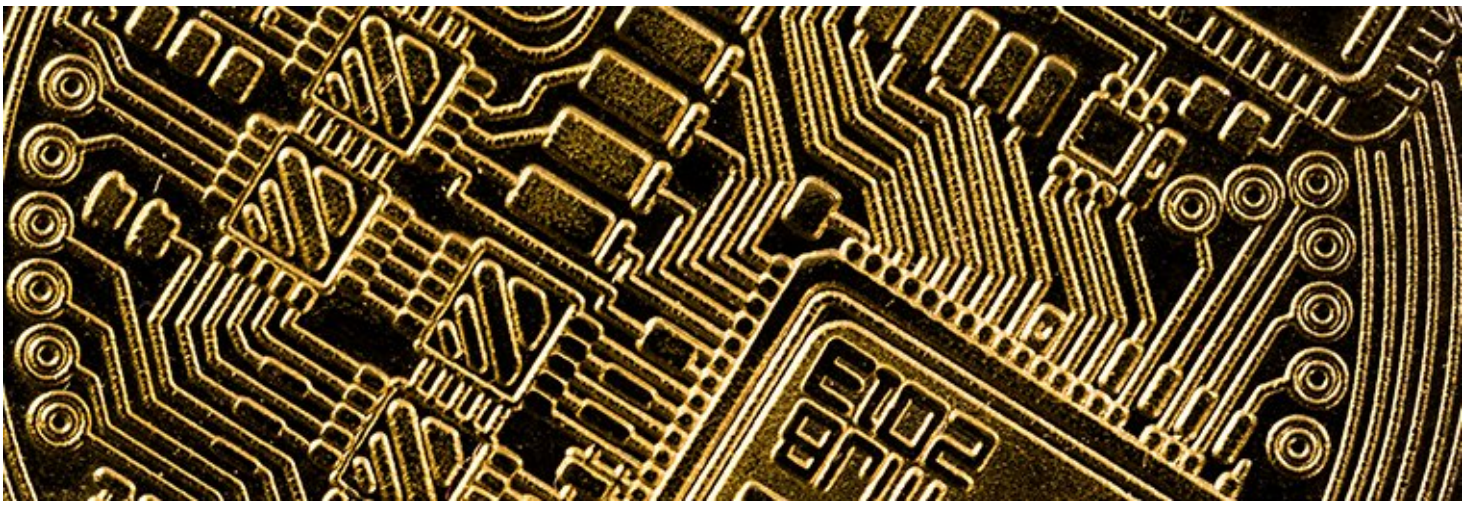


Unpacking the DOJ's cryptocurrency guidance: Enforcement priorities and industry implications

White Collar Alert

Financial Services Alert

15 October 2020
By: Benjamin Klein | Deborah R. Meshulam

On October 8, 2020, the US Department of Justice's (DOJ) Cyber-Digital Task Force issued its first crypto-related guidance, "Cryptocurrency: An Enforcement Framework," an 83-page report intended to help the industry comply with US legal obligations. While the DOJ's report praises blockchain and digital ledger technology for their "breathtaking possibilities," it also issues a stark warning: "cryptocurrency technology plays a role in many of the most significant criminal and national security threats that the United States faces." After providing a helpful overview of cryptocurrency for lay readers, the report examines the role of the DOJ in prosecuting crypto-related misconduct, including applicable federal statutes, key partnerships and enforcement challenges.

The report was issued mere days after the DOJ announced one of its most significant crypto-related prosecutions of 2020: the criminal indictment of the founders and senior executives of one of the world's biggest cryptocurrency exchanges – the Bitcoin Mercantile Exchange (BitMEX). On October 1, 2020, the SDNY announced money laundering charges against four BitMEX executives, accusing the group of Bank Secrecy Act violations. On the same day as the DOJ indictment, the Commodity Futures Trading Commission (CFTC) brought a civil enforcement action against BitMEX executives as well as five entities that own and operate BitMEX, claiming that they are operating an unregistered trading platform and violating anti-money laundering (AML) and other CFTC

DLA Piper is a global law firm operating through various separate and distinct legal entities. Further details of these entities can be found at www.dlapiper.com. This may qualify as

regulations. Three of the four individual defendants remain at large; the fourth defendant was released on $5 million bail last week.[1] As of the date of this article, all of the individual defendants have stepped down from their executive positions at BitMEX, including the former CEO and former CTO.[2]

Read together, the report and unsealed BitMEX indictment serve notice on offshore cryptocurrency exchanges and other money services businesses (MSBs) thought to be operating outside of the reach of US authorities – US law enforcement agencies have a long reach and will not hesitate to act. In this alert, we offer three key takeaways for crypto exchanges, issuers and other industry participants, as well as thoughts on what to expect going forward.

A. Many weapons in the prosecutorial arsenal – including statutes that can ensnare foreign actors

Federal prosecutors have relied on – and will continue to rely on – a number of statutes prosecuting crypto-related crimes, including charges for wire/mail fraud (18 U.S.C. §§ 1343, 1341), securities fraud (15 U.S.C. §§ 78j and 78ff), access device fraud (18 U.S.C. § 1029), identity theft/fraud (18 U.S.C. § 1028), fraud/intrusion in connection with computers (18 U.S.C. § 1030), money laundering (18 U.S.C. §1956 et seq.), tax evasion (26 U.S. Code § 7201), failure to comply with Bank Secrecy Act requirements (31 U.S.C. § 5331 et seq.), and the operation of an unlicensed money transmitting business (18 U.S.C. § 1960). Other relevant federal laws include those criminalizing drug trafficking (21 U.S.C. § 841 et seq.), sale/possession of counterfeit items (18 U.S.C. § 2320), illegal sale/possession of firearms (18 U.S.C. § 921 et seq.), child exploitation (18 U.S.C. § 2251 et seq.), and transactions involving proceeds of illegal activity (18 U.S.C. § 1957). The government can also seek criminal and civil forfeiture of cryptocurrency and other assets, as it has in cases involving state actors and terrorist organizations. Under civil forfeiture laws, US authorities can seize assets even where there are no criminal charges or where a defendant may not be prosecutable.

The report emphasizes the use of money laundering statutes to address cryptocurrency crimes, explaining that the DOJ "can bring to bear a wide variety of money laundering charges in cases involving misuse of cryptocurrency." Money laundering is identified as one of the most significant risks for cryptocurrency due to the "the explosion of online marketplaces and exchanges that use cryptocurrency," which provide criminals with the ability to "move vast sums of money efficiently across borders" while "cover[ing] their financial footprints and to enjoy the benefits of their illegitimate earnings."

The report also warns that issuers, exchangers and brokers of digital assets are considered to be MSBs subject to anti-money laundering and "know your customer" (KYC) requirements, and that such companies/individuals are subject to oversight by the Department of the Treasury's Financial Crimes Enforcement Network (FinCEN). Notably, FinCEN's requirements apply with equal force to both domestic- and foreign-located MSBs, "even if the foreign-located MSB does not have a physical presence in the United States," if the MSB conducts business "in whole or substantial part in the United States."

While the DOJ observes that "some of the largest cryptoasset exchanges operate outside of the United States" (see our note on "jurisdictional arbitrage" below), it also warns exchanges to "take seriously their legal and regulatory obligations . . . to protect users and to safeguard potential evidence in criminal or national security investigations." The DOJ states that it will "take appropriate action" if crypto exchanges breach these obligations, and the BitMEX prosecutions will serve as an important test case. The indictment accuses the BitMEX defendants – three out of four of whom are outside the US – of Bank Secrecy Act violations for willfully failing to establish, implement and maintain AML and KYC controls.

B. Strategic partnerships with other regulators

The DOJ works with multiple federal regulators and enforcement agencies, including the US Securities and Exchange Commission (SEC), the CFTC, the Internal Revenue Service, FinCEN, and the Office of Foreign Assets Control, among others. For instance, the DOJ and SEC have coordinated in recent years on numerous matters involving allegedly fraudulent initial coin offerings (ICOs). In January 2018, the SEC filed a civil complaint in federal court in Texas seeking to halt an allegedly fraudulent ICO involving a crypto startup called AriseBank. The DOJ brought criminal charges against AriseBank's CEO later that year, claiming that he defrauded investors out of millions of cryptocurrency assets. The CEO ultimately pled guilty in the criminal case to one count of securities

DLA Piper is a global law firm operating through various separate and distinct legal entities. Further details of these entities can be found at www.dlapiper.com. This may qualify as

fraud; in the civil action, the CEO and the COO agreed to pay nearly $2.7 million in disgorgements, interest and penalties.

In 2017, the DOJ and the SEC similarly brought parallel enforcement proceedings against Brooklyn businessman Maksim Zaslavskiy for securities fraud in connection with two ICOs. In its September 2017 complaint, the SEC alleged that Zaslavskiy's companies, RECoin Group Foundation LLC and DRC World Inc., sold digital tokens in a pair of ICOs that qualified as unregistered offerings of securities, and that Zaslavskiy made false or misleading representations and omissions in connection with both token sales. In October 2017, the DOJ filed a criminal complaint charging Zaslavskiy with securities fraud conspiracy for similar misconduct – engaging in illegal, unregistered securities offerings and making material misstatements to deceive investors in connection with the ICOs. Zaslavskiy pled guilty to conspiring to commit securities fraud in November 2018 and, a year later, was sentenced to 18 months' imprisonment for the crime.

The BitMEX prosecutions are the most recent example of the DOJ's cross-agency collaborations. While neither the DOJ/CFTC have offered any detailed comments on their collaboration, both actions were announced on the same day, and the SDNY thanked the "attorneys and investigators at the CFTC for offering their expertise in the development of this investigation" in its press release.

Separately, the DOJ is also coordinating with foreign regulators, including through the Financial Action Task Force (FATF), an intergovernmental organization founded to promote effective implementation of legal, regulatory, and operational measures for combating money laundering and other threats to the international financial system. The US is a founding member of the FATF and, "while holding the FATF presidency from July 2018 through June 2019, made it a priority to regulate [virtual asset service providers] for AML" and combatting the financing of terrorism. The report also highlights several internationally coordinated enforcement actions targeting the use of digital assets in a wide range of criminal activity ranging from drug trafficking to child sexual exploitation.

C. Challenges to enforcement

Despite its successes, the DOJ acknowledges several significant crypto-related enforcement challenges, including:

> **Geography:** The report claims that industry participants are engaging in "jurisdictional arbitrage" and deliberately operating from more lax jurisdictions. The DOJ describes the "inconsistency" in regulations as "detrimental to the safety and stability of the international financial system" and claims it has "imped[ed] law enforcement's ability to investigate, prosecute, and prevent criminal activity involving or facilitated by virtual assets." The BitMEX indictments address this point, accusing the defendants of taking "affirmative steps purportedly designed to exempt BitMEX from application of US laws like AML and KYC requirements," noting that the company "incorporate[d] in the Seychelles, a jurisdiction they believe had less stringent regulation."[3]
>
> **Anonymity:** In addition to geographic hurdles, the DOJ must overcome the challenges posed by anonymity mechanisms baked into the technology. While some cryptocurrencies like Bitcoin have public blockchains and thus offer some level of transaction transparency, others operate on non-public or private blockchains, and their transactions are more opaque. Consider Monero, Zcash, and Dash – cryptocurrencies described in the report as "private coins" or "anonymity enhanced cryptocurrencies."
>
> **Obfuscation:** There are a number of mechanisms for helping disguise and conceal cryptocurrency transactions, including "mixing," "tumbling," and "chain hopping" – all of which make it more difficult to track and trace assets. Mixers and tumblers are entities intended to obfuscate the source or owner of particular units of cryptocurrency by commingling the cryptocurrency of several users prior to delivery of the units to their ultimate destination. The DOJ warns that companies offering mixing or tumbling services are engaged in money transmission, and therefore are MSBs subject to AML and similar requirements. As explained in the report: "operators of these services can be criminally liable for money laundering because these mixers 'conceal or disguise the nature, the location, the source, the ownership, or the control' of a financial transaction." "Chain hopping" is the practice of moving from one cryptocurrency to another, often in rapid succession, and is criticized by the DOJ as "a potential way to obfuscate the trail of virtual currency by shifting the trail of transactions."

DLA Piper is a global law firm operating through various separate and distinct legal entities. Further details of these entities can be found at www.dlapiper.com. This may qualify as

D. What comes next

The report's detailed presentation of laws and regulations applicable to digital assets, US government agencies with relevant enforcement capabilities, and representative cases initiated to date sends a strong message that the DOJ and its sister agencies remain very focused on preventing the use of digital assets and blockchain technology for criminal purposes. That focus and creativity of US law enforcement in pursing these cases will likely increase as cryptocurrency adaptation increases. In the meantime, it would be prudent to expect that the DOJ and other US regulators will continue to expand their efforts to combat crimes in this area, using the full array of available statutes, and will not shy away from hard and challenging matters, with the BitMEX prosecutions serving as important test cases.

An earlier version of this article appeared on *Law360* on October 14, 2020.

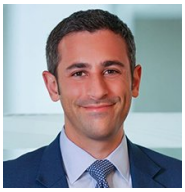
---

[1] Daniel Palmer, "BitMEX CTO Released in US After Payment of $5M Bond," *Coindesk* (Oct. 12, 2020), available at https://www.coindesk.com/bitmex-cto-reed-us-5m-bond

[2] Yogita Khatri, "BitMEX announces leadership changes after U.S. government charges, Arthur Hayes no longer CEO," *The Block* (Oct. 8, 2020), available at https://www.theblockcrypto.com/post/80163/bitmex-announces-leadership-changes-arthur-hayes-no-longer-ceo

[3] According to the indictment, HAYES allegedly "bragged in or about July 2019 that the Seychelles was a more friendly jurisdiction for BitMEX because it cost less to bribe Seychellois authorities – just 'a coconut' – than it would cost to bribe regulators in the United States and elsewhere." United States v. Hayes, 20 Cr. 500, Indictment, Para. 21. FBI Assistant Director William F. Sweeney Jr. included the following retort in the DOJ's October 1, 2020 press release: "Thanks to the diligent work of our agents, analysts, and partners with the CFTC, [the defendants] will soon learn the price of their alleged crimes will not be paid with tropical fruit, but rather could result in fines, restitution, and federal prison time."

AUTHORS



Benjamin Klein
Of Counsel
Washington, DC | T: +1 202 799 4000
ben.klein@dlapiper.com

Deborah R. Meshulam
Partner
Washington, DC | T: +1 202 799 4000
deborah.meshulam@dlapiper.com

DLA Piper is a global law firm operating through various separate and distinct legal entities. Further details of these entities can be found at www.dlapiper.com. This may qualify as