November 19, 2020

DOJ Provides Framework for Cryptocurrency Enforcement

Attorneys
Ryan Rohlfsen
Paige Berges
David Y. Chen
Thanithia Billings
John R. Santacruz

On October 8, 2020, the Department of Justice released "Cryptocurrency: An Enforcement Framework" (the "Framework"), setting out risks and enforcement initiatives related to cryptocurrency-related crime. The Framework is the second report[1] published by the Cyber-Digital Task Force (the "Task Force"), established by former Attorney General Jeff Sessions in February 2018 to analyze the "many ways that the Department is combatting the global cyber threat, and… to identify how federal law enforcement can more effectively accomplish its mission in this vital and evolving area."

In the publication press release, Attorney General Barr remarked, "Cryptocurrency is a technology that could fundamentally transform how human beings interact, and how we organize society. Ensuring that use of this technology is safe, and does not imperil our public safety or our national security, is vitally important to America and its allies." Through the Framework, the DOJ seeks to ensure safe usage of cryptocurrencies and related technology by acknowledging and highlighting their unique potential as a threat to public safety or national security. To that end, the Framework highlights the threats and illicit opportunities that the increasing use of cryptocurrencies might create.

Illicit Uses of Cryptocurrencies

Part I of the Framework first describes the fundamental attributes of cryptocurrencies and their legitimate uses, before introducing the potential illicit uses. According to the Task Force, illicit uses of cryptocurrencies generally fall into three categories:

1. Using cryptocurrency to engage in criminal activity through financial transactions. Examples include financing terrorism, sales of illegal substances, and extortion.

2. Using cryptocurrency to conceal criminal financial activity. This includes money laundering, tax evasion, and avoidance of other legal reporting requirements.

3. Committing crimes against the cryptocurrency marketplace itself, such as hacking, theft, phishing, fraud, etc., to obtain cryptocurrency illegally from victims.

Legal and Regulatory Framework

Part II of the Framework details the legal and regulatory framework that has evolved in response to the growth of cryptocurrency use, and the enforcement tools available to the DOJ and other regulators. Across both criminal and regulatory enforcement, government regulators have sought to bring action for fraud, firearm, and child exploitation-related offenses as well as regulatory breaches of Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT), sanctions, and securities laws.

1. Criminal Enforcement

Cryptocurrency is described in the Framework as an increasingly preferred payment method for distributing contraband and other illegal goods or services. As a result, enforcement agencies have been able to bring a wide variety of charges related to the misuse of cryptocurrency, including wire fraud, mail fraud, securities fraud, identity theft/fraud, computer fraud, illegal sale and possession of firearms, possession and distribution of counterfeit items, child exploitation crimes, and money laundering, among other criminal violations. The wide variety of cryptocurrency-related criminal charges that a prosecutor could pursue demonstrates how cryptocurrency has proliferated as a tool for criminal actors.

2. Regulatory Enforcement

Several U.S. government agencies and entities are involved in the growing regulation of cryptocurrency. In addition to the Department of the Treasury's Financial Crimes Enforcement Network ("FinCEN"), the Securities and Exchange Commission ("SEC"), the Commodity Futures Trading Commission (CFTC), the Internal Revenue Service ("IRS"), and state attorneys general have acted in recent years through increased enforcement and regulation to respond to the risks posed by the rapid development of cryptocurrency technology.

a. Anti-Money Laundering/Counter-Terrorist Financing

AML/CFT standards under the Bank Secrecy Act ("BSA") have been a critical tool to address cryptocurrency-related risks. Financial institutions will be familiar with these requirements, but the definition of money services businesses ("MSBs") now includes those that conduct business in virtual currency. MSBs are defined by regulation as individuals or entities who act as currency dealers or exchangers, check cashers, money transmitters, or issuers, sellers, or redeemers of traveler's checks, money orders, or stored value. The BSA, administered by FinCEN, requires MSBs to register with FinCEN, establish an AML program reasonably designed to prevent money laundering and terrorist financing, including monitoring transactions for suspicious activity and reporting suspicious transactions to relevant regulators through suspicious activity reports ("SARs").

Examples of MSBs in the cryptocurrency space include cryptocurrency exchanges (*e.g.*, Coinbase) and kiosks, as well as certain issuers, exchangers, and brokers of virtual assets such as Stellar and Abra. According to recent FinCEN guidance,[2] exchangers and administrators of virtual currencies qualify as money transmitters under the BSA and are considered MSBs (and therefore subject to the above AML/CFT requirements) to the extent they accept or transmit convertible virtual currency ("CVC," or any virtual currency that has an equivalent value as currency or acts as a substitute for currency).

FinCEN's requirements apply equally to domestic and foreign-based MSBs, even if the foreign-located MSB does not have a physical presence in the United States. The MSB need only do business in whole or substantial part in the United States.[3]

Traditional financial institutions can also face enforcement risk when doing business with customers who operate virtual currency money services businesses. In 2020, the Office of the Comptroller of the Currency ("OCC") entered into a cease-and-desist consent order with M.Y. Safra Bank after alleging that the bank (1) violated BSA requirements for establishing an adequate AML program; and (2) failed to investigate suspicious transactions and timely file SARs when opening accounts for such customers.

b. Securities Fraud

U.S. regulators have also pursued enforcement actions related to fraud, for example, in "initial coin offerings" ("ICOs") (a cryptocurrency capital-raising equivalent to an IPO). In 2017, the SEC cautioned that such ICOs may be subject to the requirements of the federal securities laws and warned investors about potential scams involving companies claiming to be related to, or asserting they are engaging in, ICOs.[4] The SEC has brought several ICO-related civil enforcement actions against individuals violating securities laws or engaging in fraudulent schemes, and has additionally issued guidance for analyzing whether a digital asset qualifies as a security.

While it has attempted to provide clarity to the industry, there is still scope for interpretation as to whether certain offerings will be considered securities. According to the SEC, "[w]hether a particular investment transaction involves the offer or sale of a security—regardless of the terminology or technology used—will depend on the facts and circumstances, including the economic realities of the transaction."[5] In October 2019, the SEC obtained a temporary restraining order against two offshore entities conducting an unregistered digital token offering both within the United States and overseas that had raised more than USD 1.7 billion of investor funds while allegedly failing to meet the registration provisions of the Securities Act of 1933.[6] A few months later, the court approved a settlement agreement that saw the entities, Telegram Group Inc. and its subsidiary TON Issuer Inc., disgorge USD 1.224 billion from the sale of its tokens as well as pay a civil penalty of USD 18.5 million.[7]

c. Economic Sanctions

The Framework also discusses how the Office of Foreign Assets Control ("OFAC") plays a role in regulating cryptocurrency use. Because of the decentralized nature of cryptocurrency and its potential to bypass traditional sanctions controls, cryptocurrency can be an attractive means for sanctioned persons to access or raise capital. In November 2018, OFAC took its first virtual-asset-related action, designating two Iran-based individuals who helped exchange Bitcoin ransom payments into Iranian currency on behalf of Iranian cyber actors involved in a computer ransomware scheme.[8] Similar ransomware attacks targeting U.S. companies have surged in recent years, and on October 1, 2020, OFAC issued a separate Advisory to clarify the risks of ransomware from a sanctions perspective.[9] OFAC has additionally designated Chinese nationals and organizations involved in illicit fentanyl manufacturing and trafficking,[10] and Russian nationals who acted or purported to act for, or on behalf of, the Internet Research Agency ("IRA"), an entity designated for its involvement in election interference activities.[11] The Chinese and Russian organizations both used cryptocurrency addresses to fund their activities.

Business Obligations as to Cryptocurrency Abuse

Part III of the Framework outlines the obligations of certain businesses that are susceptible to abuse in the cryptocurrency space and the DOJ's ongoing strategies for addressing emerging threats to the legal operation of the cryptocurrency marketplace.

Business Models that May Facilitate Criminal Activity and Regulatory Liability

The Framework identifies several business models at higher risk of misuse, but which continue to fall short of implementing regulatory requirements designed to mitigate these risks. Cryptocurrency exchanges—even those that do not accept fiat currency and operate only within cryptocurrency—are one such example. Exchanges are required to follow FinCEN recordkeeping and reporting requirements but often fail to, and may therefore miss signs of suspicious activity. Peer-to-peer exchangers, which seek to buy or sell cryptocurrency outside of registered or licensed exchanges and financial institutions, are also considered MSBs for the purposes of AML/CFT requirements. In practice, most peer-to-peer exchangers fail to register with FinCEN, and therefore similarly may not implement necessary controls to mitigate facilitating criminal activity. Cryptocurrency kiosk operators—also considered MSBs in the United States—often do not comply with regulations requiring the implementation of AML/CFT programs, including identification and reporting of suspicious transactions, despite the fact that such kiosks have been linked to illicit use by drug dealers, credit card fraud schemers, prostitution rings, and unlicensed virtual asset exchangers. Regulators have therefore been seeking to enforce regulatory breaches to encourage higher-risk businesses to implement controls to mitigate misuse.

In a recent example, on October 1, 2020, the founders and executives of a cryptocurrency derivatives exchange, the Bitcoin Mercantile Exchange ("BitMEX"), were indicted for violating the BSA and conspiring to violate the BSA by willfully failing to establish, implement, and maintain an adequate AML program. The DOJ characterized the indictment as another push "to bring platforms for money laundering into the light." Other emerging business models, such as virtual currency casinos, anonymity-enhanced cryptocurrencies, and entities that obfuscate the source or owner of units of cryptocurrency by mixing the currencies of several users prior to delivery—known as "mixers" or "tumblers"—all face similar risks and should implement appropriate AML/CFT controls to mitigate risk of criminal misuse and regulatory enforcement.

DOJ Outlook Going Forward

The DOJ stresses in the Framework that it will continue to engage with its regulatory partners in FinCEN, OFAC, the SEC, the CFTC, and the IRS to address the misuse and abuse of cryptocurrencies. The DOJ will continue to prosecute entities and individuals who violate U.S. law, even when they are not located inside the United States, due to the DOJ's jurisdiction over virtual asset transactions that touch financial, data storage, or other computer systems within the United States.

The Framework also underscores the increasing amount of resources set aside for cryptocurrency enforcement that are necessary to develop and maintain the knowledge and skills necessary to identify evolving threats. The Task Force additionally states that it will continue to foster cooperation with state and international authorities to counteract the global nature of the cryptocurrency industry and adopt consistent regulations across jurisdictions.

Key Takeaways

1. **Cryptocurrency-related activity is increasingly subject to a greater number of criminal laws and regulatory requirements.**

    a. FinCEN and other agencies like the OCC have made clear that the requirements of the BSA, particularly those related to AML/CFT, apply to cryptocurrency exchanges, issuers, exchangers, and brokers, even when they are based in foreign jurisdictions, so long as they do business in whole, or substantial part, in the United States.

    b. The SEC continues to actively monitor and take action against digital token offerings suspected of violating the Securities Act, such as the 2019 Telegram offering, to ensure that issuers cannot avoid federal securities laws by labeling offerings cryptocurrency.

    c. As criminal actors use cryptocurrency in new and creative ways to facilitate criminal acts such as ransomware, drug trafficking, and child exploitation-related offenses, state and federal prosecutors have responded with a variety of potential charges.

2. **Cryptocurrency-related businesses should design and maintain compliance programs to mitigate the risks identified by DOJ, or they may face criminal or regulatory enforcement.**

    a. Institutions should be aware of the ways that cryptocurrencies are being misused. As actions targeting funds flowing to sanctioned entities in Iran, China, and Russia have shown, cryptocurrency is a preferred method for illicit activity and may subject entities to sanctions designation. Robust compliance programs, including comprehensive sanctions screenings, should be considered best practice for any cryptocurrency-related business.

    b. Institutions should undertake a risk assessment to identify how cryptocurrencies may impact the organization's risk for exposure to money laundering and sanctions violations.

    c. Institutions may need to include information relevant to identifying cryptocurrency misuse in its Customer Due Diligence procedures, including but not limited to collecting information on wallet addresses, IP addresses, and expected cryptocurrency activity, including types of cryptocurrencies expected to be used.

1. Report of the Attorney General's Cyber Digital Task Force (July 2, 2018), available at https://www.justice.gov/ag/page/file/1076696/download.
2. Press Release, "FinCEN Issues Guidance on Virtual Currencies and Regulatory Responsibilities," U.S. DEPT. OF THE TREASURY, FIN. CRIMES ENF'T NETWORK, (Mar. 18, 2013), available at https://www.fincen.gov/news/news-releases/fincen-issues-guidance-virtual-currencies-and-regulatory-responsibilities.
3. According to FinCEN, relevant factors in determining whether an MSB does business in whole, or substantial part, in the United States include whether the foreign-located MSB is providing services to customers located in the United States, whether or not on a regular basis, or as an organized or licensed business concern. Advisory, "Foreign-Located Money Services Businesses,"

U.S. DEPT. OF THE TREASURY, FIN. CRIMES ENF'T NETWORK, (Feb. 15, 2012), available at https://www.fincen.gov/sites/default/files/advisory/FIN-2012-A001.pdf.

4. The specific digital asset in question, DAO Tokens, qualified as a security because it met the requirements of an investment of money in a common enterprise with a reasonable expectation of profits to be derived from the entrepreneurial or managerial efforts of others. Press Release, "SEC Issues Investigative Report Concluding DAO Tokens, a Digital Asset, Were Securities," U.S. SEC. AND EXCH. COMM'N, (July 25, 2017), available at https://www.sec.gov/news/press-release/2017-131
5. *Id.*
6. Press Release, "SEC Halts Alleged $1.7 Billion Unregistered Digital Token Offering," U.S. SEC. AND EXCH. COMM'N, (Oct. 11, 2019), available at https://www.sec.gov/news/press-release/2019-212.
7. Press Release, "Telegram to Return $1.2 Billion to Investors and Pay $18.5 Million Penalty to Settle SEC Charges," U.S. Sec. and Exch. Comm'n, (June 26, 2020), available at https://www.sec.gov/news/press-release/2020-146.
8. Press Release, "Treasury Designated Iran-Based Financial Facilitators of Malicious Cyber Activity and for the First Time Identifies Associated Digital Currency Addresses," U.S. DEPT. OF THE TREASURY, (Nov. 28, 2018), available at https://home.treasury.gov/news/press-releases/sm556.
9. Client Alert, "Between a Rock and a Hard Place: OFAC Issues Advisory on Ransomware Payments," ROPES & GRAY LLP, (Oct. 2, 2020), available at https://www.ropesgray.com/en/newsroom/alerts/2020/10/Between-a-Rock-and-a-Hard-Place-OFAC-Issues-Advisory-on-Ransomware-Payments.
10. Press Release, "Treasury Targets Chinese Kingpins Fueling America's Deadly Opioid Crisis," U.S. DEPT. OF THE TREASURY, (Aug. 21, 2019), available at https://home.treasury.gov/news/press-releases/sm756.
11. Press Release, "Treasury Sanctions Russia-Linked Election Interference Actors," U.S. DEPT. OF THE TREASURY, (Sept. 10, 2020), available at https://home.treasury.gov/news/press-releases/sm1118.