases, FinCEN employs an activity-based test to determine when someone dealing with virtual currency qualifies as a money transmitter. The guidance clarifies definitions and expectations to ensure that businesses engaged in such activities are aware of their regulatory responsibilities, including registering appropriately.

Furthermore, FinCEN closely coordinates with its state regulatory counterparts to encourage appropriate application of FinCEN guidance as part of the states' separate AML compliance oversight of financial institutions.

Earlier this year, FinCEN expanded upon this guidance, issuing two administrative rulings. The rulings provide additional information on our regulatory coverage of certain activities related to convertible virtual currency. In both rulings, the convertible virtual currency at issue was the crypto-currency, Bitcoin, and we were clarifying how users who obtain virtual currency only for their own use or investment are not money transmitters.

I am also pleased to report that since FinCEN issued its guidance, dozens of virtual currency exchangers have registered with FinCEN, and some virtual currency exchangers are beginning to comply with reporting requirements and are filing SARs. They appear to be appreciative of the need to develop controls to make themselves resilient to abuse by bad actors. And they are also coming to terms with the fact that as administrators and exchangers they must obtain, verify, and store key information about the senders and recipients of virtual currency and, under certain circumstances, pass that information on to other administrators or exchangers involved in the transaction.

This last issue is key. Simply put, these exchangers and administrators, like other money transmitters, are subject to the so-called Travel Rule. Thus, they have to incorporate into their business models the same transparency with respect to funds transfers as other money transmitters.

While we are encouraged by these industry efforts to increase transparency in this space, I do, however, remain concerned that there appear to be many domestic virtual currency exchangers that are not fulfilling their recordkeeping and reporting requirements.

Those who do not comply with these rules should understand that their actions will have consequences. Not only are they subject to civil monetary penalties, but the knowing failure to register a money transmitting business with FinCEN – or with state authorities where there is a state licensing requirement – is a federal criminal offense.

One thing is clear: With all we have seen transpire this past year, the virtual currency industry has clearly reached a crossroads. I think we can all agree that the stakes are too high – for both the industry and the government – to allow virtual currency systems to be used by bad actors. So it is important that we continue to engage in open dialogue with responsible members of the virtual currency community.

And we will continue to engage in open dialogue. In that vein, I am pleased to announce that, for the first time, we will be including a member of the virtual currency community as part

of the Treasury's BSAAG. The BSAAG consists of representatives from regulatory and law enforcement agencies, financial institutions, and trade associations who advise Treasury on policy recommendations. We are hopeful that formally including the virtual currency community's voice in BSAAG will mean that our regulatory approach as a whole, including virtual currencies specifically, is better informed and more effective.

In mentioning BSAAG, I would also like to update you on our ongoing Delta Team efforts. As I noted last year, FinCEN was just beginning to explore the delta between compliance risk and illicit finance risk through our Delta Team, a subcommittee of the BSAAG.

During our Delta Team discussions to date, we have heard many common themes raised, which I think many of you here today will agree with. We heard that additional information on money laundering trends – including more specifics on schemes and methods for illicit finance and the identification of red flags – would help industry to better align its efforts with law enforcement priorities. Providing increased transparency in this area is something with which we certainly agree.

We also heard that FinCEN needs to find ways for more dynamic, real-time information sharing, both by and between financial institutions, and with FinCEN and law enforcement. A key aspect here is to again promote information sharing between financial institutions through Section 314(a) and (b) of the USA PATRIOT Act.

In response, we have begun exploring new ways to expand information sharing from government to industry under 314(a) authorities in more targeted circumstances, and using a more dynamic and iterative approach, where warranted. We obviously cannot provide any further details publicly as the concept involves the sharing of sensitive information; however, we are working now on developing the methodology with the hope that it will one day become more routine.

I would like to turn now to one of FinCEN's most recent areas of focus, which of course is the ongoing situation in Ukraine. There are a number of efforts underway throughout the U.S. government to assist the Government of Ukraine, and I would like to speak specifically about FinCEN's efforts to help Ukraine combat corruption and recover stolen assets in hopes of restoring financial stability and economic growth to the country.

FinCEN issued an Advisory on February 25, 2014 to U.S. financial institutions to remind them of their responsibility to take reasonable, risk-based steps regarding the potential suspicious movement of assets related to Viktor Yanukovych and other senior officials resigning from their positions or departing Kyiv.

Financial institutions should also be aware that on March 6, 2014, as well as yesterday, March 17, the President of the United States issued Executive Orders authorizing the Secretary of the Treasury, in consultation with the Secretary of State, to designate individuals or entities that contribute to the undermining of Ukraine's democracy, peace, security, sovereignty or territorial integrity, or responsible for the misappropriation of Ukraine's state assets. These Executive Orders require U.S. persons, including U.S. financial institutions and any foreign

branch, to block assets of any designated individuals or entities that come under U.S. jurisdiction.

The measures being taken against these former Ukrainian officials and their close associates increase the risk that they will seek to move their assets in a deceptive fashion. To help mitigate this risk, FinCEN's most recent Advisory on March 6, 2014 provides U.S. financial institutions with the names and identifying information of those persons who have been subject to European Union and Canadian sanctions because of their apparent role in the misappropriation of state assets or instability in Ukraine. As the inclusion of this information highlights, FinCEN's efforts are not just domestic, but global.

FinCEN's Advisory reminds U.S. financial institutions that they are required to apply enhanced scrutiny to private banking accounts held by or on behalf of senior foreign political figures and to monitor transactions to or from those accounts that could potentially represent misappropriated or diverted state assets, the proceeds of bribery or other illegal payments, or other public corruption proceeds.

Financial institutions should be aware of the possible impact that public reports of high-level corruption by senior members of the Yanukovych administration and other illicit activity by members of the administration may have on patterns of financial activity when assessing risks related to particular customers and transactions.

FinCEN's advisory is focused on potentially suspicious transactions involving senior members of the Yanukovych administration or those acting for or on their behalf, and is not intended to call into question the maintenance of normal relationships between financial institutions in the United States and Ukraine.

If a financial institution knows, suspects, or has reason to suspect that a transaction relating to senior foreign political figures involves funds derived from illicit activity, including money laundering, terrorist financing, or any other violation of law or regulation, or if the transaction appears to have no business or lawful purpose or has a purpose inconsistent with the customer's known business, the financial institution must file a SAR consistent with FinCEN's regulations.

In addition, financial institutions are reminded of the regulations implementing Section 312 of the USA PATRIOT Act, which require a written due diligence program for private banking accounts held for non-U.S. persons designed to detect and report any known or suspected money laundering or other suspicious activity. In instances where senior foreign political figures maintain private banking accounts at a covered institution, those financial institutions are required to apply enhanced scrutiny of such accounts to detect and report transactions that may involve the proceeds of foreign corruption.

In April 2008, FinCEN issued Guidance to assist financial institutions with reporting suspicious activity regarding proceeds of foreign corruption. That Guidance, available on FinCEN's website, also discusses potential indicators that transactions may be related to proceeds of foreign corruption. Financial institutions may find this Guidance useful in assisting

with suspicious activity monitoring and due diligence requirements related to senior foreign political figures.

All of this is to say that, as the situation with respect to Ukraine unfolds, we appreciate the help of your financial institutions in monitoring the suspicious movement of assets tied to former Ukrainian officials and their associates. We must work together to remain vigilant and to proactively identify and address illicit financial activity.

One last issue on the policy front: customer due diligence. The cornerstone of a strong AML compliance program is the adoption and implementation of internal controls, which include comprehensive customer due diligence (CDD) policies, procedures, and processes for all customers, particularly those that present a high risk for money laundering or terrorist financing.

The issues surrounding CDD are complicated, and we are continuing to work hard in hopes of issuing the Notice of Proposed Rulemaking soon.

This past year, FinCEN also established a stand-alone Enforcement Division to ensure that we are fulfilling our role in the enforcement of our AML regime.

Our Enforcement Division serves as the primary action arm for asserting our regulatory authorities against jurisdictions and financial institutions that are of primary money laundering concern outside the United States, as well as civil enforcement of the BSA at home. FinCEN has broad ground to cover with a small, but dedicated, staff.

When bad actors take their business offshore, FinCEN will take action to counter these threats. As our Section 311 authority shows, once FinCEN determines that a foreign financial institution, foreign jurisdiction, type of account, or class of transaction is of "primary money laundering concern," the Director has the authority to require domestic financial institutions to take certain special measures to address the concern.

As I mentioned earlier, through a Notice of Proposed Rulemaking, FinCEN identified Liberty Reserve, a Web-based virtual currency service, as a financial institution of primary money laundering concern under Section 311 of the USA PATRIOT ACT. The action was the first use of Section 311 authorities by FinCEN against a virtual currency provider. Liberty Reserve was widely used by criminals around the world to store, transfer, and launder the proceeds of their illicit activities. Liberty Reserve's virtual currency had become a preferred method of payment on websites dedicated to the promotion and facilitation of illicit Web-based activity, including identity fraud, credit card theft, money laundering, online scams, and dissemination of computer malware. It sought to avoid regulatory scrutiny while tailoring its services to illicit actors.

Likewise, when bad actors compromise financial institutions in the United States, FinCEN will take action to stop these abuses, as well. And nowhere is this more important than in those sectors of the financial industry where FinCEN is the only federal regulator with AML enforcement authorities, such as money services businesses (MSBs).

Just last month, FinCEN assessed a civil money penalty against an MSB after our investigation determined serious and willful violations of BSA program, recordkeeping, and reporting requirements. As part of FinCEN's enforcement action, the MSB and its individual owner agreed to cease operating as an MSB and immediately surrendered the MSB's registration to FinCEN.

As Director, I feel it is important that financial institutions take responsibility when their actions violate the BSA. And by accepting responsibility, it is not just about admitting to the facts alleged in FinCEN's enforcement action. It is also about admitting a violation of the law. Over the last year, we have changed our practice at FinCEN to one in which our presumption is that a settlement of an enforcement action will include an admission to the facts, as well as the violation of law. And we have begun implementing this practice in our enforcement actions against all sizes and types of financial institutions.

Integrity and transparency goes a long way. It is a great bestowal of trust that enables financial institutions to be part of the U.S. financial system, to be part of the global financial system. And that trust – that privilege – comes with obligations. One of those obligations is a responsibility to put effective AML controls in place so criminals and terrorists are not able to operate with impunity in the U.S. financial system.

As FinCEN's recent enforcement actions show, FinCEN will act under such circumstances to protect the integrity and transparency of the U.S. financial system.

I know I have covered quite a bit of ground today, but I hope you found my updates helpful in understanding how FinCEN is approaching a number of high-priority issues. But in looking ahead, it is clear that there is still much work to be done, and there will always be new threats to mitigate. And the overriding key to our success is our ongoing partnerships with all of you here today.

Thank you for the role you play in building the strong public-private partnerships that are so vital to our collective efforts to safeguard the financial system from illicit use. For me, building these partnerships – and learning from each of you – is truly the most rewarding and inspiring part of my job.

Being here today, where we can all learn how to 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 as we work together to protect the integrity and transparency of the U.S. financial system.

###