SULLIVAN & CROMWELL LLP

October 12, 2020

# Department of Justice Cryptocurrency Enforcement Framework

## DOJ Calls for Increased Interagency and International Cooperation in Enforcing Virtual Currency Regulations.

### SUMMARY

On October 8, 2020, the Attorney General's Cyber-Digital Task Force (the "Task Force") issued a "Cryptocurrency Enforcement Framework" report (the "Framework"), outlining the Department of Justice's position on cryptocurrency-related crimes and the role of regulators in enforcement against cryptocurrency-related businesses. While observing that cryptocurrency has "transformative potential," the Framework notes that cryptocurrency has played an outsized role in financial transactions associated with criminal activity, fraud, money laundering, tax evasion, and theft; that strong interagency and international partnerships have led to significant criminal and civil enforcement actions in the cryptocurrency space; and that the Department still faces cryptocurrency enforcement challenges, especially due to decentralized finance business models and anonymity-enhancing activities that may impede scrutiny. Throughout, the Framework emphasizes the need for cryptocurrency-related businesses to comply with applicable anti-money laundering ("AML") requirements and declares that the Department will assert jurisdiction broadly in order to reach those companies in the United States and in other countries and will coordinate with other federal and state agencies in the exercise of their regulatory authorities.

### BACKGROUND

Virtual currencies are digital representations of value. While certain countries are exploring the issuance of digital or virtual fiat currencies, the virtual currencies prominent today are not fiat currencies (*i.e.*, government-issued currencies not backed by gold or other commodities) and are not generally recognized as legal tender.[1] Cryptocurrencies are virtual currencies—common examples include Bitcoin and Ether—that rely on (i) decentralized, distributed ledgers or blockchains, and (ii) networks of users who verify the

validity of transactions on the blockchain.[2] Cryptocurrencies are generally stored in electronic "wallets," which interact with the relevant blockchain and require both a publicly available public key and a private key to hold and transact in the currency.[3] The Framework observes that while cryptocurrencies have many benefits, they also have facilitated myriad transnational crimes.[4]

In 2018, the Department established the Cyber-Digital Task Force to evaluate the role of law enforcement in light of the rapid development of new technologies. Later that year, the Task Force issued its first report, which identified, among other things, the potential threats posed by cryptocurrencies, including their use in cyber-attacks, drug and child sex trafficking, and foreign influence campaigns.[5] That report also recommended that the Department "continue evaluating the emerging threats posed by rapidly developing cryptocurrencies that malicious cyber actors often use."[6] The Framework results from the Department's continued evaluation of those threats.

## THE FRAMEWORK

On October 8, 2020, the Task Force issued the Framework based on the Department's and other agencies' recent investigations and prosecutions of cryptocurrency-related actors.[7] Although the Framework recognizes that distributed ledger technology and cryptocurrencies present numerous possibilities for the advancement of society, and acknowledges that various U.S. governmental agencies and institutions are exploring and supporting the development of this technology, the Framework emphasizes that cryptocurrencies play an ongoing role in serious criminal and national security threats. Described by Attorney General William Barr as a "first-of-its-kind framework" that lays out "federal enforcement priorities," the Framework proceeds in three parts.[8] Part I details the Department's findings on cryptocurrency-related crimes. Part II outlines the applicable laws and regulations. And Part III summarizes the ongoing challenges faced by the Department in the virtual currency space.[9] Following its three-part analysis, the Framework concludes that the Department will continue ensuring that "uses of cryptocurrency adhere to the law" and continue "strengthening its key partnerships" with other agencies, state authorities, and international partners.[10]

***Cryptocurrency-Related Crimes***. Part I of the Framework identifies three major areas of cryptocurrency-related crime: (1) use of cryptocurrency to commit crimes or support terrorism; (2) use of cryptocurrency to obscure financial activity; and (3) commission of crimes within cryptocurrency markets themselves.[11]

With respect to the first category, the Framework notes that criminals and terrorists may use cryptocurrencies to avoid large cash transactions and traditional bank accounts that trigger bank reporting requirements.[12] The activities in the first category include buying and selling illegal goods (*e.g.*, drugs, firearms, and terrorism-supporting tools); extortion, such as demanding cryptocurrencies as payment in ransom and blackmail schemes; and raising funds directly for criminal and terrorist activities.[13]

As to the second category, the Framework details a number of activities that facilitate the evasion of regulatory requirements, thereby promoting the financing of illicit conduct and concealing its proceeds.[14] The Framework notes that criminals increasingly are laundering the proceeds of criminal activity by taking advantage of the "explosion of online marketplaces and exchanges that use cryptocurrency."[15] The Framework emphasizes that unlicensed or unregistered virtual currency exchanges—defined as individuals or entities engaged in the business of exchanging virtual currency for fiat currency, other forms of virtual currency, or other types of assets—can "provide an avenue of laundering for those who use digital currency for illicit purposes," as can any such exchange that fails to comply with AML standards and know-your-customer procedures.[16] Other evasive activities identified in the Framework include tax evasion—usually by failing to report capital gains from cryptocurrency transactions—and evasion of economic sanctions by using decentralized exchanges to sponsor sanctioned individuals and countries.[17]

In the final category, the Framework notes that to steal cryptocurrencies, criminals have hacked individual wallets, exchanges, and even the computers that "mine" for cryptocurrency on the blockchain (a practice known as "cryptojacking").[18] The Framework further notes that fraudsters operating exchanges have bilked investors out of funds by misappropriating their cryptocurrencies.[19]

***Applicable Laws and Regulations***. Part II of the Framework lists the available legal tools used by federal, state, and international regulators in enforcement actions concerning cryptocurrency-related crimes. The voluminous list spans seven federal agencies, various state regulators, and international regimes. Highlighting significant enforcement successes from the last two years, the Framework emphasizes that interagency partnership, as well as collaboration with international regulatory and criminal enforcement authorities, have been and will continue to be critical for the effective leveraging of these legal tools.

- **Department of Justice**: The Department has a "wide variety of federal charges" at its disposal, including no less than 14 potential charges for cryptocurrency-related crimes: (1) wire fraud; (2) mail fraud; (3) securities fraud; (4) access device fraud; (5) identity theft and fraud; (6) fraud and intrusions in connection with computers; (7) illegal sale and possession of firearms; (8) possession and distribution of counterfeit items; (9) child exploitation activities; (10) possession and distribution of controlled substances; (11) money laundering; (12) transactions involving proceeds of illegal activity; (13) operation of an unlicensed money transmitting business; and (14) failure to comply with Bank Secrecy Act ("BSA") requirements.[20] In addition, the Department "frequently" uses criminal and civil asset forfeiture laws to seize assets in connection with illicit activity.[21]
- **Financial Crimes Enforcement Network ("FinCEN")**: The Framework summarizes final rules and guidance issued by FinCEN that broadly identified virtual currency exchangers (including entities "engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency"),[22] and administrators as money services businesses ("MSBs").[23] Entities classified as MSBs must comply with the BSA, including by having adequate AML programs and filing suspicious activity reports.[24] Significantly, the Framework clarified that, for MSBs doing business in the United States, "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."[25]
- **Office of Foreign Assets Control ("OFAC")**: The Framework notes that U.S. persons and others subject to OFAC jurisdiction cannot transact in virtual currencies with OFAC-sanctioned persons and countries or otherwise engage in OFAC-sanctioned activities.[26] It further warns that persons

who violate or seek to evade OFAC requirements by transacting in virtual currencies could be criminally and civilly liable under the International Emergency Economic Powers Act, the Trading with the Enemies Act, and other statutes.[27]

- **Office of the Comptroller of the Currency ("OCC")**: The Framework reiterates recent guidance from the OCC that "holding the unique cryptographic keys associated with cryptocurrency" is considered a traditional banking activity that must comply with applicable laws.[28]
- **Securities & Exchange Commission ("SEC")**: The Framework notes that the SEC has been active in regulating and litigating claims related to initial coin offerings ("ICOs") and reviews the SEC's recent framework for when virtual currencies qualify as securities under the securities laws.[29]
- **Commodity Futures Trading Commission ("CFTC")**: The Framework explains that the CFTC has jurisdiction when a virtual currency is the underlying asset in a derivatives contract or when fraud or manipulation occurs in connection with virtual currencies traded in interstate commerce.[30] The Framework further notes that the CFTC has been heavily involved in litigating against and regulating cryptocurrency-related entities.[31]
- **Internal Revenue Service ("IRS")**: The Framework summarizes recent IRS guidance on cryptocurrencies, including that capital gains from cryptocurrency transactions are taxable income.[32]
- **State Authorities**: The Framework underscores the role that state attorneys general, securities regulators, and departments of financial services play in protecting the public and notes that state authorities are actively investigating virtual currency activities, "particularly those involving the issuance or sale of ICOs and other investment products."[33]
- **Financial Action Task Force ("FATF")**: At the international level, the Framework notes that "Recommendation 15" of FATF standards provides that countries should regulate virtual asset service providers for proper AML procedures and terrorist financing risks.[34]

***Ongoing Challenges***. Part III of the Framework concludes by analyzing two major challenges for the Department in enforcement against cryptocurrency businesses: decentralized business models that may facilitate criminal activity, and anonymity-enhancing activities.[35] The Framework notes that entities operating cryptocurrency exchanges (defined as exchanges that allow users to buy and sell cryptocurrencies or convert cryptocurrency to other virtual currencies or fiat currency), peer-to-peer ("P2P") exchanges, cryptocurrency kiosks, and virtual currency casinos must follow applicable FinCEN regulations.[36] Specifically, the Framework warns that foreign-located cryptocurrency exchanges that serve U.S. customers must register with FinCEN; and that P2P exchanges, cryptocurrency kiosks, and unlicensed casinos are MSBs and thus subject to FinCEN reporting requirements.[37]

Moreover, the Framework cautioned that certain cryptocurrencies—such as Monero, Dash, and Zcash—are "anonymity enhanced" and that their use is considered "a high-risk activity that is indicative of possible criminal conduct" because of the difficulty of applying AML controls to users of these cryptocurrencies.[38] Similarly, the Framework identifies "mixers" and "tumblers"—which obscure the source or owner of cryptocurrencies, typically by processing those cryptocurrencies through a series of transactions designed to complicate their digital history—as entities that the Department considers to be specifically designed to disguise material information about financial transactions.[39] Finally, the Framework notes that some virtual asset service providers operate in jurisdictions with a "complete absence" of AML regulation, allowing for gaps in criminal enforcement.[40]

## IMPLICATIONS

The Framework affirms that the "aggressive" investigation and prosecution of cryptocurrency-related crimes will remain a Department priority. Indeed, the Framework discusses the multitude of legal tools the Department has used—and will continue using—to investigate and bring to justice cryptocurrency-related businesses who the Department believes have violated the law. The Framework indicates that the Department may play a significant role in coordinating regulatory investigations by the Department of the Treasury (including FinCEN, OFAC, and the IRS), SEC, and CFTC and highlights that the Department can "maximize its impact" by "appropriately coordinating parallel enforcement actions."[41] Similarly, the Framework recommends increased cooperation with state authorities.[42]

The Framework also suggests an expansion in the Department's enforcement priorities, especially with respect to foreign virtual asset service providers that service U.S. customers. The Framework asserts that the Department has "robust authority" to prosecute foreign providers so long as "virtual asset transactions touch financial, data storage, or other computer systems within the United States."[43] In addition, the Framework suggests that the Department is interested in—and may take aim at—business models using decentralized finance, P2P exchanges, and anonymity-enhancing cryptocurrencies that do not comply with applicable AML regulations.[44]

Finally, the Framework reasserts that the United States is committed to harmonizing AML regulations internationally and closing gaps in regulation across the globe. Notably, the Framework notes that the Department "will continue to encourage these partnerships in support of multi-jurisdictional parallel investigations and prosecutions" and will "work internationally to level the legal and regulatory playing field related to virtual assets."[45] As just one example, the Framework specifically notes that, contrary to the position taken by some virtual currency exchanges, the Department does not believe that the EU General Data Protection Regulation ("GDPR") shields disclosure by companies subject to U.S. jurisdiction of information requested by criminal grand jury subpoenas because of relevant exceptions and derogations provided for by the GDPR.[46]

* * *

## ENDNOTES

[1] U.S. DEP'T OF JUSTICE, REPORT OF THE ATTORNEY GENERAL'S CYBER-DIGITAL TASK FORCE 2-3 (Oct. 2020) [hereinafter FRAMEWORK], https://www.justice.gov/ag/page/file/1326061/download.

[2] *Id.* at 3-4.

[3] *Id.*

[4] *Id.* at 5-6.

[5] *See generally* U.S. DEP'T OF JUSTICE, REPORT OF THE ATTORNEY GENERAL'S CYBER-DIGITAL TASK FORCE (July 2018), https://www.justice.gov/ag/page/file/1076696/download.

[6] *Id.* at 126.

[7] Under Executive Order 13891, the Department issued the Framework as a guidance document, meaning the Framework is not legally binding and does not have the force and effect of law.

[8] Press Release, U.S. Dep't of Justice, Attorney General William P. Barr Announces Publication of Cryptocurrency Enforcement Framework (Oct. 8, 2020).

[9] FRAMEWORK, at viii-ix.

[10] *Id.* at 52.

[11] *Id.* at 6-16.

[12] *Id.* at 6.

[13] *Id.* at 6-7.

[14] *Id.* at 13.

[15] *Id.*

[16] *Id.* at 13-14. The Framework acknowledges that "the requirements for exchanges to register, obtain licenses, and collect information about customers and their transactions are not consistent across international jurisdictions," which "can create challenges for international law enforcement and regulatory agencies operating in this space." *Id*. at 14.

[17] *Id.* at 14-15.

[18] *Id.* at 15-16.

[19] *Id.* at 15-16 (citing Press Release, U.S. Dep't of Justice, Operating of Bitcoin Investment Platform Pleads Guilty to Securities Fraud and Obstruction of Justice (July 23, 2018); Press Release, U.S. Dep't of Justice, Trader Sentenced to 15 Months in Federal Prison for Misappropriating $1.1 Million in Cryptocurrencies (Nov. 13, 2018)).

[20] *Id.* at 20-21.

[21] *See* 18 U.S.C. §§ 981-82; 21 U.S.C. § 853.

[22] U.S. DEP'T OF THE TREASURY, FIN. CRIMES ENF'T NETWORK, FIN-2013-G0001, APPLICATION OF FINCEN'S REGULATIONS TO PERSONS ADMINISTERING, EXCHANGING, OR USING VIRTUAL CURRENCIES 2 (Mar. 18, 2013), https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf.

[23] FRAMEWORK, at 23-24.

[24] *See generally* 31 C.F.R. pt. 1022.

[25] FRAMEWORK, at 25 ("The MSB need only do business in whole or substantial part in the United States.").

[26] *Id.* at 26.

[27] *Id.*

## ENDNOTES (CONTINUED)

28 *Id.* at 29 (quoting Off. of the Comptroller of the Currency, Interpretative Letter #1170 on Authority of a National Bank to Provide Cryptocurrency Custody Services for Customers (July 22, 2020)).

29 *Id.* at 29-31 (citing U.S. SEC. & EXCH. COMM'N, FRAMEWORK FOR "INVESTMENT CONTRACT" ANALYSIS OF DIGITAL ASSETS (Apr. 3, 2019)).

30 *Id.* at 32.

31 *Id.* at 32-33 & nn.127-34 (listing cases).

32 *Id.* at 33-34 (citing I.R.S. Notice 2014-21, 2014-16 I.R.B. 938 (2014)).

33 *Id.* at 34.

34 *Id.* at 35-36 (citing FIN. ACTION TASK FORCE, THE FATF RECOMMENDATIONS: INTERNATIONAL STANDARDS ON COMBATING MONEY LAUNDERING AND THE FINANCING OF TERRORISM & PROLIFERATION 15, 69-70 (June 2019)).

35 *Id.* at 37-44.

36 *Id.* at 37-41.

37 *Id.*

38 *Id.* at 41.

39 *Id.* at 41-44.

40 *Id.* at 44. The Framework further notes that the Department may assert the principle of protective jurisdiction, whereby the Department could assert jurisdiction "anywhere in the world" for activity amounting to supporting terrorism. *Id.* at 45.

41 *Id.* at 45.

42 *Id.* at 49.

43 *Id.* at 45.

44 *See id.* at ix ("Finally, decentralized platforms, peer-to-peer exchangers, and anonymity-enhanced cryptocurrencies that use non-public or private blockchains all can further obscure financial transactions from legitimate scrutiny.").

45 *Id.* at 49, 51.

46 *Id.* at 50.

## ABOUT SULLIVAN & CROMWELL LLP

Sullivan & Cromwell LLP is a global law firm that advises on major domestic and cross-border M&A, finance, corporate and real estate transactions, significant litigation and corporate investigations, and complex restructuring, regulatory, tax and estate planning matters. Founded in 1879, Sullivan & Cromwell LLP has more than 875 lawyers on four continents, with four offices in the United States, including its headquarters in New York, four offices in Europe, two in Australia and three in Asia.

## CONTACTING SULLIVAN & CROMWELL LLP

This publication is provided by Sullivan & Cromwell LLP as a service to clients and colleagues. The information contained in this publication should not be construed as legal advice. Questions regarding the matters discussed in this publication may be directed to any of our lawyers listed below, or to any other Sullivan & Cromwell LLP lawyer with whom you have consulted in the past on similar matters. If you have not received this publication directly from us, you may obtain a copy of any past or future publications by sending an e-mail to SCPublications@sullcrom.com.

## CONTACTS


**New York**

| | | |
|---|---|---|
| Nicolas Bourtin | +1-212-558-3920 | bourtinn@sullcrom.com |
| David H. Braff | +1-212-558-4705 | braffd@sullcrom.com |
| Robert E. Buckholz | +1-212-558-3876 | buckholzr@sullcrom.com |
| Justin J. DeCamp | +1-212-558-1688 | decampj@sullcrom.com |
| Theodore Edelman | +1-212-558-3436 | edelmant@sullcrom.com |
| Stephen Ehrenberg | +1-212-558-3269 | ehrenbergs@sullcrom.com |
| Mitchell S. Eitel | +1-212-558-4960 | eitelm@sullcrom.com |
| Jared M. Fishman | +1-212-558-1689 | fishmanj@sullcrom.com |
| Nicole Friedlander | +1-212-558-4332 | friedlandern@sullcrom.com |
| C. Andrew Gerlach | +1-212-558-4789 | gerlacha@sullcrom.com |
| Robert J. Giuffra Jr. | +1-212-558-3121 | giuffrar@sullcrom.com |
| Richard H. Klapper | +1-212-558-3555 | klapperr@sullcrom.com |
| Sharon Cohen Levin | +1-212-558-4334 | levinsc@sullcrom.com |
| Ryne V. Miller | +1-212-558-3268 | millerry@sullcrom.com |
| Sharon L. Nelles | +1-212-558-4976 | nelless@sullcrom.com |
| Ann-Elizabeth Ostrager | +1-212-558-7357 | ostragerae@sullcrom.com |
| Samuel W. Seymour | +1-212-558-3156 | seymours@sullcrom.com |
| Rebecca J. Simmons | +1-212-558-3175 | simmonsr@sullcrom.com |
| Stephanie G. Wheeler | +1-212-558-7384 | wheelers@sullcrom.com |
| Alexander J. Willscher | +1-212-558-4104 | willschera@sullcrom.com |

| | | |
|---|---|---|
| **Washington, D.C.** | | |
| Judson O. Littleton | +1-202-956-7085 | littletonj@sullcrom.com |
| Kathleen S. McArthur | +1-202-956-7591 | mcarthurk@sullcrom.com |
| Aisling O'Shea | +1-202-956-7595 | osheaa@sullcrom.com |
| Kamil R. Shields | +1-202-956-7040 | shieldska@sullcrom.com |
| Christopher Michael Viapiano | +1-202-956-6985 | viapianoc@sullcrom.com |
| **Los Angeles** | | |
| Anthony J. Lewis | +1-310-712-6615 | lewisan@sullcrom.com |
| Adam S. Paris | +1-310-712-6663 | parisa@sullcrom.com |
| Robert A. Sacks | +1-310-712-6640 | sacksr@sullcrom.com |
| **Palo Alto** | | |
| Brendan P. Cullen | +1-650-461-5650 | cullenb@sullcrom.com |
| Laura Kabler Oswell | +1-650-461-5679 | oswelll@sullcrom.com |
| **London** | | |
| Theodore Edelman | +44 20 7959 8450 | edelmant@sullcrom.com |