DOJ's Cryptocurrency Enforcement Framework

October 22, 2020

On October 8, 2020, the Department of Justice released a Cryptocurrency Enforcement Framework authored by the Attorney General's Cyber Digital Task Force . The Framework discusses law enforcement's increasing concerns with the use of cryptocurrency, the legal and regulatory tools the government uses to combat crimes involving cryptocurrency, and the enforcement challenges cryptocurrencies pose to regulators. Attorney General William Barr described the report as "a cohesive, first-of-its kind framework for those seeking to understand federal enforcement priorities in this growing space." Also in October of 2020, federal prosecutors in New York and Pennsylvania brought separate indictments against individuals for crimes involving cryptocurrencies.

Because cryptocurrencies are to money what cell phones were to the telephone, we urge businesses and professionals of all kinds to familiarize themselves with this not-so-new form of money, and to be aware of the many pros and cons of working with cryptocurrencies. As evidenced by DOJ's new Cryptocurrency Enforcement Framework, failing to do so can result in unwelcome scrutiny from US law enforcement. In addition, as the Enforcement Framework highlights, US and global regulators are increasingly partnering together to investigate and prosecute crimes involving cryptocurrencies, given the global popularity of this new form of money.

What is cryptocurrency?

Cryptocurrency is a medium of exchange used to facilitate the trade of goods and services between parties. Quite simply, it is a form of money. Unlike paper money (also known as "fiat" currency), which is typically printed and controlled by a central bank, cryptocurrency is often created by decentralized networks and housed on a blockchain —a digital ledger maintained by a disparate network of computers.

On the one hand, cryptocurrencies are complex and sophisticated instruments - they are secured by cryptography that makes them nearly impossible to counterfeit or double-spend, and they are sent and received at electronic "addresses" that consist of long chains of alphanumeric characters. While the transactions between addresses can be analyzed, it can be difficult to connect those transactions to their underlying users.

On the other hand, cryptocurrencies are simple and accessible to just about anyone. For example, people can "buy" cryptocurrencies like Bitcoin in kiosks at many malls and gas stations. People can then transmit cryptocurrencies directly between two cell phones, store them in electronic wallets or the equivalent of electronic safety-deposit boxes, and borrow, lend and trade them like money. Cryptocurrencies allow users to avoid traditional intermediaries like banks and other financial institutions, which is helpful for those who live in countries where inflation is rampant or governments are unstable and corrupt. The ability to cut out banks and financial intermediaries also means the fees associated with those institutions can be eliminated. Bitcoin is the most well-known cryptocurrency, although there are thousands of different cryptocurrencies, with a total market capitalization in the hundreds of billions of dollars.

Anyone who thinks they will never deal with cryptocurrencies might be surprised - Microsoft, Overstock.com,

Starbucks, Subway, Burger King and Playboy are just a few of the many companies around the world that accept payment in cryptocurrency.

Cryptocurrency's Greatest Strengths are its Greatest Weaknesses

The decentralization, security and anonymity that cryptocurrencies offer make them ideal for many legitimate financial applications. However, those same characteristics also make cryptocurrencies useful for engaging in criminal activities. For example, cryptocurrencies can facilitate transactions on the dark web, including for drugs and weapons. Cryptocurrencies are also the preferred payment method for criminals perpetrating cybercrimes involving ransomware, blackmail and extortion, and for terrorists, drug cartels and other criminal syndicates looking to raise funds. Cryptocurrencies also provide criminals with many new opportunities to launder money.

DOJ's Framework on Cryptocurrency Enforcement

The DOJ's Cryptocurrency Enforcement Framework recognizes the positive potential for cryptocurrencies to "fundamentally transform how human beings interact and how we organize society." However, it also notes that cryptocurrencies play "a role in many of the most significant criminal and national security threats our nation faces."

The Framework contains three parts. Part I contains a brief summary of what cryptocurrency is, how it works, and how it can be used. Part II summarizes existing laws and regulations surrounding cryptocurrencies, and discusses some of the primary regulators in the cryptocurrency space: the Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) and Office of Foreign Assets Control (OFAC); the Office of the Comptroller of the Currency (OCC); the Securities and Exchange Commission (SEC); and the Commodity Futures Trading Commission (CFTC). Part III explores the challenges the government continues to face in investigating crimes that involve cryptocurrency, and the strategies that DOJ intends to pursue going forward, which primarily relate to increased coordination among federal, state and international law enforcement.

Recent DOJ Prosecutions Involving Cryptocurrencies

Two recent indictments highlight DOJ's increasing interest in prosecuting crimes involving cryptocurrencies. These cases involve defendants who allegedly used cryptocurrencies to (1) launder money for criminal syndicates, or (2) provide opportunities to launder money by intentionally refusing to implement anti-money laundering and know your customer controls.

The QQAAZZ Indictment

In *United States v. Nika Nazarovi et al.*, 2:20-cr-00295-MJH (W.D. Pa. 2020), the government charged fourteen Eastern European defendants with being part of a transnational organized crime network known as "QQAAZZ." The indictment alleges that QQAAZZ "provided money laundering services to significant cybercriminal organizations that stole money from unwitting victims in the United States and abroad." The defendants allegedly laundered the stolen funds both through a series of bank accounts, and in and out of digital currencies, to conceal the source of the funds. They allegedly collected fees as high as 50 percent from clients for their services.

The BitMEX Indictment

In *United States v. Arthur Hayes et al.*, 20 CR 500 (S.D.N.Y. 2020), the government charged four individuals with running an online trading platform called the Bitcoin Mercantile Exchange or BitMEX. According to the indictment, BitMEX solicited and accepted orders for trades in futures contracts and other derivatives tied to the value of cryptocurrencies, including Bitcoin. BitMEX allegedly served thousands of customers located in the United States.

The indictment claims that the defendants willfully failed to establish an adequate anti-money laundering program and

failed to engage in adequate customer identification (i.e. a Know Your Customer or KYC program), all in violation of the Bank Secrecy Act. The indictment also claims that the BitMEX exchange operated as an unregistered futures commission merchant in violation of applicable CFTC regulations. The indictment includes allegations that the "defendants … took affirmative steps purportedly designed to exempt BitMEX from the application of US laws like AML and KYC requirements. For example, the defendants caused the Company to formally incorporate in the Seychelles, a jurisdiction they believed had less stringent regulation, and from which they could still service US customers and operate within the United States without performing AML and KYC." The government also focused on the fact that defendants allegedly "caused BitMEX to reject adoption or implementation of formal policies, procedures, and internal controls for AML; independent compliance testing for AML; and training for appropriate personnel in AML."

These indictments make clear that the government will closely scrutinize those who provide opportunities to launder money through cryptocurrencies. They also make clear that DOJ is aggressively targeting individuals and companies - wherever located - that use cryptocurrencies to victimize US citizens.

The Bottom Line

The bottom-line takeaway from DOJ's Enforcement Framework and these recent indictments is that businesses which accept payment in cryptocurrencies, facilitate transactions in cryptocurrencies, or seek US customers in connection with businesses involving cryptocurrencies must be mindful of a host of state, federal and global-wide compliance obligations. For example, such businesses may require state money transmitter licenses, as well as registration and compliance with requirements promulgated by FinCEN, OFAC, the SEC and CFTC. Companies must also focus on applicable AML/KYC responsibilities. In addition, companies that transact in cryptocurrencies at the global level must be aware of the many registration and AML/KYC requirements that exist in any country in which they have customers or are marketing to customers, particularly since, as DOJ's alert makes clear, global regulators are increasingly reliant on one another to investigate and prosecute crimes involving cryptocurrencies.

Your Key Contacts

Adrian Stewart
Counsel, New York
D +1 212 768 6887
M +1 917 301 5322
adrian.stewart@dentons.com

Victor H. Boyajian
Global Chair, Venture Technology and Emerging Growth Companies,
New York
D +1 212 768 5349
M +1 650 815 5146
victor.boyajian@dentons.com