DOJ Releases Framework for Cryptocurrency Enforcement

October 15, 2020

On October 8, 2020, the U.S. Department of Justice ("DOJ") released the publication "Cryptocurrency: An Enforcement Framework," ("Framework") which described emerging threats and enforcement challenges associated with cryptocurrency. DOJ's Cyber-Digital Task Force produced the Framework to highlight important relationships DOJ has built with other domestic and international regulatory and enforcement partners, and its strategic response to address emerging issues concerning cryptocurrency and the "blockchain" or "distributed ledger" technology underlying it. The Framework's stated goal is to ensure that cryptocurrencies and associated technologies are safe and do not imperil public safety or national security. While DOJ explicitly recognizes cryptocurrency's potential in the Framework, it also outlines both threats and illicit opportunities that cryptocurrency provides for nefarious actors. The Framework is divided into three parts.

Part I

Part I of the Framework begins with an overview of potential threats presented by use of cryptocurrency, and a recognition of the unique challenges it presents due to inherent features that can enable illicit use (decentralized operation and a high degree of anonymity). While also outlining cryptocurrency's legitimate uses (*e.g.*, enabling worldwide transfers of value without utilizing a financial intermediary, thereby minimizing transaction costs), the

Authors/Presenters

J. Ashley Ebersole

Partner
Washington
ashley.ebersole@bclplaw.com

Benjamin M. Saul

Partner
Washington
benjamin.saul@bclplaw.com

Mark A. Srere

report goes on to identify three categories into which illicit uses of cryptocurrency typically fall:

- 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;
- money laundering and unlawfully shielding legitimate activity from taxes, reporting obligations, or other legal requirements; or
- crimes directly implicating the cryptocurrency marketplace, such as stealing cryptocurrency from exchanges through hacking, or defrauding investors through the use or promise of cryptocurrency.

Partner / Co-Leader, Investigations, Financial Reg. and White Collar
Washington
mark.srere@bclplaw.com

Jason C. Semmes

Associate
Washington
jason.semmes@bclplaw.com

Part II

Part II of the Framework outlines the legal and regulatory tools available to the DOJ to confront these threats. The section outlines the typical federal crimes charged for improper conduct involving cryptocurrency, and highlights DOJ's goal of furthering enforcement by leveraging relationships with other federal regulatory and enforcement agencies, such as the Securities and Exchange Commission ("SEC"), Commodity Futures Trading Commission ("CFTC"), and Department of the Treasury components including the Financial Crimes Enforcement Network ("FinCEN"), Office of Foreign Assets Control ("OFAC"), Office of Comptroller of the Currency ("OCC"), and the Internal Revenue Service ("IRS"). Also highlighted was DOJ's coordination with state attorneys general and international law enforcement agencies. The Framework details important milestones in the agencies' coordinated efforts, including significant indictments and disgorgement of billions of dollars in ill-gotten gains.

Part III

The Framework's third and final section details challenges the government faces in cryptocurrency enforcement. It underscores that complex technologies present novel questions for law enforcement, and describes facets of cryptocurrency business models (*e.g.*, peer-to-peer exchanges, Bitcoin kiosks, and virtual casinos) and evasive measures (*e.g.*, "mixing" or "tumbling" crypto assets to conceal their source) that often facilitate criminal activity. The report closes with responsive strategies DOJ is actively employing, including continued aggressive investigation and prosecution of malicious actors, maintaining

relationships with other enforcement agencies, and engaging with the private sector to detect and punish bad actors.

The Framework is notable for its recognition of the need to balance aggressive enforcement of illicit activities with an appreciation of the important ways that cryptocurrency and blockchain technology are transforming how we interact and organize in finance, business, and beyond. The Framework's lasting effects will be borne out over time, particularly given its structure as a document that is largely descriptive summary and its emphasis on the primacy of existing relationships with other regulators. And DOJ's opportunities to take transformative action may lie in the degree to which the agency fulfills its goals of enhancing the "vigorous enforcement plan, regulatory scheme, and policy framework" that exists among its sister agencies – domestic and abroad, and furthering expertise among law enforcement (including via private sector outreach efforts).

Bryan Cave Leighton Paisner's Fintech team has extensive experience helping clients navigate the complex legal and regulatory environment surrounding cryptocurrencies and crypto-assets in the US and across the globe. Those with questions should contact a member of the team.

RELATED PRACTICES

Fintech

Securities & Corporate Governance

White Collar/Corporate Crime