REMARKS OF JENNIFER SHASKY CALVERY
DIRECTOR
FINANCIAL CRIMES ENFORCEMENT NETWORK

FLORIDA INTERNATIONAL BANKERS ASSOCIATION
ANTI-MONEY LAUNDERING CONFERENCE

FEBRUARY 20, 2014
MIAMI, FL

Good afternoon. It is a pleasure to be joining you again this year. Today, I will focus my remarks on some of the key events for FinCEN in the last year (a bit of a "year in review"), as well as some of the issues we expect to be a prominent part of our collective anti-money laundering (AML) conversation during the year ahead.

Looking Back

The past year has been a busy one for FinCEN within our policy area, as we tackled a number of very high-profile and sensitive issues.

Just last week, in seeking to promote greater financial transparency in the marijuana industry, FinCEN, in coordination with the U.S. Department of Justice, issued guidance that clarifies 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.

Virtual currency issues have also been on the front burner 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.

That being said, it is also important to 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.

Just a few weeks after I spoke last year, FinCEN issued interpretive guidance in March 2013 to bring clarity and regulatory certainty for businesses and individuals engaged in money transmitting services and offering virtual currencies.

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.

The first ruling states that, to the extent a user creates or "mines" a convertible virtual currency solely for a user's own purposes, the user is not a money transmitter. The second states that a company purchasing and selling convertible virtual currency as an investment exclusively for the company's benefit is not a money transmitter.

Since our March 2013 guidance was issued, many of the questions we have received have been about the applicability of our regulations to users of convertible virtual currency and, in particular, Bitcoin. We are hopeful that these rulings will help provide clarity in this area.

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 Bank Secrecy Act Advisory Group (BSAAG). I would be remiss if I didn't spend a few moments acknowledging the invaluable contributions Clemente Vasquez Bello made to our BSAAG efforts over the years.

The passion and dedication that Clemente brought for many years to our BSAAG discussions was second to none, and he has been sorely missed. I know from my own discussions with Clemente that an area he cared deeply about was striking the right balance between money laundering prevention and BSA reporting.

On one hand, if you focus too much on the prevention side within your financial institution, you could lose visibility as illicit actors burrow deeper into layers of client relationships, and we lose valuable reporting. But, if you focus only on reporting suspected illicit activity, while allowing illicit actors to continue receiving services, prevention-related efforts will be undermined and the U.S. financial system compromised.

What we all learned from our discussions with Clemente about this, as well as many other issues, is that there is no bright line. This is one of many issues that lie on a spectrum, and where financial institutions need to strike a balance. Strong public/private partnerships play an important role in helping strike that balance.

Clemente's fervor for these issues continues to resonate and will have a long-lasting impact on our work within the Delta Team. And we are grateful to have David Schwartz now representing FIBA within BSAAG to continue bringing valuable perspectives to our discussions.

I want to turn back for a moment to some of the common themes raised through our Delta Team discussions. 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 publically 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.

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.

Since I spoke with you last year, FinCEN named 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 st 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 this 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 a money services business and immediately surrendered the MSB's registration to FinCEN.

The MSB admitted to failing to implement any AML/CFT program. During its operation, the MSB transmitted approximately 1,400 wires per year to Yemen, a high-risk country for terrorist activity and money laundering. The MSB failed to review any of these or other transactions for suspicious activity and admitted to deliberately ignoring its BSA obligations for fear of losing customers. The MSB also admitted that its conduct violated the BSA.

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.

Looking Ahead

I would now like to focus on some of the threats that will continue keeping our attention this year, as well as some new concerns on our radar.

On the virtual currency front, with all we have seen transpire this past year; it is clear that the virtual currency industry has 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. FinCEN will continue to draw from the knowledge we have gained through our regulatory efforts, use of targeted financial measures, analysis of the financial intelligence we collect, independent study of virtual currency, outreach to industry, and collaboration with our many partners in law enforcement to protect the integrity and transparency of the U.S. financial system.

An area of increasing concern to FinCEN is third party money launderers. Third party money launderers are professional money launderers. For example, for the *Breaking Bad* fans out there, Saul Goodman would be considered a third party money launderer.

Using their connections, professional expertise, and influence, third party money launderers transfer funds on behalf of others, knowing that the funds are involved in illicit activity. This access allows criminals to circumvent anti-money laundering controls both in the United States and abroad.

Third-party money launderers rely on different schemes to infiltrate financial institutions, including: layering financial transactions, creating or using shell and shelf corporations, creating or using false documentation, using political influence to facilitate financial activity, and exerting inappropriate influence over key employees in financial institutions.

Let me be clear. Just because a third party money launderer may be located outside of our borders does not mean they can operate with impunity within our financial system. FinCEN's 311 and other authorities can – and will – be used to take action against third party money launderers located outside of the United States.

FinCEN is also trying to get a better handle on the use of cash in the securities sectors for other countries. For example, FinCEN's analysis recently revealed that Mexican casa de bolsas (Mexican securities firms) are starting to bring U.S. cash dollars into the United States and deposit this cash into U.S. banks. U.S. financial institutions dealing with foreign securities firms should be mindful of their source of funding, given the heightened drug trafficking and money laundering risks associated with U.S. cash dollars from Mexico.

More broadly, when securities firms offer services similar to banks, they need to also consider the vulnerabilities associated with engaging in these types of services, and to make sure that their compliance programs are commensurate with such risks. To the extent that these entities are providing bank-like services, we need to make sure that essentially the same types of AML obligations and compliance activities applicable to banks are in place – notwithstanding the fact that the institution might not be a bank.

FinCEN also continues to focus on the major threat posed by trade-based money laundering, one of the most popular methods used by Transnational Organized Crime (TOC) groups to move their money all over the world. By moving their illegal proceeds, often through the formal banking system, criminals are able to disguise their illegal proceeds as legitimate trade transactions. In the process, criminal organizations are able to exploit the complex and sometimes confusing documentation that is frequently associated with legitimate trade transactions.

Moving forward, FinCEN aims to use our new advanced analytics tools to not only detect, but anticipate where trade-based money laundering activities might be manifested. This type of analysis will significantly improve our efforts by allowing us to focus on those regions or financial sectors where money laundering or financial crimes are most prevalent and the most vulnerable.

On the policy front, another area where I see discussions going forward, and where your insights will be valuable, is balancing the policy motivations behind data privacy and secrecy laws in different jurisdictions with the need for an appropriate level of transparency to combat money laundering and terrorist financing. This issue is particularly critical in the area of correspondent banking, and strongly implicates the future of de-risking.

This issue is beginning to gain momentum, particularly as financial institutions grapple with how they can share information to ensure transparency in the global financial system, as well as feel comfortable processing specific transactions. We are working closely with a variety of jurisdictions through the Financial Action Task Force and other bilateral and multilateral venues to address this issue.

Looking forward on the enforcement side, we know that the vast majority of the industry, and in particular the compliance officers within financial institutions, are doing everything they can to comply with their responsibilities. We appreciate all you are doing to keep your financial institutions safe from illicit use. We also appreciate, however, your own frustrations when you see institutions not doing what they are supposed to be doing, and not taking compliance seriously enough.

FinCEN will continue to employ all of the tools at our disposal and hold accountable those institutions and individuals who recklessly allow our financial institutions to be vulnerable to terrorist financing, money laundering, proliferation finance, and other illicit financial activity.

Conclusion

In closing today, I would like to circle back to a common theme woven throughout our work at FinCEN: Partnership. 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.

I think my remarks today illustrate our most recent efforts to counter many high-profile and pressing threats. 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.

In addressing new threats, FinCEN works hard to consider the needs and equities of all stakeholders, including law enforcement, regulators, foreign financial intelligence units, industry, and the public. That is why 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.

###