Prepared Remarks of FinCEN Director Kenneth A. Blanco, delivered at the Consensus Blockchain Conference

May 13, 2020

Consensus Blockchain Conference (Virtual)

Introduction

Good morning, everyone. Thank you so much for that very kind introduction.

It is great to be with you today, a bit ironic, via this virtual technology to discuss FinCEN, its mission, and how we—government and the virtual currency industry (all of you)—can work together to shape the virtual currency environment to combat criminal exploitation of this space, including the tech industry, to better ensure our national security and protect our financial system, our communities, and our families from harm.

This is truer today than ever before given the global situation we now find ourselves in—the need for our collaboration is clear and undeniable.

Joining this conference today are many financial institutions, including virtual currency service providers. As I have said many times before, you are the backbone of the financial system and are on the front lines of the anti-money laundering (AML) and countering the financing of terrorism (CFT) framework—protecting people from harm. I also know that many of FinCEN's government partners are joining today too, experts and key leaders from the Department of Justice and other law enforcement agencies, fellow regulators, and many other government partners with whom we work on a daily basis to protect people from harm.

Both the public and private sectors are critical to combating exploitation of virtual currency, and when working together, our national security and citizens are safer. There is no substitute for the private sector's visibility into and ability to prevent criminal exploitation of virtual currency products and platforms—particularly those of you who are organizing, developing, and administering these products and platforms. Our work together plays a significant role not just in advancing financial transparency, inclusion, and the development of the future of payment systems, but also in identifying, tracking, and stopping criminals including terrorists and other bad actors from harming others, particularly the most vulnerable. It is our shared responsibility to ensure that this technology does not get hijacked by criminals and bad actors—we cannot let innovation become the conduit for crime, hate, and harm—it is a national security issue.

As many of you know, FinCEN plays two roles in the U.S. national security apparatus:

First: FinCEN is the primary regulator and the administrator of the Bank Secrecy Act, or BSA, part of the comprehensive legal architecture in the fight against money laundering and its related crimes, and terrorism and its financing. FinCEN, through its administration of the BSA, is a global leader in both regulating convertible virtual currency activity and taking action against its illicit use.

Second: FinCEN is the Financial Intelligence Unit, or FIU, of the United States—the world's largest and most powerful economy.

Today, I would like to share with you some of our recent work in the virtual currency space and use my brief time today to clarify a few misconceptions.

I will address three things:

1. FinCEN's efforts to provide guidance and combat money laundering and its related crimes, and terrorism and its financing, involving virtual currency related to the COVID-19 pandemic;
2. The Travel Rule and trends FinCEN is seeing with respect to compliance; and
3. Opportunities for collaboration in the fight against the illicit use of virtual currencies and key challenges.

COVID-19

These are, without a doubt, unprecedented times. The last few months have had a profound effect on the world as we know it or knew it, including in the area of illicit finance threats and related crimes. With businesses and individuals in our country and across the globe facing new and challenging circumstances, along with the rollout of major new Federal, State, local, and foreign government initiatives to combat the COVID-19 pandemic and its economic consequences, the entire AML community has been adapting in real time.

Over the last couple of months, FinCEN has pursued several important public-facing and strategic lines of effort relevant to your institutions:

- First, AML Resources: FinCEN has issued two Notices—one on March 16 and another on April 3 of this year—to financial institutions advising them to stay alert for malicious or fraudulent transactions, with examples of similar indicators that we have seen in the wake of natural disasters. These Notices also provide financial institutions with information regarding AML operations during the COVID-19 pandemic and a direct contact mechanism for urgent COVID-19-related issues. Please reach out to us proactively if you anticipate challenges fulfilling your BSA reporting obligations due to the pandemic.

- Second, Criminal Typologies and Investigative Support: FinCEN is also continuously monitoring criminal activity exploiting the current pandemic. We are supporting law enforcement investigations into COVID-19-related cybercrime, scams, and fraud. FinCEN also plans to publish multiple advisories highlighting common typologies used in the pervasive fraud, theft, and money laundering activities related to the pandemic to better help the financial sector detect and report this activity. The mission for all of us in the financial space is to get badly needed funds to the intended recipients who need it—some for their financial survival—not to exploitive criminals and fraudsters.

Cybercrime:

I want to spend a few moments covering various forms of cybercrime that criminals continue to pursue and adapt during the pandemic. FinCEN has observed that cybercriminals predominantly launder their proceeds and purchase the tools to conduct their malicious activities via virtual currency. Your institutions have the opportunity, and obligation, to help identify these illicit criminal networks in your suspicious activity reporting to FinCEN, so that FinCEN can aggregate and analyze this information to identify red flags, permitting industry to spot risks.

To be clear, this obligation goes much deeper than to FinCEN or the law or to regulations—it is an obligation to others, your families, your loved ones, your friends, your neighbors, and fellow citizens who are victims or potential victims of these crimes. During this time of crisis where our people could be more at risk and more vulnerable than

ever, we, all of us, have a duty and responsibility to use our abilities, tools, and talents to protect others and ensure the stability of this ecosystem that we are creating and that depends on trust.

Here is some of what we are seeing:

- *COVID-19 as Lure:* FinCEN and U.S. law enforcement have seen reports of cybercriminals leveraging COVID-19 themes as lures, often targeting vulnerable individuals and companies that seek healthcare information and products or are contributing to relief efforts. This type of cybercrime in the COVID-19 environment is especially despicable, because these criminals leverage altered business operations, decreased mobility, and increased anxiety to prey on those seeking critical healthcare information and supplies, including the elderly and infirm.

- *Adapting to Opportunities:* Because of increased remote work by many companies and government institutions worldwide, many distinct threat vectors, risk considerations, and mitigation strategies are being used by criminals and bad actors. FinCEN is aware that cybercriminals are targeting vulnerabilities in remote applications—including virtual private networks and remote desktop protocol exploits—to steal sensitive information and compromise transactions. Whether with COVID-19 lures or not, cybercriminals and malicious state actors are using wide-scale phishing campaigns, malware, extortion, business email compromise, and other exploits against remote platforms to steal credentials, conduct fraud, and spread disinformation.

- *Scams:* Many prevalent scams involving virtual currency payments exploit COVID-19, from extortion, ransomware, and the sale of fraudulent medical products, to initial coin offering investment scams, which will likely continue to grow during the pandemic.

- *Undermining Due Diligence:* Criminals are also working to undermine "know your customer" processes in the remote environment. Virtual currency businesses should remain vigilant against attacks targeting their onboarding and authentication processes, for example "deepfakes" manipulating digital images and account takeovers facilitated by credential stuffing attacks. Financial institutions should consider the risks of the current environment in their business processes, and the appropriate level of assurance needed for digital identity solutions to mitigate criminal exploitation of your products and platforms. Even financial institutions that typically manage their lines of business remotely, such as some virtual currency exchangers, may find themselves more exposed given the changing threat environment.

TRAVEL RULE

I now want to turn to another major topic, and the primary theme of today's discussions, the Travel Rule. The United States has long maintained an expectation that financial institutions identify counterparties involved in transactions for a variety of purposes, including AML/CFT and sanctions, even for transactions in virtual currency. Any asset that allows the instant, anonymized transmission of value around the world with no diligence or recordkeeping is a magnet for criminals, including terrorists, money launderers, rogue states, and sanctions evaders.

As a result, we applaud steps taken by the Financial Action Task Force (FATF) last June to establish a consistent approach to the position we have taken when it adopted, as an International Standard, Interpretive Note to FATF Recommendation 15, which included, among other things, FATF's interpretation that countries should apply FATF Recommendation 16's Travel Rule to virtual asset service providers such as virtual currency exchanges.

We are encouraged that so many creative solutions are being developed by industry to address these Travel Rule obligations.

In particular, FinCEN is optimistic about the growth of various cross-sector organizations and working groups focusing on developing international standards and solutions addressing the Travel Rule. I know those efforts involve many of you here today. FinCEN will continue to monitor your developments, whether as observers in working groups, learning about your efforts in forums like this, or meeting with you under the FinCEN Innovation Hours Program, where fintech and regtech companies present to FinCEN new and innovative products and services for potential use in the financial sector.

While we are glad to see the increased emphasis on compliance, I must emphasize again that the United States has maintained this expectation to understand who is on the other side of a transaction for years.

As I mentioned at the Chainalysis conference in November, recordkeeping violations are the most commonly cited violation by our delegated Internal Revenue Service (IRS) examiners against money services businesses (MSBs) engaged in virtual currency transmission.

We have also previously highlighted our confidence that industry can absolutely carry out this requirement. We know technologies exist to support compliance with all recordkeeping obligations. Most challenges we see across the sector relate to governance and process rather than technologies, and many solutions in both governance and technology models could ultimately comply. FinCEN takes a technology neutral approach and we encourage the virtual currency sector to continue collaborative efforts to develop and implement these solutions and to keep FinCEN apprised of their progress, including by considering participating in FinCEN's Innovation Hours Program.

OTHER OPPORTUNITIES FOR COLLABORATION AND CHALLENGES

Finally, I would like to briefly highlight some of our key opportunities for collaboration in combating illicit virtual currency use and the top remaining challenges we see, which hopefully those of you here today can help address.

Our partnerships across regulators, supervisors, law enforcement, and industry are the cornerstone of our efforts to disrupt the illicit use of virtual currency and illicit cyber activity. FinCEN has worked alongside law enforcement initiatives like the National Cyber Investigative Joint Task Force (NCIJTF) and the Joint Criminal Opioid Darknet Enforcement (J-CODE) to investigate criminal networks exploiting virtual currency for the purchase of fentanyl, narcotics, cybercrime tools, and child pornography on darknet marketplaces. We also work with international partners bilaterally or through multilateral forums like the Egmont Group of 164 FIUs, the Heads of FATF FIUs Symposium, of which we are a founding and leading member, and separately with FATF itself, with Europol, and with our FVEY partners as well, to enhance international capacity to investigate and prosecute criminals using virtual currencies for illicit purposes.

And of course, our partnerships with industry are paramount in the virtual currency space. FinCEN has provided priority information on typologies of illicit virtual currency use to financial institutions through our advisory and FinCEN Exchange programs. FinCEN is also sharing cyber indicators of compromise to help the financial sector detect, report, and defend against cyber activity that may be connected with illicit financial activity.

The information we are able to share with industry is built on top of high quality information we receive in BSA reporting.

Since 2013, FinCEN has received nearly 70,000 Suspicious Activity Reports (SARs) involving virtual currency exploitation. Just over half of these reports come from virtual currency industry filers, likely many of you participating today. We also get valuable reporting from more traditional financial institutions that also have a unique window into illicit financial flows involving virtual currency, such as banks that may see ransomware payments made by customers or MSBs that see funds transfers derived from account takeovers.

This reporting is incredibly valuable to FinCEN and law enforcement, especially when you include technical indicators associated with the illicit activity, such as Internet Protocol (IP) addresses, malware hashes, malicious domains, and virtual currency addresses associated with ransomware or other illicit transactions.

However, there remain significant issues that concern us in the virtual currency space. Many of these are issues some of you may have heard me address before:

- Risks associated with anonymity-enhanced cryptocurrencies, or AECs, remain unmitigated across many virtual currency financial institutions. We expect each financial institution to have appropriate controls in place based on the products or services it offers, consistent with the obligation to maintain a risk-based AML program. This means we are taking a close look at the AML/CFT controls you put on the types of virtual currency you offer—whether it be Monero, Zcash, Bitcoin, Grin, or something else—and you should too. To be sure, FinCEN and our delegated examiners at the IRS are focused on this.

- We are also increasingly concerned that businesses located outside the United States continue to try to do business with U.S. persons without complying with our rules. These include registering, maintaining a risk-based AML program, and reporting suspicious activity, among other requirements. If you want access to the U.S. financial system and the U.S. market, you must abide by the rules. We are serious about enforcing our regulations, including against foreign businesses operating in the United States as unregistered MSBs. We take this very seriously and encourage you to include detailed information about such businesses in your SAR filings when you identify suspicious activity. If you are going to avail yourself of the U.S. financial system from abroad, you cannot do so without engaging in the financial integrity practices that make this financial system so powerful, stable, trusted, and desirable.

Conclusion

As I conclude, I want to thank you all again for giving me this time today. FinCEN is committed to enhancing our capabilities and understanding of virtual currencies and to encouraging and fostering responsible innovation. We look forward to continuing our efforts with all of you in this regard.

Thank you.

###