Remarks of Sigal Mandelker, Under Secretary for Terrorism and Financial Intelligence CoinDesk Consensus Conference

May 13, 2019

I. INTRODUCTION

Good morning, everyone – it's a pleasure to be here today.

As the Under Secretary for Terrorism and Financial Intelligence, I spend my time tracking and targeting money laundering, terrorist financing, proliferation financing, and a myriad of other illicit activities. My office consists of more than 800 career professionals, who are the best in the world at shutting down the avenues bad actors use to launder money around the globe.

Before I get into our efforts involving digital currency, I want to describe briefly the offices within the Treasury Department that I oversee:

- The Office of Foreign Assets Control, or OFAC, is the beating heart of the sanctions program.
- The Financial Crimes Enforcement Network, or FinCEN, oversees compliance with anti-money-laundering/combating the financing of terrorism (AML/CFT) obligations, and is also the Financial Intelligence Unit of the United States.
- I have a policy office called the Office of Terrorist Financing and Financial Crimes that does extensive international outreach to help foreign countries harden their networks against illicit finance.
- And Treasury is actually the only finance ministry in the world that has its own intelligence unit, the Office of Intelligence and Analysis, which maps illicit financial flows and networks around the world.

Each of these components plays a critical role in our efforts to ensure that blockchain and other

distributed ledger technologies are not exploited by bad actors.

E-Gold Digital Currency

The idea of using digital currencies to launder money and mask identities is not a new one. I led a team of prosecutors at the Department of Justice more than a decade ago that successfully prosecuted the digital currency E-Gold. E-Gold users were able to set up accounts under names like “Donald Duck” and “Mickey Mouse” and believed they could get away with horrible things, like trafficking in child pornography. They were wrong. In 2008, we convicted E-Gold’s directors of felonies, and they paid multi-million dollar fines.

Today, other bad actors are trying to leverage virtual currencies to make an end-run around our laws and regulations.

Threats

I start every morning at Treasury with a briefing on the threats we face as a nation. Without divulging any state secrets, I want to start by sharing some of the challenges I see facing the virtual currency industry.

Sanctions Evasion and Nation States:

In recent years, economic sanctions have emerged as one of the top tools in our national security arsenal. Without putting boots on the ground or troops in harm’s way, sanctions can help disrupt the operations of state sponsors of terrorism, human rights abusers, and weapons proliferators by cutting off their sources of funding. In this Administration, Treasury has brought unprecedented economic pressure on Iran, North Korea, and Russia, among many others.

Time and again, as regimes and bad actors are cut off from the global financial system, they search for alternatives. This has resulted in some countries and rogue actors trying to turn to digital currencies to offset the impact of economic sanctions.

For example, the Department of Justice recently indicted and OFAC sanctioned Park Jin Hyok. He was part of a North Korea-sponsored hacking team known as the Lazarus Group that is allegedly responsible for stealing $81 million from Bangladesh’s Central Bank, among other

global attacks. As many of you know, the Lazarus Group used spear phishing techniques with Bank of Bangladesh employees to gain access to the bank's network, and from there, accessed the SWIFT payment terminal to cause funds to be transferred out of Bank of Bangladesh's account.

In addition to efforts to steal from banks, the Lazarus Group has also leveraged virtual currency and exchanges to quickly transfer stolen and extorted funds. My team at Treasury back-tracked these stolen funds that were moved through various victims' wallets and laundered through mixers. We traced some of the money through fraudulently opened accounts at exchanges, as it chain-hopped from one blockchain to another around the world. We then worked closely with law enforcement and international partners to identify those responsible.

These types of schemes and other large-scale thefts from virtual currency exchanges have been used to generate massive revenues for bad actors. In fact, FinCEN's analysis estimates $1.5 billion in stolen funds related to cyber hacks of virtual currency exchangers and administrators over just the past two years.

In addition, several countries, including Iran, Venezuela, and Russia, have launched or announced plans to launch a national digital currency. Some have publicly and brazenly stated that the explicit intent of this currency is to evade our sanctions. As you all know, Venezuela's ostensibly oil-backed "Petro" was the Maduro regime's attempt to establish a national digital currency on top of Ethereum and other blockchains. While it failed to attract many investors to this risky venture, we know that other dictators and rogue regimes will inevitably try to succeed.

Terrorists:

Like rogue states, terrorist organizations and their supporters and sympathizers are also constantly looking for ways to raise and transfer funds without detection or tracking by law enforcement. In February 2019, Hamas began soliciting bitcoin donations via social media, using two bitcoin addresses. To make the transactions more difficult to monitor on the public blockchain, Hamas has begun to provide unique funding addresses for each person making a donation.

[1] As of late March 2019, two known addresses had received over $5,000 worth of bitcoin. This might not seem like that much money. But the cost of carrying out a terrorist attack can be low.

When FinCEN analyzed millions of dollars of remittance transactions with suspected links to terrorism, it found they averaged less than $600 each. In an era where a radicalized suicide bomber can bring a tragic end to the lives of hundreds for nothing more than the price of duct tape, a vest, and supplies, we cannot afford to allow any money to flow to terrorists.

II. What do digital currency users, businesses and exchanges need to know about complying with the regulatory and sanctions regimes?

In this context, AML/CFT and sanctions expectations for the digital currency industry should not be viewed as a chore. It should be viewed as a duty serving our national security. If your business is to succeed and thrive, then your business model needs to be built on a strong foundation of anti-money laundering and sanctions compliance from the very beginning. If you wait until you are contacted by regulators or law enforcement, it is too late.

Anonymity-Enhanced Virtual Currencies:

For example, bad actors today remain intent on abusing anonymity-enhanced virtual currencies and services designed to hide transaction flows. Just consider that over $140,000 worth of bitcoin from the global WannaCry 2.0 ransomware attacks was converted into Monero in the months following the attacks to conceal the stolen funds. Products designed to obscure the path of a transaction and enhance anonymity are rife for exploitation by bad actors.

Nobody here wants to see innovative products and services misused to support terrorism and weapons proliferation, or become another vehicle for criminals to carry out child pornography or human trafficking. Some of the features of emerging technologies that appeal most to users and businesses – like speed of transfers, rapid settlement, global reach, and increased anonymity – can also create opportunities for rogue regimes and terrorists. It is for this reason that industry compliance with our regulations is so critical.

Compliance with BSA obligations:

Since 2011, FinCEN's regulations have stated that 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 Bank Secrecy Act and its implementing regulations. This includes transactions in fiat-to-virtual currency, as well as virtual currency-to-virtual currency.

When IRS or FinCEN examiners show up at the door to your business, they will be looking to see if you complied with all of these requirements. That is, did you: (1) register with FinCEN as a money services business, (2) develop, implement, and maintain an AML program designed "to prevent [them] from being used to facilitate money laundering and terrorist financing," and (3) establish recordkeeping, and reporting measures, including filing Suspicious Activity Reports (SARs) and Currency Transaction Reports (CTRs)? We will be checking whether you did all this right from the start of your business – not just after you got a call from regulators or law enforcement.

Virtual currency money transmitters are required to undergo regular, routine compliance examinations—just like every other U.S. financial institution—to help identify weaknesses and ensure compliance. Our exams have focused on business models including virtual currency trading platforms, administrators, virtual currency kiosk (or ATM) companies, crypto-precious metals dealers, and individual peer-to-peer exchangers.

The point of these compliance programs is not to be a roadblock to innovation or divert limited resources from a startup. It is to ensure that you establish a reporting system that keeps bad actors away from your businesses and protects our national security. Remember, you are not only doing this to comply with our regulatory expectations, but also to make sure you are not the next business that North Korea or Hamas or narcotraffickers exploit.

We have found great partners in your industry committed to this objective. Since 2013, FinCEN has received over **47,000** suspicious activity reports (SARs) mentioning bitcoin or virtual currency more broadly. Half of these SARs were filed by *virtual currency exchangers or administrators themselves*. These filings have been critical to law enforcement efforts.

Just take as an example the notorious illicit virtual currency exchanger BTC-e. SARs filed by both depository institutions and virtual currency exchangers helped law enforcement to identify virtual currency wallet addresses used by BTC-e and to detect different illicit streams of activity moving through the exchange.

We are pleased to see that some virtual currency companies have developed their own proprietary sophisticated compliance systems to improve responses to law enforcement requests and overall cyber resilience. Along those same lines, we have seen companies use creative ways to collect and report cyber indicators like device identifiers, IP addresses with associated time stamps, virtual currency wallet addresses, and transaction hashes. In fact, it was this innovative reporting led by the private sector that helped influence FinCEN's recent update of the SAR form to explicitly allow for reporting of these cyber-specific indicators.

FinCEN Exchange Partnership

We believe that it is important that the private and public sectors work collaboratively to protect our financial system. That is why just earlier this month, we held an information exchange under our FinCEN Exchange program where we shared illicit finance methodologies with the virtual currency industry and law enforcement to better protect the financial system. FinCEN also just issued an advisory describing red-flags and common typologies used in exploiting virtual currencies and businesses.

And just last week, FinCEN issued guidance (30 pages long!) directly addressing areas of interest gleaned from ongoing industry engagement about how our regulations apply to different business models, such as peer-to-peer exchangers, virtual currency kiosks, decentralized (distributed) applications (DApps), and anonymizing services. I encourage you all to read it closely.

In addition, just last week, the Financial Action Task Force (FATF)—the international standard-setting body for combating money laundering and the financing of terrorism and proliferation ——currently led by the United States—hosted a private sector consultative forum on the various services and business models in the digital currency space, and discussed how industry can comply with vital AML/CFT obligations, including in the context of asset transfers. During its presidency of the FATF, the United States has worked with other countries to clarify how all countries should regulate and supervise activities and providers in the digital currency space. We anticipate that in June the FATF will adopt a final version of its Interpretative Note, along with updated guidance to further assist countries and industry with their obligations.

Requiring AML/CFT standards around the world is vital for creating a level playing field and ensuring that bad actors don't just gravitate to jurisdictions that have no safeguards. I also want to be clear that our rules apply to any money transmitter — even if foreign-located—so long as they do business in whole or substantial part in the United States.

Compliance with OFAC sanctions:

Turning now to OFAC sanctions. OFAC compliance obligations are the same regardless of whether a transaction is in digital currency or traditional fiat currency. OFAC requirements apply equally to brick and mortar banks as they do to the digital currency world. And compliance is not optional: there are civil and criminal penalties if you fail.

There is no "one-size-fits-all" sanctions compliance program, but there are common themes that are found in all successful sanctions compliance programs:

- Developing a tailored, risk-based program that accounts for the risks in your particular type of business;
- Knowing your customers and conducting sufficient due diligence on them before providing services;
- Making sure you are not conducting prohibited transactions with individuals and entities that appear on OFAC's sanctions lists or facilitating prohibited transfers connected to sanctioned jurisdictions, like Iran, or involving digital currency addresses highlighted on our sanctions lists;
- Communicating with your customer so they understand the types of transactions and activity you expect to see from the relationship, and the types of activity you will not do or perform on their behalf.

We just recently published a document outlining these essential components called "A Framework for OFAC Compliance Commitments," which you can find on OFAC's website.

Our sanctions are ever-changing, and our sanctions lists are dynamic with new individuals and entities, as well as updated identifying information, regularly being added. So your compliance process must be dynamic as well.

I urge you to take our sanctions lists and do additional analysis to make sure you are not doing business with designated parties or conducting prohibited transactions with parties in sanctioned locations. We find that the best compliance programs are those that incorporate red flags and typologies into their programs to protect their businesses, and then use this information to provide reporting back to us, as appropriate, including through suspicious activity reports.

In addition, OFAC's sanctions programs target not just specific individuals and entities, but also whole jurisdictions, such as Cuba, Iran, North Korea, and Syria. So, if your program only runs a check of names against OFAC's lists, you could completely miss other prohibited activity.

Enforcement

Early on in this speech, I told you that we will identify where compliance is not taking place and take appropriate action. Treasury is very focused on pursuing those who disregard their obligations.

As I'm sure everyone here is familiar, we've gone after some of the biggest non-compliant actors in this industry, such as BTC-e, which was shut down, and one of its directors and supervisors, Alexander Vinnik, indicted.

But we will also go after the individual actors who—while maybe smaller in size— egregiously flaunt their obligations. For example, just last month, FinCEN issued a money penalty against a peer-to-peer exchanger named Eric Powers. Mr. Powers failed to register as a money services business and had no written policies or procedures for ensuring compliance with the BSA. He advertised his intent to purchase and sell bitcoin on the Internet, and completed many transactions directly with Darknet Market vendors without ever reporting any suspicious transactions. He conducted over 200 transactions involving the physical transfer of more than $10,000 in currency, yet failed to file a single currency transaction report. As a result of our action, Mr. Powers not only paid a fine, but is now barred from providing money transmission services or participating in the work of any financial institution.

Conclusion

In closing, I hope you understand how much we value your role in protecting our national security and this industry. We applaud those individuals and entities who make compliance an essential part of their businesses, and urge the industry to prioritize compliance before choosing to bring a product or service to the market.

[1] https://www.forbes.com/sites/yayafanusie/2019/03/29/jihadists-upping-their-bitcoin-game/#5fd2aec179bc