Alert

October 9, 2020

COZEN O'CONNOR

The Department of Justice Announces the First-of-its-Kind Cryptocurrency Enforcement Framework

On October 8, 2020, Attorney General William Barr announced the release of a Cryptocurrency Enforcement Framework produced by the Department of Justice (DOJ) Cyber-Digital Task Force. The 83-page framework is intended to help cryptocurrency entrepreneurs understand and comply with U.S. legal obligations. The framework outlines the DOJ's strategies for addressing emerging cyber threats associated with the cryptocurrency industry.

Among the many important insights provided by this framework, here are three key takeaways:

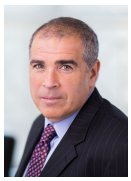
- Cryptocurrency exchanges and related entities that exchange or transmit virtual assets for a fee are considered money services businesses (MSBs) subject to anti-money laundering (AML) and "know your customer" (KYC) requirements and oversight by the Department of the Treasury's Financial Crimes Enforcement Network (FinCEN).
- FinCEN's requirements apply equally to U.S.-based and foreign-based cryptocurrency businesses that operate in the United States, including businesses that have no physical presence in the United States.
- DOJ has clearly signaled in this report that failure to comply with U.S. regulatory requirements can result in federal criminal charges and forfeiture.

The report first details three common categories of illicit uses of cryptocurrency: (1) financial transactions associated with the commission of crimes; (2) money laundering and shielding income from tax obligations and/or reporting requirements; and (3) crypto crimes directly implicating the cryptocurrency marketplace.

It then reviews the array of federal criminal laws at DOJ's disposal to prosecute these crimes, which include federal laws requiring compliance with the Bank Secrecy Act (BSA), and laws prohibiting wire and mail fraud, securities fraud, tax crimes, identity theft and fraud, money laundering, transactions involving proceeds of illegal activity, and operation of an unlicensed money transmitting business. Relevant federal laws also cover child exploitation, drug trafficking, and illegal trafficking of firearms.

The framework highlights that "individuals and entities that offer money transmitting services involving virtual assets … as well as certain issuers, exchangers, and brokers of virtual assets, are considered MSBs … subject to AML/combating the financing of terrorism (CFT) regulations as well as certain licensing and registration requirements[.]" The report notes that "such virtual currency administrators and exchangers are obligated to have AML programs, to file Suspicious Activity Reports (SARs), and to follow other BSA requirements." The report adds that anonymizing service providers offering mixing and tumbling services are likewise considered money transmitters required to register with FinCEN. The framework stresses that "FinCEN's requirements apply equally to domestic and foreign-located MSBs — even if the foreign located MSB does not have a physical presence in the United States" as long as the "MSB do[es] business in whole or substantial part in the United States."

The report emphasizes the importance of money laundering statutes as a tool to combat cryptocurrency crimes, explaining that "[t]he Department also can bring to bear a wide variety of money laundering charges in cases involving misuse of cryptocurrency." The framework warns that "individuals and companies engaged in money transmission involving virtual assets … may be subject to, and may fail to comply with, both federal and State registration, record keeping, and reporting requirements[,]" and details potential charges for virtual asset service providers who fail to comply with such requirements.



Barry Boss

**Co-Chair, Commercial Litigation Department
 Co-Chair, White Collar Defense & Investigations**

bboss@cozen.com
Phone: (202) 912-4818
Fax: (866) 413-0172

Related Practice Areas

- White Collar Defense & Investigations

Industry Sectors

- Cryptocurrency and Blockchain Technology

The framework further discusses the civil and criminal forfeiture laws at DOJ's disposal to seize and forfeit virtual assets and other property derived from crimes involving cryptocurrency. The DOJ explains that these statutes "allow the government to 'arrest' the assets themselves, even in cases where no person is charged criminally or where a defendant may not be prosecutable due to … death or flight from a jurisdiction."

The report additionally outlines the regulatory frameworks overseen by the Securities and Exchange Commission (SEC), the Commodity Futures Trading Commission (CFTC), and the Department of Treasury. In so doing, the DOJ makes the significant observation that the "CFTC has concluded that certain virtual currencies are 'commodities' under the [Commodity Exchange Act (CEA)]" and observes that "multiple federal courts have held that virtual currencies fall within the CEA's definition of commodity." This report thus confirms that regulation of many well-established digital assets should fall under the auspices of the CFTC rather than the SEC.

Turning to SEC oversight, the report focuses on regulating initial coin offerings (ICOs) and emphasizes that the "SEC encourages individuals and entities in the digital asset marketplace to engage proactively with SEC staff as the marketplace continues to develop." In addition, in discussing Treasury regulations, the framework observes that "[i]ncome, including capital gains, from virtual currency transactions is taxable, and virtual currency transactions themselves must be reported on a taxpayer's income tax return." These observations offer critical guidance for cryptocurrency entrepreneurs.

The final section details DOJ's ongoing concerns regarding business models deployed by certain cryptocurrency exchanges that may facilitate criminal activity. The framework notes that cryptocurrency exchanges, peer-to-peer exchangers, cryptocurrency kiosks, and virtual currency casinos play a key role in the cryptocurrency ecosystem and "have a heightened responsibility to safeguard their platforms and businesses from exploitation by nefarious actors and to ensure that customer data is protected and secured." The report also stresses the responsibility of these entities to collect and maintain customer and transactional information required by the BSA. The report finally highlights that it considers the listing and trading of anonymity enhanced cryptocurrencies such as Monero, Dash, and Zcash, by MSBs "to be a high-risk activity that is indicative of possible criminal conduct." Thus, exchanges should carefully consider whether listing these anonymity enhanced virtual assets is worth the increased risk of regulatory exposure.