Prepared Remarks of FinCEN Director Kenneth A. Blanco, delivered at the 2018 Chicago-Kent Block (Legal) Tech Conference

2018 Chicago-Kent Block (Legal) Tech Conference

Chicago-Kent College of Law at Illinois Institute of Technology
565 West Adams Street
Chicago, IL 60661

August 09, 2018

Thank you, Clay Porter, for that wonderful introduction.

Good afternoon.

I am delighted to be here today. Thank you for having me.

I am excited to dive into the fireside chat. But before I do, I would like to anchor the conversation with some brief benchmarks in FinCEN's approach to virtual currency and emerging technology.

I think it is important, particularly for me in my role as a regulator, that when I take the time to give a speech, or appear on a panel or give a presentation, I have something meaningful or important to say, and that I am clear about what it is that I am saying.

Purpose, clarity, and transparency are important, particularly in what we do.

1) So first, I want to discuss how FinCEN is approaching virtual currency and financial innovation;

2) Second, I want to discuss the value of Bank Secrecy Act (BSA) filings we receive from financial institutions, including exchangers in virtual currencies. This information is critical to our mission of keeping our country strong, our financial system secure, and our families and communities safe from harm.

Virtual Currencies and Innovation

Let me begin with our approach to virtual currency.

Innovation in financial services can be a great thing—providing customers greater access to an array of financial services and at faster speeds than ever before. However, as industry evolves and adopts these new technologies, we also must be cognizant that financial crime evolves right along with it, or indeed sometimes because of it, creating opportunities for criminals and bad actors, including terrorists and rogue states.

Virtual currency is an example of both aspects. Major money services businesses are looking at how to incorporate blockchain payments to expedite remittances to locations around the world. But like any payment system or medium of exchange, virtual currency has the potential to be exploited for money laundering and other illicit finance.

Nobody here today wants to see innovative products and services misused to support terrorism, facilitate child exploitation, or become another vehicle for criminals to carry out fraud, identity theft, corruption, or extortion. There are already too many victims out there who may never be made whole again, and harm can be done with devastatingly increasing speed, breadth, and obscurity in the digital world.

The BSA and its regulations are designed to guard against these threats, but these laws and regulations can only do so much on their own. Compliance with our anti-money laundering (AML) and countering the financing of terrorism (CFT) framework is critical to protecting our financial system and safeguarding the incredible innovations within the FinTech space.

Our role at FinCEN is to protect and secure our financial system from those who seek to misuse important technological advancements for nefarious purposes—harming victims while undermining trust in our financial system upon which innovation and our country prosper.

Regulation of Virtual Currency

FinCEN's leadership in AML/CFT regulation and supervision in the area of virtual currency goes back years, focusing on exchangers, administrators, and other persons involved in money transmission denominated in convertible virtual currency.

In 2011, FinCEN issued a final rule amending definitions and other regulations relating to money services businesses to provide that money transmission covers the acceptance and transmission of value that substitutes for currency.[1] Virtual currency is such a substitute and is covered by that regulation. To further clarify this point, in 2013, FinCEN issued guidance on the application of FinCEN's regulations to persons administering, exchanging, or using virtual currencies. [2]

Since then, FinCEN has issued several administrative rulings clarifying how this impacts different business models in the virtual currency space.

1. January 2014 Administrative Ruling on the Definition of User in Context of Mining[3];
2. January 2014 Administrative Ruling on the Definition of User in Context of Software Development and Investing in Virtual Currencies[4];
3. April 2014 Administrative Ruling on Rental of Computer System for Mining Virtual Currency[5];
4. October 2014 Administrative Ruling on Virtual Currency Trading Platform[6];
5. October 2014 Administrative Ruling on Virtual Currency Payment System[7]; and
6. August 2015 Administrative Ruling on Persons Issuing Physical or Digital Negotiable Certificates of Ownership of Precious Metals.[8]

In addition, we are working closely with our federal regulatory colleagues, including the SEC and CFTC, for coordinated policy development and regulatory approaches, including addressing risks.

These risks include potential illicit finance and fraud surrounding Initial Coin Offerings (ICOs). As my SEC and CFTC colleagues have pointed out, this rapidly growing area has gained a lot of recent public attention. While ICO arrangements vary and, depending on their structure, may be subject to different authorities, one fact remains absolute: FinCEN, and our partners at the SEC and CFTC, expect businesses involved in ICOs to meet all of their AML/CFT obligations. We remain committed to taking appropriate action when these obligations are not prioritized, and the U.S. financial system is put at risk.

I wanted to take a moment today just to make a few additional clarifications based on questions we have received.

First, as our March 2013 guidance indicates, FinCEN's rules apply to all transactions involving money transmission—including the acceptance and transmission of value that substitutes for currency, which includes virtual currency. Thus, our regulations cover both transactions where the parties are exchanging fiat and convertible virtual currency, but also to transactions from one virtual currency to another virtual currency.

Further, businesses providing anonymizing services (commonly called "mixers" or "tumblers"), which seek to conceal the source of the transmission of virtual currency, are money transmitters when they accept and transmit convertible virtual currency, and, therefore, have regulatory obligations under the BSA.

In short, individuals and entities engaged in the business of accepting and transmitting physical currency ***or*** convertible virtual currency from one person to another or to another location are money transmitters subject to the AML/CFT requirements of the BSA and its implementing regulations.

To comply with these obligations, virtual currency money transmitters are required to (1) register with FinCEN as a money services business, (2) develop, implement, and maintain an AML program designed "to prevent the [MSB] from being used to facilitate money laundering and terrorist finance," and (3) establish recordkeeping, and reporting measures, including filing Suspicious Activity Reports (SARs) and Currency Transaction Reports (CTRs).

It is important to understand that these requirements apply equally to domestic and foreign-located convertible virtual currency money transmitters, even if the foreign located entity has no physical presence in the United States, as long as it does business in whole or substantial part within the United States.

Similarly, we would expect financial institutions adopting new FinTech to assess and understand whether the new financial products and services may be vulnerable to exploitation for financial crime; and whether this financial service activity has AML/CFT obligations under FinCEN's regulations. We can help answer the question, but avoiding the question for fear of the answer is not a legitimate strategy; indeed it is unwise.

Examination and Supervision Efforts

Examination and supervision are critical components of our efforts to proactively mitigate potential illicit finance risks associated with virtual currency.

Working closely with our delegated BSA examiners at the Internal Revenue Service (IRS), FinCEN has worked to ensure that virtual currency money services businesses understand and

comply with their regulatory obligations through effective supervisory examinations. FinCEN and the IRS have examined over 30 percent of all registered virtual currency exchangers and administrators since 2014. Our goal is to ensure that all virtual currency money transmitters undergo regular, routine compliance examinations—just like every other U.S. financial institution—to help illuminate weaknesses and strengthen protocols before a lapse occurs.

Our efforts here have had a tangible, positive impact on compliance programs, and we have seen SAR filings from virtual exchanges rise tremendously over the past few years.

Also important is that our examinations have included a wide array of virtual currency businesses: virtual currency trading platforms, administrators, virtual currency kiosk (or ATM) companies, crypto-precious metals dealers, and individual peer-to-peer exchangers. We have focused on both registered and unregistered exchanges.

This variety is important because, whether a business is operating as an individual peer-to-peer exchanger of one virtual currency, or a large, multi-national trading platform offering numerous virtual currencies, we expect you to comply with your AML/CFT regulatory obligations.

And there is no question we have noticed some compliance shortcomings.

All financial institutions should be implementing a strong AML program long before they first receive notice that an examination is forthcoming. We have been surprised to see financial institutions establish an adequate number of compliance staff and take appropriate steps to meet their regulatory requirements only <u>after</u> they receive notice.

Let this message go out clearly today: This does not constitute compliance.

Compliance does not begin because you may get caught, or because you are about to be discovered. That is not a culture that protects our national security, our country, and our families. It is not a culture we will tolerate.

A strong culture of compliance should be part of building your operations from the ground up, and you can expect that we will identify where this is not taking place and take appropriate action.

There is too much at stake in this space, for our nation, for our financial system, for our communities, and for our families. We will hold companies and individuals accountable when they disregard their obligations and allow the financial system to be exploited by criminal actors, whether in wire transfers or cryptocurrencies.

My hope is that professionals like yourselves take the time to read about the details of actions taken by FinCEN—even if they aren't assessments against banks—to learn ways to improve your own compliance regime.

<u>BTC-e</u>

An example of FinCEN's commitment to pursuing those whose failures to have even basic controls have enabled criminals to launder proceeds is the $110 million penalty we issued against BTC-e—our first action against a foreign-located MSB and our most recent civil action involving virtual currency. BTC-e was an Internet-based virtual currency exchanger that offered exchange in fiat currency, as well as convertible virtual currencies like Bitcoin, Dash, and

Ether. At one point BTC-e served approximately 700,000 customers across the world and was associated with bitcoin wallets that had received over 9.4 million bitcoins.

The company lacked even basic controls to prevent the use of its services for illicit purposes. As a result, they attracted and maintained a customer base that included many criminals who desired to conceal proceeds from crimes such as ransomware, fraud, identity theft, public corruption, and drug trafficking. Included in FinCEN's findings, we discussed BTC-e's failure to establish policies and procedures to handle transactions going through anonymizing services like bitcoin mixers, and offering the anonymity-enhanced cryptocurrency Dash. Importantly, FinCEN's BSA enforcement investigation also led to the assessment of a $12 million civil money penalty against one of BTC-e's administrators, Alexander Vinnik—the largest individual liability penalty FinCEN has assessed to date.

While FinCEN led the civil investigation on this entity, we also partnered with our law enforcement and Department of Justice colleagues who indicted and shuttered the exchange. We will aggressively pursue individuals and companies, in any venue necessary, who do not take their obligations under U.S. law seriously.

FinCEN prioritizes ensuring that all exchangers and administrators comply with the BSA and its implementing regulations regardless of their size. While the implementation of AML/CFT requirements may vary depending on whether or not the business is a peer-to-peer exchange or a large high-volume exchanger, it is important that all financial institutions are playing their part to protect the financial system and the people using it.

Egmont

We also are sharing experience on cryptocurrency with foreign partners through the Egmont Group of Financial Intelligence Units (FIU) and other international forums. I will be leading a special forum of FIU heads. One of the priority areas we will focus on involves virtual currencies. We selected this issue as a priority area for discussion, due to the impact that enhanced FIU analysis and customer products can have on the effectiveness of an FIU and its ability to combat money laundering and terrorist financing. Our work in this forum will help FIUs gain a better understanding of virtual currency risks and typologies and effective approaches to the analysis and use of relevant financial information. It will also aim to help FIUs better advise reporting entities on what to report about potential virtual currency transactions, or activity and other relevant information for revealing the flows, actors, and methods involved in financing illicit activities.

SAR Filings

Let me assure you, our success in protecting financial institutions and innovative virtual currency payment and FinTech systems from being exploited for money laundering and other illicit financing purposes depends very much on effective implementation by you, the private sector.

One great success we have seen recently is the substantial increase in virtual currency SAR filings over the past few years.

We now receive over 1,500 SARs per month describing suspicious activity involving virtual currency, with reports coming from both MSBs in the virtual currency industry itself and other

financial institutions. We see the industry developing new techniques for identifying suspicious activity in virtual currency, showing us what is possible and giving us unique insight into certain financial crimes. By helping us identify and investigate this illicit activity, the industry can focus on legitimate applications and innovations, and stamp out negative perceptions of virtual currency as the coinage of the dark web and bad actors.

I know you frequently hear FinCEN and our law enforcement partners laud the importance and value of SARs, but I want to emphasize the differences these filings can make. Recall the BTC-e case example I discussed earlier. SAR filings played a critical role in the investigation of that case. It was filings by both banks and other virtual currency exchanges that provided critical leads for law enforcement. This information included beneficial ownership information, additional activity attributed to the exchange of which we were previously unaware, jurisdictional information, and additional financial institutions we could contact for new leads. All of this was obtained through SARs and the supporting documents filed by financial institutions.

Other individual filings continue to help us work to combat threats here in this country, including the opioid crisis that has been plaguing communities across the nation. On April 3, Attorney General Jeff Sessions recognized FinCEN's participation in Operation Disarray, part of the Joint Counter Opioid Darknet Enforcement (J-CODE) effort—a nation-wide effort to target darknet drug traffickers across the country. In this and other operations with law enforcement, BSA data has been instrumental. We have worked with law enforcement to investigate leads provided in SARs on opioid vendors to combat the illicit use of virtual currency—leading to arrests of dealers and distributors, identification of overseas suppliers, and disruption of the marketplaces that have facilitated the distribution of these destructive, addictive opioids.

Additional Efforts

We also are actively working to develop information sharing programs to help the financial services sector defend itself from these threats—programs like FinCEN Exchange and other cyber defense programs offered by the Treasury. We are in the process of setting up a virtual currency-focused FinCEN Exchange program with the private sector and law enforcement, which will provide a platform for all of us to engage with industry developments, concerns, and share risks and threats that we are seeing.

Lastly, we are continuously developing our technological capabilities and expertise to remain in step with the evolution of industry as well as the threats that persistently seek to take advantage of new vulnerabilities. We will be just as persistent. We are working hard on the dynamic infrastructure across analytic, operational, policy, and legal areas to be as agile and forward-looking as the world in which we operate and the financial system that is our mission to protect and advance. To that, I have brought into my Front Office a Chief of Strategic Advancement & Tactical Development, Michael Mosier, to spearhead this forward-looking, cross-functional approach.

All of these efforts—including the use of advisories to increase effective SAR reporting, and the establishment of FinCEN Exchange as an information sharing mechanism—help financial institutions protect themselves, their customers, and our financial system.

Conclusion

As I conclude, I want to make clear:

1) We are focused on swiftly and continuously building our capabilities and understanding in the emerging technologies space to (a) rapidly identify risks, (b) close gaps, and (c) support responsible innovation through clarity;

2) SAR reporting is of critical importance to our work in the virtual currency space to help identify emerging threats and typologies, (a) for the sake of the victims that are targeted, (b) for financial institutions to better understand and effectively report on these threats, and (c) for public trust and reliance in the good work being done in the financial innovation space;

3) We will continue to update our guidance relating to emerging technology, such as virtual currency, in close dialogue with industry, so that we are improving our understanding of both the risks and the clarity that is needed to support responsible innovation; and

4) FinCEN will aggressively pursue individuals and companies who do not take their obligations under U.S. law seriously, whether by targeting victims or enabling those who do.

I very much appreciate the opportunity to engage in a substantive discussion with Clay and the other industry experts here, so that we can work together to advance innovation while protecting the integrity of the financial system upon which the success of your businesses and our country depend. It is important that we keep this dialogue going.

Thank you for having me here today.

###

---

[1] See https://www.gpo.gov/fdsys/pkg/FR-2011-07-21/pdf/2011-18309.pdf

[2] See https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf

[3] See https://www.fincen.gov/sites/default/files/shared/FIN-2014-R001.pdf

[4] See https://www.fincen.gov/sites/default/files/shared/FIN-2014-R002.pdf

[5] See https://www.fincen.gov/sites/default/files/administrative_ruling/FIN-2014-R007.pdf

[6] See https://www.fincen.gov/sites/default/files/administrative_ruling/FIN-2014-R011.pdf

[7] See https://www.fincen.gov/sites/default/files/administrative_ruling/FIN-2014-R012.pdf

[8] See https://www.fincen.gov/sites/default/files/administrative_ruling/FIN-2015-R001.pdf