Testimony for the Record
Thomas P. Ott
Associate Director, Enforcement Division
Financial Crimes Enforcement Network
U.S. Department of the Treasury
House Committee on Financial Services
Subcommittee on Terrorism and Illicit Finance
June 20, 2018

Introduction

Chairman Pearce, Ranking Member Perlmutter, and members of the Subcommittee, thank you for inviting me to appear before the Subcommittee on Terrorism and Illicit Finance on behalf of the Financial Crimes Enforcement Network (FinCEN). FinCEN's mission is to safeguard the financial system from illicit use and to promote national security through the collection, analysis, and dissemination of financial intelligence.

I appreciate the opportunity to discuss Treasury's work on virtual currency and the national security implications and illicit finance risks presented by virtual currency.

FinCEN, together with other components of U.S. Department of the Treasury's Office of Terrorism and Financial Intelligence, or TFI, works to combat the illicit finance threats presented by both traditional and emerging payment systems. In doing so, our aim remains to deter, detect, and disrupt illicit finance threats from the financial system while promoting responsible technological innovation in the financial sector.

FinCEN's Regulatory Treatment of Virtual Currency

The United States has led the world in regulating and supervising virtual currency payments, including decentralized virtual currency payment activities, for anti-money laundering and countering the financing of terrorism (AML/CFT) purposes. Treasury has worked on issues pertaining to virtual currency since the early 2000s. At the federal level, FinCEN, which has the primary responsibility for administering the Bank Secrecy Act (BSA) and implementing its regulations, regulates individuals or entities engaged in the business of accepting and transmitting virtual currency from one person to another person or location as money transmitters.

Most importantly, in 2011, FinCEN issued a final rule, which among other things, defined "money transmission services" to include accepting and transmitting "currency, funds, or other value that substitutes for currency" by any means.[1] The term "other value that substitutes for currency" is intended to encompass circumstances in which the transmission does not involve

[1] Bank Secrecy Act Regulations - Definitions and Other Regulations Relating to Money Services Businesses, 76 FR 43585 (July 21, 2011). *See* also 31 CFR § 1010.100(ff)(5)(i)(A).

currency as defined by regulation, [2] or funds, but instead involves something that the parties to a transaction recognize has value that is equivalent to or can substitute for real currency. The definition of money transmission is technology neutral: whatever the platform, protocol, or mechanism, the acceptance and transmission of value from one person to another person or location is regulated under the BSA.

The 2011 rule establishes the foundation for our regulation of certain virtual currency activity and sets out the obligations of financial institutions that are money transmitters of virtual currency under the BSA.

FinCEN established that money services businesses (MSBs) that conduct money transmission denominated in other forms of value, such as virtual currency, are obligated to meet the same AML/CFT standards as other money services businesses under the BSA. This includes registering with FinCEN, establishing an AML program reasonably designed to prevent money laundering and terrorist financing, and meeting certain recordkeeping and reporting obligations—including filing Suspicious Activity Reports (SARs). The requirements apply equally to domestic and foreign-located virtual currency money transmitters, even if the foreign-located entity does not have a physical presence in the United States, as long as it does business in whole or substantial part in the United States.

To provide additional clarity and respond to questions from the private sector, in March 2013, FinCEN issued interpretive guidance on the application of FinCEN's regulations to certain transactions involving the acceptance of currency or funds and the transmission of virtual currency ("2013 Guidance"). [3] The 2013 Guidance identified the participants to some virtual currency arrangements, including an "exchanger," "administrator," and "user," and further clarifies that exchangers and administrators generally qualify as money transmitters under the BSA, while users do not. FinCEN has subsequently issued several administrative rulings providing additional clarity on virtual currency matters including, but not limited to, discussing virtual currency issues such as mining[4] and operating a virtual currency-trading platform.[5] FinCEN expects financial institutions, including those operating in virtual currency, to comply with FinCEN's regulations. This may require them to proactively evaluate their business models using the guidance and rulings that FinCEN publishes. Financial institutions that consult the regulations and guidance but are still uncertain as to whether their particular business model falls

[2] 31 CFR § 1010.100(m) (Defines currency as "[t]he coin and paper money of the United States or of any other country that is designated as legal tender and that circulates and is customarily used and accepted as a medium of exchange in the country of issuance. Currency includes U.S. silver certificates, U.S. notes and Federal Reserve notes. Currency also includes official foreign bank notes that are customarily used and accepted as a medium of exchange in a foreign country.").

[3] FIN-2013-G001, "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies," March 18, 2013.

[4] FIN-2014-R001, "Application of FinCEN's Regulations to Virtual Currency Mining Operations," January 30, 2014.

[5] FIN-2014-R011, "Request for Administrative Ruling on the Application of FinCEN's Regulations to a Virtual Currency Trading Platform," October 27, 2014.

within FinCEN's regulations may seek formal and informal regulatory interpretations from FinCEN.

Illicit Finance Risks

Fundamentally, we must maintain the integrity and accessibility of the global financial system and protect it from abuse. Virtual currency payments pose money laundering, sanctions evasion, and other illicit financing risks that necessitate careful assessment and mitigation. In particular, we are concerned about the growing use of decentralized convertible virtual currency to facilitate illicit activity, including cybercrime, fraud, extortion, drug trafficking, money laundering, and other crimes.

We have seen virtual currency exploited to support billions of dollars in what we would consider suspicious activity. For example, FinCEN analysis indicates that virtual currency transactions include over $1 billion in ransomware extortion funds and over $1.5 billion has been stolen through hacks of virtual currency exchangers and administrators over the past two years. FinCEN analysis also estimates that at least $4 billion in virtual currency has moved through darknet marketplaces since 2011.

While traditional financial methods remains the primary vehicle for most illicit activity, FinCEN believes virtual currency presents specific illicit finance risks and that without vigilance and action, the scale of this activity could grow.

In fact, we have seen an increase in SAR filings by financial institutions identifying illicit virtual currency activity. Since 2003, BSA information identifying suspicious activity involving virtual currency has grown rapidly, increasing 90 percent from 2016 to 2017. These reports have identified many thousands of virtual currency addresses tied to a wide range of suspected criminal activity and have proven immensely useful to investigations. This reporting has directly assisted important criminal and civil actions taken by law enforcement and regulators in the United States.

International Regulation

Foremost among our challenges in combatting this activity is the lack of consistent AML/CFT regulations and supervision of virtual currency activity in most jurisdictions around the world. The global nature, distributed structure, and speed of most leading virtual currency systems means that vulnerabilities in foreign jurisdictions can enable illicit activity here in the United States. Success cannot come without concerted action in the international community. We have seen great strides to address this regulatory gap in places like Australia, Japan, and South Korea, but most jurisdictions still do not have a regulatory framework in place or in-progress to address virtual currencies. Until jurisdictions ensure that these businesses adhere to the same international AML/CFT standards as other financial institutions, there will be vulnerabilities that expose the U.S. to illicit finance risks. Bad actors will continue to seek jurisdictions that permit illicit behavior and find ways to offer their services around the world.

FinCEN and other Treasury components are working to engage key jurisdictions directly and help them address these vulnerabilities in their AML/CFT regime. Our experts have provided training directly to foreign regulators and law enforcement to improve their oversight and understanding of these technologies, and will continue to conduct outreach and engagement in this area.

Further, through international standard setting bodies like the Financial Action Task Force (FATF), the United States has prioritized establishing and applying international standards for AML/CFT that cover virtual currency payments. Under the FATF Recommendations, countries should identify and assess the money laundering and terrorist financing risks in their jurisdictions related to virtual currency activities and adopt risk-based measures to mitigate those risks. Prompt and effective implementation and enforcement of the FATF AML/CFT requirements for virtual currency exchangers, hosted wallets, and similar businesses by all jurisdictions are vital for combatting the abuse of virtual currency and promoting safe, responsible innovation in the financial sector. We are pressing for jurisdictions to effectively regulate and supervise virtual currency exchangers, hosted wallets, and other virtual currency businesses that act as gateways to the regulated fiat financial system, in compliance with the international standards set by the FATF.

Anonymity-Enhanced Cryptocurrencies

There have also been developments in technology that have enabled the concealment of transaction and identity information involving virtual currency. Anonymity-enhanced cryptocurrencies (AECs)—sometimes referred to as "privacy coins"—are increasingly prevalent across exchange platforms and average around $300 million in daily transaction volume at domestic and foreign-located exchanges. We have seen AECs gain greater adoption by criminals looking for alternatives to bitcoin on darknet marketplaces. For example, AECs were adopted by the darknet marketplace AlphaBay prior to its shut down by U.S. law enforcement last year and U.S. law enforcement seized AECs from Alexander Cazes, the site's administrator.

Combating Illicit Virtual Currency Use

As part of developing and rigorously enforcing one of the most effective AML/CFT regimes in the world, FinCEN has increasingly prioritized identifying, tracing, and disrupting the flow of illicit virtual currency activity. But, as strong as our AML/CFT framework is, malicious actors will continue to attempt to exploit any vulnerability to move their illicit proceeds undetected through legitimate financial channels, in order to hide, foster, or expand the reach of their criminal or terrorist activity.

Supervision and Examinations

One of the ways FinCEN protects the financial system is by examining financial institutions for compliance with their regulatory obligations in preventing money laundering and terrorist financing. FinCEN has provided training to our delegated examiners, the Internal Revenue Service's (IRS) Small Business/Self-Employed Division. And, since late 2014, the IRS, together with FinCEN, has conducted examinations of virtual currency exchangers and administrators

across the United States. In that time, more than one-third of all registered virtual currency money transmitters in the United States have been examined, including numerous trading platforms, foreign-located exchangers, virtual currency kiosk companies, individual peer-to-peer exchangers, and five of the 20 largest exchanges by volume. Our goal is to ensure that virtual currency exchangers and administrators are subject to the same routine compliance examinations for AML/CFT as any other financial institution.

This year FinCEN has also provided virtual currency examination training to a number of state examiners, so that we can increase the reporting we receive of AML/CFT deficiencies and provide better oversight of this industry.

As with our BSA supervision of other parts of the financial services industry, these exams help FinCEN determine whether virtual currency exchangers and administrators are meeting their compliance obligations under the applicable rules. Where we identify problems, we will use our supervisory and enforcement authorities to appropriately penalize non-compliance and drive compliance improvements. Compliance only works with an effective enforcement regime.

Enforcement Actions

FinCEN has also taken significant public actions. For example, in 2013, FinCEN identified Liberty Reserve as a financial institution of primary money laundering concern under Section 311 of the USA PATRIOT Act. Liberty Reserve, a Costa Rica based administrator of the virtual currency LRDollars and LREuros, processed billions of dollars of criminal proceeds including from hackers and extortion schemes and sought to provide anonymous money laundering services to criminals around the globe. FinCEN imposed special measure five under Section 311, prohibiting U.S. financial institutions from opening or maintaining correspondent accounts with Liberty Reserve, thereby shutting it out of the U.S. financial system.

In 2015, FinCEN took its first civil enforcement action against a virtual currency business, imposing a $700,000 civil money penalty against Ripple Labs in coordination with a concurrent action by the U.S. Attorney's Office for the Northern District of California. FinCEN's action identified that Ripple Labs had operated as an unregistered MSB, had AML program failures, and failed to file SARs. Importantly, in addition to the penalty, Ripple Labs agreed to implement a remedial framework designed to bring the company into compliance with the BSA – a framework they remain under to this day. In taking this action, FinCEN wanted to provide a clear path of what compliance looks like. Our ultimate goal is not to shut down every virtual currency actor, but rather to ensure that all virtual currency entities meet AML/CFT standards.

However, we are not afraid to single out bad actors and take action. Most recently, in July 2017, FinCEN assessed a penalty of over $110 million against BTC-e; an internet-based, foreign-located money transmitter that exchanged fiat currency as well as the virtual currencies Bitcoin, Litecoin, Namecoin, Novacoin, Peercoin, Ethereum, and Dash. This action was taken with a parallel criminal action by our law enforcement partners including the Federal Bureau of Investigation, United States Secret Service, and Homeland Security Investigations, as well as those at Main Justice and the U.S. Attorney's Office for the Northern District of California. At the time, it was one of the largest virtual currency exchanges by volume in the world. BTC-e

facilitated transactions involving ransomware, computer hacking, identity theft, tax refund fraud schemes, public corruption, and drug trafficking. As part of this action, FinCEN also assessed a $12 million penalty against one of BTC-e's operators – the highest penalty we have ever assessed against an individual.

Collaboration

Collaboration is critical to combat the growing threats presented by virtual currency. To further collaboration across the financial sector, Secretary Mnuchin has convened a working group through the Financial Stability Oversight Council to bring together federal financial regulators whose jurisdictions are relevant to the oversight of virtual currencies and their underlying technologies. The working group seeks to enable the agencies to collaborate regarding these issues, including to promote consistent regulatory approaches and to identify and address potential risks.

Along these same lines, Under Secretary Mandelker has created Strategic Impact Units to combine the expertise of all TFI components to address various illicit finance challenges, including those posed by virtual currency. We have also increased our collaboration with our law enforcement partners, including those represented with me today, as well as our regulatory partners.

Just last month, I met with my enforcement counterparts at the Commodity Futures Trading Commission (CFTC) and Securities and Exchange Commission (SEC). My staff, and others at FinCEN, carefully and closely coordinate with these agencies on an ongoing basis in order to best allocate our resources to assess and address the greatest threats. This partnership has been fruitful, and the benefits are apparent through the excellent respective work by the SEC, CFTC, and FinCEN in targeting illicit actors and combating fraud related to the misuse of virtual currencies.

One area where we continue to work together is on the illicit finance risks surrounding Initial Coin Offerings (ICOs). As my SEC[6] and CFTC[7] colleagues have pointed out at prior hearings, this issue has gained a lot of attention from the public, and ICOs have experienced rapid growth since 2017. 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 that businesses involved in ICOs meet all of their AML/CFT obligations. We will remain committed to take appropriate action when these obligations are not prioritized and the U.S. financial system is put at risk.

I also want to highlight the important collaborations we have with our partners in law enforcement. We are extremely fortunate to have a team of experts within FinCEN who work very hard to keep pace with the quickly evolving technology in this area. We share that

[6] Jay Clayton, Chairman, U.S. Securities and Exchange Commission, Testimony before the Committee on Banking, Housing, and Urban Affairs, U.S. Senate, Feb. 6, 2018.

[7] J. Christopher Giancarlo, Chairman, Commodity Futures Trading Commission, Testimony before the Committee on Banking, Housing, and Urban Affairs, U.S. Senate, Feb. 6, 2018.

knowledge and analysis with law enforcement, regulators, and prosecutors domestically and globally, as we are all on the front lines of investigating illegal use of emerging payment systems.

To that end, FinCEN has provided support to over 100 cases since 2016. FinCEN's experts help law enforcement, regulators, and prosecutors trace different types of virtual currency activity, identify suspicious sources of funds, target unregistered MSBs that do business in whole or substantial part in the United States, and disrupt transnational criminal networks operating in virtual currency. To assist in tracing virtual currencies, FinCEN analysts produce detailed reports on typologies and methodologies addressing the movement of funds and the techniques used to launder illicit proceeds using virtual currency. FinCEN leverages the BSA data we receive from financial institutions to support law enforcement and develop our understanding of the threats. We also use our knowledge and resources to provide training to our law enforcement partners and help identify best practices for tracing funds and building cases.

Conclusion

As we continue to see technology evolve and integrate into the U.S. and global financial system, we must ensure that it does so in a way that allows for the transparency needed to protect the financial system. FinCEN looks forward to working with this Committee, the public sector, law enforcement, the intelligence community, and our regulatory partners to identify strategies to help ensure the United States remains both a global hub for innovation and a safe and secure financial system. Thank you for having me here today. With your support, FinCEN will continue combatting money laundering and illicit finance threats to secure our financial system, keep our nation safe and prosperous, and protect our communities and families from harm. I am happy to answer any questions you may have.