GT GreenbergTraurig

Alert | White Collar Defense & Special Investigations/ Blockchain

October 2020

DOJ's Cryptocurrency Framework: A New Perspective?

On October 8, 2020, the Department of Justice's Cyber-Digital Task Force (DOJ) published "Cryptocurrency: An Enforcement Framework" (the Framework), which provides DOJ's perspective on emerging law enforcement issues and challenges in areas involving cryptocurrency. As we have discussed previously, the government's scrutiny of virtual currencies has increased as challenges surrounding regulation of this burgeoning space reveal themselves to be novel and increasingly complex. DOJ's newest Framework is the second detailed report issued by the Attorney General's Cyber-Digital Task Force, which was established in February 2018. In issuing the Framework, U.S. Attorney General William Barr stated that ensuring the use of cryptocurrency "is safe, and does not imperil our public safety or our national security, is vitally important to America and its allies." The Framework thus represents DOJ's latest articulation of its evolving perspective as it relates to the cryptocurrency regulatory landscape.

The Framework is split into three sections: an overview of the cryptocurrency space and its illicit uses; the laws and regulatory agencies that oversee the space; and the current enforcement challenges and potential strategies to address them. While the Framework discusses the various ways that cryptocurrency is susceptible to abuse, it also recognizes that digital assets may offer several legitimate uses. The Framework, consequently, evidences a shift in DOJ's perspective, from viewing the use of cryptocurrency as a presumptive red flag for money laundering and criminality, to recognizing cryptocurrency as a legitimate instrument of commerce with law enforcement challenges like any other means of exchange.

The Framework begins with an overview of the basics of cryptocurrency and some legitimate uses for digital tokens. The Framework discusses the concept of "virtual currencies," which it defines as "a digital representation of value that, like traditional coin and paper currency, functions as a medium of exchange – i.e., it can be digitally traded or transferred, and can be used for payment or investment purposes." The Framework notes that virtual currency "is separate and distinct from digital representations of traditional currencies, securities, and other traditional financial assets" because virtual currency "does not have legal tender status in any particular country or for any government or other creditor." The Framework then discusses cryptocurrencies, a specific type of virtual currency with "key characteristics," such as "[reliance on] complex algorithms, a distributed ledger that is often referred to as the 'blockchain,' and a network of peer-to-peer users to maintain an accurate system of payments and receipts." The Framework also explains how cryptocurrency can be used illicitly, by: (1) engaging 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) engaging in money laundering or shielding otherwise legitimate activity from tax, reporting, or other legal requirements; or (3) committing 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. DOJ illustrates these examples by citing criminal cases brought by DOJ and civil enforcement actions brought by the Commodity Futures Trading Commission (CFTC) and the Securities and Exchange Commission (SEC) – an example listed is *SEC v. Telegram Group*, discussed on GT's Blockchain blog.

The second section details the legal authorities DOJ uses to prosecute those who misuse cryptocurrency and describes the roles and responsibilities of other agencies with oversight or enforcement power in the space, such as the Financial Crimes Enforcement Network (FinCEN), the Office of Foreign Assets Control (OFAC), the Office of the Comptroller of the Currency (OCC), the SEC, the CFTC, and the Internal Revenue Service (IRS). The Framework also highlights DOJ's partnership with the Financial Action Task Force (FATF), an intergovernmental organization that in recent years has assumed a significant role in promoting uniform global anti-money laundering standards, including in the cryptocurrency space.

The third section explains enforcement challenges in combating illicit uses of cryptocurrency, and specifically explores the obligations of certain businesses and other entities that are particularly vulnerable to abuse in the cryptocurrency space. Here, DOJ takes the opportunity to discuss its strategies for addressing emerging threats to the cryptocurrency marketplace. Also, DOJ recognizes that new players in the market often use business models (like cryptocurrency exchanges, peer-to-peer platforms, kiosks, and casinos) that make these transactions difficult to regulate and often fail to comply with applicable reporting and registration requirements. Further, DOJ warns that business selling "mixing" or "tumbling" services, which obscure the source of funds, may run afoul of U.S. money laundering restrictions. Finally, DOJ notes that the cross-border nature of cryptocurrency transactions leads to compliance gaps, inconsistent regulations, and "jurisdictional arbitrage," when participants move virtual assets to jurisdictions where authorities lack regulatory frameworks to support investigations.

In addressing these enforcement gaps, DOJ commits to "using all the tools" available to the agency in order to mitigate these challenges. It notes that it can expand its resources by conducting parallel investigations with other domestic and foreign agencies. The Framework also explains that DOJ's cross-border jurisdictional reach can be quite broad; a jurisdictional nexus exists when the aim of criminal activity is to cause harm inside the United States or to U.S. citizens or interests, even if individuals committing criminal activity are non-citizens acting entirely abroad.

The publication of this Framework signals DOJ's effort to prevent criminal activity using cryptocurrency, including a specific focus on the proliferation of cryptocurrency to facilitate terrorist activity and money

laundering. While cryptocurrency provides many benefits to financial institutions and users alike – a fact that DOJ now openly acknowledges – companies and individuals dealing in the cryptocurrency space should be attentive to the illicit cryptocurrency uses and risks identified by DOJ to avoid unwanted law enforcement scrutiny.

Authors

This GT Alert was prepared by:

- Kyle R. Freeny ‡ | +1 202.331.3118 | freenyk@gtlaw.com
- David I. Miller | +1 212.801.9205 | David.Miller@gtlaw.com
- Charlie Berk | +1 212.801.6436 | berkc@gtlaw.com
- Sarah M. Mathews | +1 303.572.6512 | mathewss@gtlaw.com

‡ Admitted in California. Practice in the District of Columbia limited to matters and proceedings before Federal courts and Agencies.