

DOJ Cryptocurrency Enforcement Framework Signals Escalating Enforcement Activity

Law360
12.10.20

This [article](#) appeared in Law360 on December 7, 2020.

Commentary provided by Daniel Stabile.

How are we to think about cryptocurrency, one of the predominant expressions of blockchain technology? Is it a banner, heralding a revolution that will transform the financial sector and other industries? Is it a car, presenting dangers that are tolerated when balanced against significant societal utility?

Reading the cryptocurrency enforcement framework,[1] published by the attorney general's Cyber-Digital Task Force in the waning days of the present administration, one gets the impression that the [U.S. Department of Justice](#) views cryptocurrency as something more like a gun.

The introduction of the framework, which is attributed to Sujit Raman, then an associate deputy attorney general and the chair of the task force, takes a balanced tack.

While emphasizing that distributed ledger technology "raises breathtaking possibilities for human flourishing" that should not be "inhibited or suppressed," Raman also rightly warns against the role that cryptocurrencies — like any new technology, product, or system — could play "in the wrong hands" or "without appropriate safeguards and oversight."

Ultimately, he sets forth the noble goal of creating public policy that "brings into alignment" the "complementary concepts" of "technological innovation and human flourishing."

But the tonal symmetry of the introduction contrasts sharply with the body of the 83-page document. The framework is divided into three parts, beginning with a threat overview.

After opening the section with a crisp and useful primer on cryptocurrency and a few paragraphs on legitimate uses, the framework adopts a more consistently sinister tone, presenting a cavalcade of cryptocurrency-related illicit activity and vice, including a darknet child pornography website that accepted bitcoin, terrorist organizations soliciting donations in cryptocurrency, and cryptocurrency exchanges serving as conduits for money laundering.

The DOJ is a law enforcement agency, and even the most ardent advocates for cryptocurrency could not have reasonably expected that the framework would focus on the positive, transformative potential of this new asset class. But regulatory tone is important, and many key actors in the

DOJ Cryptocurrency Enforcement Framework Signals Escalating Enforcement Activity

bourgeoning industry sector perceive hostility in the environment.

For example, just days before the release of the framework, a co-founder of [Ripple Labs Inc.](#), a cross-border payments firm that serves institutions such as [American Express Co.](#) and major international banks,[2] told a reporter from Fortune: "[t]he message is blockchain and digital currencies are not welcome in the U.S." [3]

Other governmental and regulatory authorities, even within the U.S., have demonstrated that it is possible to set a different tone while maintaining a commitment to appropriately monitoring the industry and protecting the public.

For instance, the U.S. [Office of the Comptroller of the Currency](#), a key prudential bank regulator, recently released an interpretive letter expressly permitting banks to custody cryptoassets for customers and to provide financial services for cryptocurrency businesses.[4]

Forbes contributor Matt Hougan described the letter as "positive and progressive," "showcas[ing] a deep understanding of the crypto market, including ... the challenges that crypto companies have historically faced in obtaining traditional banking services." [5]

As the OCC's general counsel later told Coindesk, a prominent digital currency news organization, the OCC has been considering the legal and supervisory questions relating to cryptocurrency for years; he also expressed intellectual humility and openness, stating that "[t]his will continue to be learning process for us" and encouraging industry "engagement." [6]

Law and Regulations

The second part of the framework, on law and regulations, begins with citations to various sections of the criminal code, the tools available to the Department of Justice to prosecute unlawful activity, ranging from anti-fraud provisions, to drug trafficking statutes, to forfeiture code sections.

But the main component of this part of the framework consists of an overview of other federal entities with overlapping authority, including the [Financial Crimes Enforcement Network](#), the U.S. [Office of Foreign Assets Control](#), the U.S. [Securities and Exchange Commission](#), the [Commodity Futures Trading Commission](#), and the [Internal Revenue Service](#).

For most of these agencies and regulatory bodies, the framework provides a broad introduction to their authority and describes each entity's interaction with the Department of Justice.

If the intention of this section of the framework is to demonstrate a coordinated and synchronized effort, it risks having the opposite effect. The financial services regulatory environment in the U.S. is complex, and its complexity is intensified as it relates to cryptocurrency because of the sometimes conflicting and underdeveloped regulatory pronouncements and rules.

DOJ Cryptocurrency Enforcement Framework Signals Escalating Enforcement Activity

Companies seeking to do business in the U.S. must confront not only the federal regulators and law enforcement agencies, but also their state counterparts. Even the most sophisticated and well-capitalized cryptocurrency-related businesses struggle to understand the full regulatory landscape, and to chart a realistic course to ensure compliance with the myriad obligations.

As Ripple's CEO articulated the problem, "many responsible private players are trying to follow the rules, but that becomes increasingly hard when there's no single arbiter of the law."^[7] While seeking a single voice in the U.S. to regulate cryptocurrency is asking for too much, given the history and structure of financial services regulation, the industry's frustration with the lack of regulatory clarity is authentic and understandable.

The framework is an essential document to help well-intentioned actors understand the government's enforcement priorities and strategy, but it does little to advance the objectives of regulatory clarity and harmonization. Without progress on that front in the short term, the U.S. risks motivating many legitimate cryptocurrency businesses to move outside of the U.S.

Ongoing Challenges and Future Strategies

The issue of jurisdictional arbitrage — taking advantage of discrepancies in different legal jurisdictions — appears to be top of mind to the task force. It is one of the issues addressed in the final section of the framework, titled "Ongoing Challenges and Future Strategies."

While the framework notes that the DOJ will work with "international counterparts to continue development of comprehensive and consistent international regulation of virtual assets," the current international landscape is deeply fractured.

Cryptocurrency by its very nature lends itself particularly well to moving between and outside of international borders. What does it mean for a bitcoin, which is a digital representation of value on a distributed ledger maintained simultaneously on machines throughout the world, to be within the U.S.? One of the most important aspects of the framework is a strong signal to offshore entities that the DOJ has enforced — and will continue to enforce — the U.S. criminal law extraterritorially.

Earlier in the framework, the task force stresses that the department:

has robust authority to prosecute [virtual asset service providers] and other entities and individuals that violate U.S. law even when they are not located inside the United States. Where virtual asset transactions touch financial, data storage or other computer systems within the United States, the Department generally has jurisdiction to prosecute the actors who direct or conduct those transactions.

DOJ Cryptocurrency Enforcement Framework Signals Escalating Enforcement Activity

The framework asserts that the department has extraterritorial jurisdiction in other situations, including when the foreign actors provide illicit services to or defraud U.S. persons.

In a demonstration of its seriousness on this point, the framework was issued shortly after the announcement of the criminal indictment of Seychelles-based Bitcoin Mercantile Exchange, or BitMEX, for violating the Bank Secrecy Act for failing to monitor money laundering activity.[8]

Conclusion

Reading the framework as a whole, the task force has created a thorough and impressive history of its enforcement efforts, an introduction to many of the other applicable regulators and law enforcement bodies, and an articulation of some of its enforcement priorities. Above all, it puts the industry on notice that its activity in this space will increase.

The cryptocurrency community remains hopeful that future guidance will address the legitimate issues of streamlining and harmonizing the legal and regulatory landscape, which will significantly help to achieve the aspiration of the framework's Introduction: to "establish background conditions that help the innovative spirit to thrive."

Daniel Stabile is a partner at [Shutts & Bowen LLP](#) and an adjunct professor at the University of Miami Law School.

[1] United States Dep't of Justice, Report of the Attorney General's Cyber-Digital Task Force, "Cryptocurrency Enforcement Framework" (Oct. 2020), available at <https://www.justice.gov/ag/page/file/1326061/download> (last visited Dec. 2, 2020).

[2] Ripple.com (last visited Dec. 2, 2020) (listing American Express, PNC, Santander and other institutions as its customers).

[3] Turner Wright, "'Crushing' regulations could drive Ripple out of US," Cointelegraph (Oct. 6, 2020), available at <https://cointelegraph.com/news/crushing-regulations-could-drive-ripple-out-of-us> (last visited Dec. 2, 2020).

[4] Letter from Jonathan V. Gould, Senior Deputy Comptroller & Chief Counsel of the Office of the Comptroller of the Currency, to Redacted Entity (July 22, 2020), available at <https://www.occ.gov/topics/charters-and-licensing/interpretations-and-actions/2020/int1170.pdf> (last visited Dec. 2, 2020).

[5] Matt Hougan, "The OCC's Notice on Crypto Is a Really Big Deal," Forbes (July 27, 2020), available at <https://www.forbes.com/sites/matthougan/2020/07/27/the-occs-notice-on-crypto-is-a-really-big-deal/?sh=3bb7cbc96301> (last visited Dec. 2, 2020).

DOJ Cryptocurrency Enforcement Framework Signals Escalating Enforcement Activity

[6] Nikhilesh De, "The OCC's Crypto Custody Letter Was Years in the Making," Coindesk (Aug. 18, 2020), available at <https://www.coindesk.com/occ-crypto-custody-years> (last visited Dec. 2, 2020).

[7] Joshua Mapperson, "Community Reacts of New DOJ Crypto Enforcement Guidelines," Cointelegraph (Oct. 9, 2020), available at <https://cointelegraph.com/news/community-reacts-to-new-doj-crypto-enforcement-guidelines> (last visited Dec. 2, 2020).

[8] Tatiana Koffman, "BitMex Charged with Failing to Prevent Money Laundering," Forbes (Oct. 1, 2020), available at <https://www.forbes.com/sites/tatianakoffman/2020/10/01/bitmex-exchange-charged-with-failing-to-prevent-money-laundering/?sh=539c8c4c3652> (last visited Dec. 2, 2020).

Practice Areas

Financial Services

Industries

Financial Services

Offices

Miami