COMPLIANCE & ENFORCEMENT

Program on Corporate Compliance and Enforcement at New York University School of Law

DOJ Issues Cryptocurrency Enforcement Framework

by J. Christopher Giancarlo, Elizabeth P. Gray, Justin L. Browder, Conrad G. Bahlke, and Richard M. Borden

On October 1, 2020, the Cyber-Digital Task Force ("Task Force") of the United States Department of Justice ("DOJ") issued a Cryptocurrency Enforcement Framework ("Framework").[1] The Framework summarizes threats posed by illicit uses of cryptocurrency, the applicable laws that the DOJ and other federal regulatory agencies apply in seeking to identify and mitigate such threats, and the ongoing challenges faced by the DOJ in prosecuting criminal conduct in the digital asset ecosystem. The Framework details an extensive array of federal, state, and international laws and regulations that apply to cryptocurrencies and reflect the emerging approach to cryptocurrency regulation and enforcement by federal and state governments. While the extensive patchwork of regulations suggests a need for harmonization, the Framework refrains from calling for any new or amended legislation, regulation, or other rules. It also does not discuss the government's use of sophisticated technology to track cryptocurrency transactions and develop its cryptocurrency-related cases. Importantly, the Framework does not advocate for legal or regulatory suppression of cryptocurrency, as some initial commentators suggested.

The Framework was published in response to a 2018 DOJ report that recommended that the Task Force "continue evaluating the emerging threats posed by rapidly developing cryptocurrencies that malicious cyber actors often use."[2] While focusing on federal enforcement against illegal use of cryptocurrency, the Framework also recognizes that distributed ledger technology "raises breathtaking possibilities for human flourishing,"[3] and that cryptocurrency represents a transformative way to store and exchange value. It notes that the market today includes over 2,000 cryptocurrencies, which enable users to transfer virtual currency around the globe in exchange for goods, services, and other sources of value.

Threats Posed by Cryptocurrency

Part I of the Framework tacitly acknowledges that cryptocurrencies and the digital asset ecosystem hold great promise for innovation in financial services, ranging from the extension of credit to individuals not served by existing banking institutions to helping individuals in countries beset by inflation avoid a decline in their nation's currency. The Framework emphasizes, however, that "whatever the overall benefits and risks of cryptocurrency, the [DOJ] seeks to ensure . . . adherence to the law and . . . the protection of public safety and national security."[4] In that regard, the Framework identifies numerous illegal activities for which cryptocurrencies are used, separated into three categories:

- **Using Cryptocurrency Directly to Commit Crimes or to Support Terrorism**, including buying and selling illegal things, buying and selling tools to commit crimes, for ransom, blackmail, and extortion, and for raising funds for criminal and terrorist activities.
- **Using Cryptocurrency to Hide Financial Activity**, including money laundering, operating unlicensed, unregistered, or non-compliant exchanges and avoiding taxes and sanctions.
- **Committing Crimes within the Cryptocurrency Marketplace Itself**, including theft and fraud, so-called "cryptojacking" whereby hackers force compromised computers to generate cryptocurrency.[5]
- **Darknet Markets** or "darknet websites and marketplaces that allow criminals around the world to connect"[6] are also highlighted as a key source of illegal activity. For example, in 2017, the DOJ seized and shut down a darkweb market known as "AlphaBay," which at the time of its seizure "serv[ed] over 200,000 users as a conduit for everything from illegal drugs and firearms to malware and toxic chemicals."[7]

Applicable Law and Regulations

a. Criminal Code Authorities

The Framework lists a wide range of criminal provisions used by the DOJ in prosecuting cryptocurrency-related conduct. Broadly, these provisions fall into four categories: (1) fraud, (2) exchange of controlled items, (3) money laundering or other financial crimes, and (4) forfeitures.

- **Fraud**. Among these are a variety of fraud statutes, including wire fraud, mail fraud, securities fraud, access device fraud, and fraud and intrusions in connection with computers.[8]
- **Exchange of Controlled Items**. The Framework enumerates federal statutes governing the illegal sale and possession of firearms, the possession and

distribution of counterfeit items or controlled substances, and the distribution of child exploitation materials as examples of laws that the DOJ has used to prosecute illegal use of cryptocurrency.

The DOJ has also pursued actions violating these statutes:

- **Money Laundering and Financial Crimes**. The Framework further provides that the DOJ brings cases under federal statutes governing money laundering, transactions involving proceeds of illegal activity, operation of an unlicensed money transmitting business and Bank Secrecy Act ("BSA") requirements.[9]
- **Forfeiture**. In cases where no person is charged criminally or a defendant is not prosecutable, the DOJ also states that it "frequently uses existing criminal authorities to seize and forfeit virtual assets."[10]

b. Regulatory Authorities

The Framework identifies six federal regulatory authorities that have jurisdiction over cryptocurrency and other digital assets, and highlights certain state and international efforts relating to cryptocurrency. The discussion brings into sharp relief the patchwork nature of cryptocurrency regulation in the U.S. and abroad.

The Framework highlights the regulatory authorities, enforcement efforts, and work the DOJ has done in cooperation with: (1) The Financial Crimes Enforcement Network ("FinCEN"), (2) the Office of Foreign Assets Control ("OFAC"), (3) the Office of the Comptroller of Currency ("OCC"), (4) the Securities and Exchange Commission ("SEC"), (5) the Commodity Futures Trading Commission ("CFTC"), (6) the Internal Revenue Service ("IRS"), (7) state authorities, and (8) international regulation and the Financial Action Task Force ("FATF").

- **FinCEN**. The Framework emphasizes the regulatory framework applicable to money services businesses ("MSBs") and virtual asset service providers ("VASPs").[11] According to the Framework, in the United States "individuals involving virtual assets, such as cryptocurrency exchanges and kiosks, as well as certain issuers, exchangers, and brokers of virtual assets, are considered MSBs." Further, it states that MSBs are subject to anti-money laundering and combating the financing of terrorism ("AML/CFT") regulations.[12] FinCEN is responsible for administering the BSA, and for overseeing the MSBs regulated under the BSA (which includes both foreign and domestic MSBs, so long as they do business with the United States). FinCEN has stated that it considers convertible virtual currency ("CVC") within its purview and expects MSBs

operating in the cryptocurrency space to abide by the same AML/CFT obligations as all other MSBs.

- **OFAC**. OFAC is responsible for enforcing economic and trade sanctions against foreign countries and governments, terrorist organizations, drug traffickers, and those trafficking weapons of mass destruction. U.S. persons and entities are responsible for ensuring that they do not violate OFAC's sanctions, including through the use of digital currency or assets.
- **OCC**. OCC is a branch of the Treasury Department "that charters, regulates, and supervises national banks and federal savings associations."[13] In July 2020, OCC published an Interpretive Letter clarifying that it is a permissible form of modern banking for "national banks and federal savings associations to provide cryptocurrency custody services for their customers" and to hold the cryptographic keys associated with cryptocurrency.[14] In 2020, OCC also entered into a cease-and-desist agreement with a bank that it alleged failed to comply with the BSA's AML rules, in part because the bank failed to implement appropriate risk controls when opening accounts for customers who operated virtual-currency money services businesses.
- **SEC**. The DOJ's discussion of the SEC's work in the cryptocurrency area focuses on "initial coin offerings" ("ICOs"). Companies use ICOs to raise capital for projects from investors who are granted tokens that give them access to goods and services, sometimes a share in the profit of the funded project, or an increase in value if the project succeeds. In 2017, the SEC issued a report putting the public on notice that ICOs and other digital asset offerings could fall within the purview of U.S. securities laws, using a longstanding definition of a "security" to determine whether the ICOs fell within that definition.[15] Subsequently, the SEC has successfully brought enforcement actions against numerous offerors of ICOs for conducting unregistered and, in some instances, fraudulent offerings.[16]
- **CFTC**. "The CFTC has oversight over derivatives contracts, including futures, options, and swaps, that involve a commodity"[17] which the CFTC has concluded can include certain virtual currencies. The CFTC has acted against alleged fraudulent offers of virtual currency and related derivatives, and against unregistered bitcoin futures exchanges illegally offering margined or financed retail virtual currency transactions and has taken steps to enforce firms' obligations to maintain appropriate AML procedures.
- **IRS**. The IRS applies general tax principles for property transactions to virtual currency transactions. Similarly, income generated by virtual currencies transactions or wages paid in virtual currency are taxed as normal (and the latter reported on W-2s).
- **State Authorities**. In some instances, the state equivalents of the above agencies have taken enforcement and regulatory actions in the virtual currency

space. New York, in particular, has taken an aggressive posture with respect to ICOs. In 2018, the North American Securities Administrators Association announced that multiple state and provincial securities regulators were coordinating actions to tackle fraudulent ICOs and cryptocurrency investment products.[18]

Joint DOJ Actions with Federal Agencies

Despite the patchwork of regulations, the DOJ and federal agencies often work hand in hand to prosecute cryptocurrency-related crimes. This coordination is critical to combatting fraud in the marketplace. For example:

- FinCEN and the DOJ cooperated in 2015 to secure a $700,000 penalty against a cryptocurrency operator who knowingly failed to comply with the BSA.[19]
- In 2018, pursuant to "cyber sanctions" imposed by executive order, OFAC identified two Iranian nationals for sanctions for their role in funneling bitcoin to Iran-based hacking organizations, and assisted the DOJ in bringing criminal charges against the individuals.[20] On March 2, 2020, the DOJ brought criminal charges against those two individuals for money laundering conspiracy and for operating an unlicensed money transmitting business. The DOJ's criminal action was brought in connection with sanctions imposed by OFAC, which had identified the two individuals who were alleged to have laundered over $100 million worth of cryptocurrency stolen from exchanges by North Korean actors.[21]
- In one DOJ fraud case, a defendant pled guilty to securities fraud after making false claims about a digital currency being sold in an ICO as well as how much money had been raised in the ICO. The SEC filed a parallel civil action, and the defendant paid nearly $2.7 million in disgorgement, interest and penalties in the civil action brought by the SEC.[22]
- In 2018, the CFTC and DOJ collaborated to bring an action related to a fraudulent scheme concerning binary options and a virtual currency. The CFTC was able to secure an order that the defendants had committed fraud and misappropriated millions of dollars in client funds, for which they had to pay $4.25 million. The DOJ was able to secure 86 months' imprisonment for wire fraud conspiracy and obstruction.[23]

Challenges and DOJ Strategies

Part IV of the Framework addresses business models which, when deployed by bad actors, present challenges to the DOJ's law enforcement efforts. According to the DOJ, the following business models may facilitate criminal activity:

- **Cryptocurrency Exchanges**. The Framework states that cryptocurrency exchanges are subject to the FinCEN recordkeeping and reporting requirements, including foreign-located exchanges with sufficient ties to the United States. As noted above, the DOJ views compliance with BSA regulations as "crucial" to their enforcement efforts.
- **Peer-to-Peer Exchanges and Platforms**. The Framework defines peer-to-peer ("P2P") exchanges or trades as networks of individuals, as opposed to registered or licensed exchanges and financial institutions, who facilitate transfers of value for the public, including the buying and selling of cryptocurrency. The Framework states that while P2P exchanges are considered MSBs and subject to FinCEN recordkeeping and reporting requirements, many fail to register with FinCEN as MSBs or to comply with the BSA.
- **Cryptocurrency Kiosks**. Cryptocurrency kiosks are stand-alone machines that allow users to convert fiat currency to and from cryptocurrencies. As with the prior examples, the Framework identifies operators of such kiosks as MSBs and subject to the BSA and further notes that many are non-BSA compliant.
- **Virtual Currency Casinos**. A virtual currency casino is a casino that facilitates various forms of betting denominated in bitcoin and other virtual currencies. These casinos are similarly subject to the BSA, either as MSBs or as licensed casinos (depending on gaming revenue), and the requirements thereunder.
- **Anonymity Enhanced Cryptocurrencies**. Cryptocurrencies which do not use public blockchain technology are known as "anonymity enhanced cryptocurrencies" or ("AECs"). The DOJ views these currencies as a particularly high-risk activity that is indicative of possible criminal conduct due to inherent features of AECs which may undermine AML/CFT controls and specifically advises companies offering AECs to consider their increased risk of use for AML/CFT activities in their compliance efforts.
- **Mixers, Tumblers, and Chain Hopping**. The DOJ describes the purpose of these entities as seeking to obfuscate the source or owner of particular units of cryptocurrency by mixing the cryptocurrency of several users prior to delivery of such currency to its ultimate destination. In addition to identifying these entities as MSBs subject to the BSA, the Framework highlights the increased risk of criminal liability for these businesses due to their inherent function of concealing the source of financial transactions.[24]

Conclusion

The Framework is a significant effort by the DOJ to define and describe its focus with respect to legal enforcement against bad actors in cryptocurrency markets. The emphasis on the BSA and the regulatory and reporting requirements applicable to

MSBs and VASPs highlights the need for market participants to have robust compliance programs, particularly with respect to AML/CFT. While the Framework provides clear examples of criminal and unlawful activities across a number of legal frameworks, the absence of robust guidelines from federal regulators overseeing the cryptocurrency markets creates a necessity for proactive and innovative compliance efforts.

Footnotes

[1] U.S. Dep't of Justice, Report of the Attorney General's Cyber-Digital Task Force: Cryptocurrency Enforcement Framework (2020) (the "Framework"), *available* here (PDF: 9 MB).

[2] Framework at vii.

[3] *Id.*

[4] *Id.* at 5.

[5] *Id.* at 2-16.

[6] *Id.* at 16.

[7] *Id.* at 47.

[8] *Id.* at 20.

[9] *Id.* at 21.

[10] *Id.* at 21.

[11] Federal law defines an MSB as a: i. currency dealer or exchanger; ii. check casher; iii. issuer of traveler's checks, money orders, or stored value; iv. seller or redeemer of traveler's checks, money orders, or stored value; v. money transmitter; or vi. the U.S. Postal Service. 31 C.F.R. § 1010.100(ff).

Under the Financial Action Task Force (FATF) Recommendations, VASPs are individuals or entities operating as a business to conduct one or more of the following activities for or on behalf of another entity or individual:

1. Exchanges between virtual assets and fiat currencies;
2. Exchanges between one or more forms of virtual assets;
3. Transfer of virtual assets;

4. Safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; or
5. Participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.

The FATF Recommendations: International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation 126 (June 2019) [hereinafter FATF International Standards], available here (last accessed Oct. 13, 2020) at 127.

[12] Framework at 22.

[13] *Id.* at 29.

[14] OCC Interpretive Letter #1170, Authority of a National Bank to Provide Cryptocurrency Custody Services for Customers (July 22, 2020), *available* here (PDF: 160 KB) (last accessed Oct. 15, 2020).

[15] U.S. Sec. & Exch. Comm'n, Release No. 81207: Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO 10 (July 25, 2017), *available* here (PDF: 172 KB) (last accessed Oct. 15, 2020).

[16] The Framework at 31.

[17] *Id.* at 32.

[18] *Id.*

[19] *Id.*

[20] *Id.* at 26.

[21] *Id.* at 27.

[22] *Id.* at 31-32.

[23] *Id.* at 33.

[24] *Id.* at 37-44.

Elizabeth P. Gray and **Justin L. Browder** are partners, **J. Christopher Giancarlo** is senior counsel, and **Conrad G. Bahlke** and **Richard M. Borden** are counsel, at Willkie Farr & Gallagher LLP.

Disclaimer

The views, opinions and positions expressed within all posts are those of the author alone and do not represent those of the Program on Corporate Compliance and Enforcement (PCCE) or of New York University School of Law. PCCE makes no representations as to the accuracy, completeness and validity of any statements made on this site and will not be liable for any errors, omissions or representations. The copyright of this content belongs to the author and any liability with regards to infringement of intellectual property rights remains with the author.