NORTON ROSE FULBRIGHT

Blockchain Law

DOJ's 'Cryptocurrency Enforcement Framework'

By Robert A. Schwinger, *New York Law Journal* — January 19, 2021

In his Blockchain Law column, Robert A. Schwinger discusses a new DOJ report which outlines the various uses of cryptocurrency, the various channels through which the DOJ will take enforcement action in regard to cryptocurrency, and the public safety challenges relating to enforcement against the illicit uses of cryptocurrency. The DOJ is sending a clear message that it will not hold back on enforcing the laws as they currently are written, and that it is well within DOJ's power to regulate criminal activity even where it involves a novel and developing area like cryptocurrency.

Debates continue to swirl over how lightly or heavily cryptocurrency should be regulated. The interest in giving breathing room for an exciting new financial technology to grow and experiment often finds itself pitted against the interest in protecting the public from unscrupulous actors who may seek to exploit an area that is not always well understood and in which consensus may not yet exist about what laws are best suited for the area given the various competing interests. Questions also are raised about to what extent enforcement actions as opposed to other regulatory avenues should be employed as the means for protecting the public.

The U.S. Department of Justice (DOJ) has not been shy about staking out its position in this area, and its position is simple and direct: To the extent cryptocurrency-related activity may fall within the scope of existing laws as written, the DOJ intends to enforce those laws against persons who violate them.

In October 2020, DOJ released an 83-page report entitled "Cryptocurrency Enforcement Framework" (the Report), authored by the Attorney General's Cyber-Digital Task Force. This is the second such report issued by the Cyber-Digital Task Force, the first having been released in February 2018. The new Report outlines the various uses—both for good or ill—of cryptocurrency, the various channels through which the DOJ will take enforcement action in regard to cryptocurrency, and the public safety challenges relating to enforcement against the illicit uses of cryptocurrency. While cryptocurrency may still be a relatively new and emerging technology, the Report notes that "this technology already plays a role in many of the most significant criminal and national security threats out nation faces." The Report represents DOJ's response.

Some early commentators have been wary of the Report's expansive nature and have expressed concerns that the Report will hinder development and innovation in the cryptocurrency

Robert A. Schwinger is a partner in the commercial litigation group at Norton Rose Fulbright US LLP. **Abigail Schwarz**, an associate in the firm's commercial litigation group, assisted in the preparation of this article.

space. The Report acknowledges that there are legitimate as well as illegitimate uses of cryptocurrency, but stands firm that the illicit uses raise concerns that call for legitimate law enforcement by the DOJ and others. In the Report, the DOJ is sending a clear message that it will not hold back on enforcing the laws as they currently are written, and that it is well within DOJ's power to regulate criminal activity even where it involves a novel and developing area like cryptocurrency, where there perhaps is not yet firm social consensus on what the optimal regulatory structures and principles governing it should be.

Uses of cryptocurrency for good or ill

The first section of the Report outlines the basics of cryptocurrency and various legitimate and illegitimate uses of cryptocurrency. It provides an overview of the basics of virtual currency and how cryptocurrency can virtually be stored and exchanged between persons, a cryptocurrency exchange, or other intermediaries.

The Report notes that there are over 2,000 cryptocurrencies that all can be legitimately used and exchanged for goods and services. It acknowledges that cryptocurrencies may be useful in countries wrought with inflation and they may help facilitate future "micro-payments" for lower cost goods and services without the need for credit or debit due to the higher transaction costs associated with those forms of payment. The Report also notes that the privacy afforded by cryptocurrency can also be beneficial as it may reduce the risk of identity theft.

While acknowledging these "legitimate uses" of cryptocurrency, the Report states "whatever the overall benefits and risks of cryptocurrency, the [DOJ] seeks to ensure that uses of cryptocurrency are functionally compatible with adherence to the law and with the protection of public safety and national security." The Report then identified three broad categories of wrongdoing that can be perpetrated through the "illicit" use of cryptocurrency:

> "(1) engage in financial transactions associated with the commission of crimes, such as buying and selling drugs or weapons on the dark web, leasing servers to commit cybercrimes, or soliciting funds to support terrorist activity; (2) engage in money laundering or shield otherwise legitimate activity from tax, reporting, or other legal requirements; or (3) commit crimes directly implicating the cryptocurrency marketplace itself, such as stealing cryptocurrency from exchanges through hacking or using the promise of cryptocurrency to defraud unwitting investors."

The Report also addresses the role that "Darknet Markets" play in facilitating illegal activity in which cryptocurrency is used. The Report describes how these "Darknet Markets" provide a place where wrongdoers, cloaked with anonymity, can further their crimes through using cryptocurrency, such as selling illegal goods and laundering money, and otherwise allow for the exploitation of cryptocurrency.

Laws covering crimes that are committed using cryptocurrency

The second section of the Report outlines the various statutory and regulatory provisions that can be used to enforce against the misuses of cryptocurrency and prosecute those who engage in such activity. While the Report highlights the breadth of statutes and regulatory provisions at the DOJ's disposal for enforcement within the cryptocurrency space, it makes clear that these are all existing legal authorities that the DOJ is well within its rights to use in enforcing against a variety of criminal conduct, even that involving cryptocurrency.

The Report enumerates various types of crimes that can be committed with the use of cryptocurrency and the corresponding federal charges that may be brought against those engaging in that type of activity. For crimes involving cryptocurrency and the sale of illegal goods and services and financial instruments, the perpetrators may be prosecuted pursuant to various federal statues including, but not limited to, wire fraud (18 U.S.C. §1343), mail fraud (18 U.S.C. §1341), securities fraud (15 U.S.C. §§78j, 78ff), access device fraud (18 U.S.C. §1029), identity theft and fraud (18 U.S.C. §1028), fraud and intrusions in connection with computer systems (18 U.S.C. §1030), illegal sale and possession of firearms (18 U.S.C. §921), possession and distribution of counterfeit items (18 U.S.C. §2320), child exploitation activities (18 U.S.C. §2251) and possession and distribution of controlled substances (21 U.S.C. §841).

For crimes involving using cryptocurrency in laundering money, federal charges that can be brought include money laundering (18 U.S.C. §1956), transactions involving proceeds of illegal activity (18 U.S.C. §1957), operation of an unlicensed money transmitting business (18 U.S.C. §1960), and failure to comply with Bank Secrecy Act (BSA) requirements (31 U.S.C. §5331). Cryptocurrency transactions can also subject an individual or organization to federal charges where the transactions facilitate support for terrorists (18 U.S.C §§2339A, 2339B) or other crimes concerning national security such as espionage (18 U.S.C. §792).

Certain virtual assets or properties may also be subject to criminal forfeiture (18 U.S.C. §982; 21 U.S.C. §853) or civil forfeiture (18 U.S.C. §981).

In addition to the wide-ranging criminal and civil federal charges that DOJ has authority to bring against cryptocurrency-related misconduct, the Report also identifies other federal agencies that can enforce statutes and regulations against persons that use cryptocurrency in illicit ways, parallel to the DOJ's own enforcement. The agencies and offices highlighted include the Financial Crimes Enforcement Network (FinCEN), the Office of Foreign Assets Control (OFAC), the Office of the Comptroller of the Currency (OCC), the Securities and Exchange Commission (SEC), the Commodity Futures Trading Commission (CFTC), and the Internal Revenue Service (IRS).

The Report takes particular note of the SEC's powers and the reach of the securities laws to address cryptocurrency by applying the "*Howey* test" for "investment contracts" from *SEC v. W. J. Howey Co.*, 328 U.S. 293, 301 (1946), to make sure that cryptocurrencies which qualify under that test as investment contracts—and thus as securities—therefore comply with securities statutes and SEC rules. The Report also points in this regard to the SEC's April 2019 Framework for 'Investment Contract' Analysis of Digital Assets, and the SEC's victory what the Report terms its "landmark Telegram case," *SEC v. Telegram Group*, 448 F. Supp. 3d 352 (S.D.N.Y. 2020).

When it comes to regulatory authorities, however, cryptocurrency enforcement does not just stop at the waterline. The Report also notes international regulatory authorities and their role in the international enforcement of laws relating to cryptocurrency. While the international regulation of cryptocurrency lacks consistent enforcement, the Report highlights the role of the Financial Action Task Force (FATF), "an intergovernmental organization that was founded in 1989 on the initiative of the G7," in bringing consistency to international enforcement of cryptocurrency crimes and misuses. The FATF aims to encourage standardized strategies globally for combatting money laundering, terrorist financing, proliferation of weapons of mass destruction, and other financial system threats, including where such crimes are perpetrated through cross-border cryptocurrency exchanges.

Cryptocurrency enforcement challenges

The third and final section of the Report outlines various challenges in enforcing against the "bad" uses of cryptocurrency and how the DOJ, along with the bevy of regulatory agencies it works with, are dealing with these challenges.

The Report identifies certain "business models" that may be at a higher risk of knowingly or unknowingly facilitating criminal activity and incurring liability through the use of cryptocurrency. These business models include typical virtual asset exchanges and brokers, but also include peer-to-peer exchanges and platforms, cryptocurrency kiosk operators, and online casinos. The Report notes that these new types of models can be difficult to regulate and can "fail to comply" with certain reporting and registration statutes that can undermine the DOJ's ability to investigate cryptocurrency adjacent crimes. The Report also states bluntly that "anonymity enhanced cryptocurrencies"—citing as examples Monero, Dash, and ZCash—are considered a "high-risk activity that is indicative of possible criminal conduct."

The Report also addresses "mixers" and "tumblers"—"entities that attempt to obfuscate the source or owner of particular units of cryptocurrency by mixing the cryptocurrency of several users prior to delivery of the units to their ultimate destination." Such entities, the Report says, are money services businesses engaged in money transmission subject to the BSA and other similar international regulations, who can face BSA liability for failing to register, conduct anti-money laundering (AML) procedures, or collect customer identification. They can be subject to criminal liability for money laundering and can run afoul of other regulations and statutes.

The Report also speaks to the lack of consistent global enforcement of virtual cross-border cryptocurrency transactions. It notes that this enforcement gap permits bad actors to engage in "jurisdictional arbitrage" and threatens the international financial system. Given these challenges and global enforcement gaps, the Report outlines the strategies that the DOJ will take to surmount them. It will continue to investigate and prosecute those who illicitly use cryptocurrency with the force of the statutes and fellow regulatory agencies discussed above. Even where these bad actors —individuals or entities—do not reside in the United States, the DOJ's position is that it has the authority to prosecute such bad actors where virtual asset transactions "touch financial, data storage, or other computer systems within the United States," asserting that the DOJ has the jurisdiction to prosecute those who "direct or conduct those transactions."

In addition to addressing the DOJ's resources for developing awareness and knowledge of cryptocurrency threats in order to better identify and prosecute such threats, the Report also notes that the DOJ will continue to foster cooperation with various state and international authorities. This cooperation will seek to promote consistent enforcement of cryptocurrency related criminal activity due to the cross-border nature of many of these transactions.

Conclusion

Some who seek to promote the use and development of cryptocurrency have expressed concerns about whether the robust tone and approach of the Report, and the DOJ's highlighting of the expansive array of resources at its disposal to enforce laws potentially implicated by cryptocurrency activity, may threaten existing and future legitimate and beneficial uses of cryptocurrency. Such concerns no doubt have been magnified by additional recent federal enforcement initiatives, such as FinCEN's controversial notice of proposed rulemaking that would require a wide variety of financial institutions "to submit reports, keep records, and verify the identity of customers" as to transactions involving certain virtual currency or digital assets. See FinCEN, Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets (Dec. 18, 2020).

But it is perhaps unrealistic to expect law enforcers like DOJ or FinCEN to take on the role of balancing social interests to devise what sound policy should be in this still relatively novel area. The Report shows that DOJ is not inserting itself in the policy debate about cryptocurrency, but rather is reaffirming that in this space it will enforce existing laws as written, particularly where bad actors make use of cryptocurrency to carry out criminal activities. To the extent that industry participants and commentators feel that it will be more beneficial to moderate enforcement of at least some existing laws in regard to cryptocurrency in order to foster innovation, the Report may simply confirm that it will only be through legislative and regulatory advocacy and change that such a goal can be achieved. As of now, though, the Report provides a firm statement that the DOJ intends to prosecute and enforce against wrongdoers in the cryptocurrency space no less than in any other.