King & Spalding

Financial Services

Providing Strategic Legal Guidance to the Global Financial Services Industry

NOVEMBER 13, 2020

For more information, contact:

Ehren Halse
+1 415 318 1216
ehalse@kslaw.com

Russell Johnston
+1 212 827 4081
rjohnston@kslaw.com

Brian Michael
+1 213 443 4317
bmichael@kslaw.com

Shas Das
+1 202 626 9258
sdas@kslaw.com

Matthew Hanson
+1 202 626 2904
mhanson@kslaw.com

Seth Atkisson
+1 202 626 9257
satkisson@kslaw.com

Christina Kung
+1 202 626 9125
ckung@kslaw.com

King & Spalding

Washington, D.C.
1700 Pennsylvania Avenue, NW
Washington, D.C. 20006-4707
Tel: +1 202 737 0500

San Francisco
101 Second Street
Suite 1000
San Francisco, CA 94105
Tel: +1 415 318 1200

Patchwork of Cryptocurrency Regulators Increasingly Stitch Together Cooperative Enforcement Efforts

Recent Enforcement Actions and Guidance from DOJ, FinCEN, and OFAC Demonstrate the Increased Commitment — and Cooperation — of Federal Regulators to Police Digital Currencies, Including Their Use in Ransomware Attacks

Amid the persistent growth in buying, selling, and issuance of digital assets,[1] federal criminal and civil enforcement authorities are becoming more vigilant in their oversight of these growing markets. Often, they are teaming up on cases where their jurisdiction overlaps, especially when criminal conduct is involved.

In a recent reminder of government authorities' continued interest in policing digital currencies, on November 5, 2020, the Department of Justice ("DOJ") filed a civil forfeiture complaint seizing thousands of Bitcoins — valued at more than $1 billion — related to the successful prosecution of the founder of Silk Road, an online criminal marketplace that at one point was used extensively by drug dealers and other illicit traders.[2] The case represents the largest seizure of cryptocurrency in DOJ history.[3]

The forfeiture action also follows recently announced guidance from DOJ, the Financial Crimes Enforcement Network ("FinCEN"), and Treasury's Office of Foreign Assets Control ("OFAC"), as well as other enforcement actions, in which regulators have warned the public of the legal and regulatory risks involved in digital asset businesses. Taken together, these developments underscore the increasing focus by federal regulators on cooperatively policing and enforcing illicit cryptocurrency and digital asset transactions.

DOJ: "CRYPTOCURRENCY: AN ENFORCEMENT FRAMEWORK"

One of the most recent comprehensive sources of U.S. cryptocurrency guidance came from DOJ's Cyber-Digital Task Force. Published on October 8, 2020, the 83-page "Cryptocurrency: An Enforcement Framework" report ("Framework") provides a comprehensive overview of the public safety and national security challenges posed by cryptocurrency technology: Part I describes various illegal uses of cryptocurrency; Part II details the legal and regulatory tools available to combat those criminal and national security threats; and, finally, Part III discusses the government's ongoing challenges involving money services businesses ("MSBs"), virtual asset service providers ("VASPs"), and cryptocurrency in general.[4]

Illegal Uses of Cryptocurrency

DOJ identifies three broad categories of criminality growing alongside the rise of digital currencies: (1) using cryptocurrency to directly commit crimes or support terrorism, such as for the purchase and sale of illegal items or for criminal and terrorist activity fundraising; (2) using cryptocurrency to hide financial activity, such as for money laundering, tax evasion, or to avoid economic sanctions; and (3) committing crimes within the cryptocurrency marketplace itself, such as by using malware to hack into another's computer to generate or "mine" cryptocurrency.[5] The Framework highlights a variety of digital currency cases where DOJ has been active in combatting malfeasance, including narcotics trafficking, arms sales, distribution of child abuse material, financial support of terrorist activities, and blackmail schemes.

Business Models of Interest

The Framework calls out MSBs[6] and VASPs[7] as the most common cryptocurrency targets of DOJ and its key regulatory partners. MSBs and VASPs are both pivotal to the functioning of the cryptocurrency ecosystem, and this key position brings with it a heightened responsibility for these businesses to be alert for illicit activity in their dealings and to safeguard customer data. DOJ's Framework highlights business models and activities that may facilitate criminal activity. In particular, it calls out cryptocurrency exchanges, peer-to-peer ("P2P") exchangers and platforms, cryptocurrency kiosks, virtual currency casinos, anonymity enhanced cryptocurrencies, and mixers, tumblers, and chain hopping.[8] Businesses operating with these models or undertaking these activities can expect DOJ and federal regulators to scrutinize their actions closely.

DOJ is particularly concerned about VASPs not being compliant with the AML/CFT standards required of MSBs by the Bank Secrecy Act ("BSA").[9] The Framework notes, for example, the practice of some VASPs applying different standards to U.S. customers, versus customers in other countries. Another example is VASPs applying different standards to virtual-asset-to-fiat transactions than to virtual-asset-to-virtual-asset transactions. The Framework calls out both of these examples as "flatly inconsistent" with BSA requirements (noting FinCEN's primary responsibility for administering and enforcing the BSA).[10] The Framework also flags as violations: failing to register with FinCEN as an MSB, failing to collect required customer and transaction information, and failing to file suspicious activity reports ("SARs").[11] This warning was recently reinforced by FinCEN's first civil money penalty action against a mixer/tumbler operator for failing to register as an MSB, failure to adopt an AML program, and failure to file SARs.[12]

Overlap and Coordination with Fellow Regulators

True to the patchwork of U.S. regulators with jurisdiction over aspects of digital assets, the Framework describes DOJ's coordination and interaction with seven government agencies.

1. **FinCEN** – FinCEN regulates individuals and entities engaged in the business of accepting and transmitting convertible virtual currency, which includes virtual currency administrators and exchangers, along with foreign-located MSBs. These participants and businesses must meet the same AML/CFT requirements under the Bank Secrecy Act as other more traditional MSBs. In addition to receiving and maintaining all SAR filings, FinCEN can take regulatory action against violators or use its civil enforcement authority to impose monetary penalties as an alternative or supplement to criminal prosecution. The Framework highlights FinCEN's work to prevent crime and to assist in DOJ investigations.
2. **OFAC** – The Framework explains that OFAC's administration and strict liability enforcement of economic and trade sanctions may also apply to participants in virtual currency transactions. Individuals and entities transacting in digital currencies must ensure that they are not engaging in prohibited transactions. The Framework provides several examples of instances of coordinated action between OFAC and DOJ, in which OFAC announced sanctions and DOJ brought criminal charges.
3. **Office of the Comptroller of the Currency ("OCC")** – The Framework reiterates the requirement that national banks and federal savings associations providing cryptocurrency custody services to their customers must effectively manage risks and comply with applicable law. This includes the establishment of an adequate AML program and implementation of appropriate risk controls.
4. **Securities and Exchange Commission ("SEC")** – The Framework highlights the SEC's focus on fraud related to cryptocurrency and "initial coin offerings" ("ICOs") as a regulatory and enforcement priority. The SEC has devoted significant resources to this area, in issuing an investigative report warning the public and investors of potential ICO-related scams, filing dozens of civil enforcement actions, and working closely with DOJ in criminal cases involving ICO offering frauds.
5. **Commodity Futures Trading Commission ("CFTC")** – The CFTC has statutory authority in the cryptocurrency space when a virtual currency is the underlying asset in a derivatives contract or when virtual currency is traded in interstate commerce and involves fraud or manipulation. Like the SEC, the CFTC collaborates with DOJ in cases where criminal fraud charges might be appropriate.
6. **Internal Revenue Service ("IRS")** – The Framework explains that general tax principles apply to virtual currency transactions just as they would for property transactions. The Framework directs readers to several FAQs from the IRS addressing relevant tax implications.
7. **State Authorities** – The Framework also points to state authorities (e.g., state attorneys generals, securities regulators, departments of financial services) as active monitors and enforcers within the virtual currency space, particularly with regard to ICOs and other cryptocurrency-related investment products.

Looking Forward

The Framework concludes by noting DOJ's continued commitment to "aggressive investigation and prosecution" that uses "an appropriate all-tools approach to dealing with cryptocurrency-related crime." In particular, the Framework reiterates that DOJ has already prosecuted P2P exchanges for money laundering and BSA violations and emphasizes DOJ's "robust authority" to prosecute foreign-located entities and individuals that violate U.S. law. For example, the Framework highlights DOJ's numerous recent enforcement efforts, including a civil forfeiture action against 303 virtual currency accounts,[13] an investigation into three terrorist financing cyber-enabled campaigns,[14] and a "coordinated international effort to disrupt opioid trafficking on the dark web."[15] DOJ also commits in the Framework to continued coordination with law enforcement, state authorities, and international partners, along with direct outreach and education of private companies operating within cryptocurrency and digital asset markets.[16] As

an example consistent with these principles, the DOJ Bitcoin seizure in the Silk Road matter was the result of a joint investigation with the IRS.

DOJ AND CFTC: REGULATOR COOPERATION ON BITMEX CASE

DOJ's case against BitMEX, filed in October, also serves to reinforce the focus and cooperation of federal law enforcement and regulatory authorities on conduct by cryptocurrency businesses, including offshore cryptocurrency exchanges.

On October 1, 2020, DOJ indicted four BitMEX founders and executives, alleging they knowingly evaded and conspired to evade the AML regulations of the BSA.[17] One of the founders who serves as BitMEX's chief technology officer was arrested in Massachusetts, while the other defendants remained at large.[18] That same day, the CFTC filed a civil enforcement action against five entities and three individuals that own and operate the BitMEX platform, charging the individuals and entities with operating an unregistered trading platform and violating multiple CFTC regulations, including failing to implement required AML procedures.[19, 20]

According to the indictment, "BitMEX made itself available as a vehicle for money laundering and sanctions violations."[21] BitMEX allegedly operated with few restrictions when it came to AML and sanctions — until very recently, not even basic identity checks were required of BitMEX customers.[22] (BitMEX reportedly hired a new Chief Compliance Officer in the days following the DOJ and CFTC charges.[23])

BitMEX's alleged flouting of basic AML and sanctions requirements and disregard for regulatory requirements brought the attention of the authorities and resulted in DOJ's indictment and the CFTC's civil suit. The chief executive officer of Binance, a cryptocurrency exchange operator, referred to the actions as a "wake-up call" to the rest of the industry that served to warn industry players to be more cautious and fully compliant.[24]

FINCEN AND OFAC: THE RANSOMWARE ADVISORIES

Among its other points of focus, DOJ's Framework also discusses a number of enforcement actions involving ransomware. Those comments should be viewed in the context of two more-targeted advisories issued by FinCEN and OFAC only a week prior. On October 1, 2020, these two divisions of the Department of the Treasury issued advisories specifically on the threat of ransomware. FinCEN published its "Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments" ("FinCEN Ransomware Advisory"),[25] and OFAC offered its "Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments" ("OFAC Ransomware Advisory").[26] Together, the FinCEN Ransomware Advisory and the OFAC Ransomware Advisory (jointly, the "Advisories") shed light on a criminal act that, in the eyes of these enforcement agencies, has been greatly facilitated by cryptocurrencies — the capture and/or locking of digital information for ransom.

The FinCEN Ransomware Advisory notes that cryptocurrency is the preferred payment method of ransomware perpetrators.[27] These attacks have become "more focused, sophisticated, costly, and numerous" in recent years; businesses of all sizes, local government agencies, hospitals, and school districts are susceptible to the threat of a ransomware cyberattack.[28] FinCEN also warns digital forensics and incident response companies and cyber insurance companies that in certain situations their activities in assisting an entity subject to a ransomware attack may require them to register as an MSB and subject them to the requirements of the BSA, including filing SARs.[29] In particular, directly receiving customers' funds, exchanging them for cryptocurrency, and then transferring the digital currency to criminal-controlled accounts is flagged as a service that may require digital forensics and incident response companies and cyber insurance companies to register as MSBs.[30]

The OFAC Ransomware Advisory flags that OFAC has designated numerous malicious cyber actors as Specially Designated Nationals and Blocked Persons ("SDNs").[31] The involvement of an SDN in a ransomware attack may make the payment of the ransom a violation of U.S. law, a fact that OFAC notes in the OFAC Ransomware Advisory.[32] Furthermore, OFAC reviews license applications involving ransomware on a case-by-case basis with a presumption of denial.[33] Entities subject to a ransomware attack must be aware of the possibility that the attack is associated with an SDN and that payment of the ransom may be in violation of U.S. laws. OFAC notes that qualified outside counsel could be helpful in navigating such complicated situations.

In light of the Advisories, expect criminal and civil regulatory enforcement agencies, including DOJ, FinCEN, and OFAC, to take action against any cryptocurrency-related business that enables or facilitates a ransomware attack.

CONCLUSION

Recent publications and enforcement actions show the intent of multiple federal regulators to hold cryptocurrency transactions and participants to existing legal standards, as well as to prevent clear fraud. As digital currency transactions increase, federal law enforcement and regulators will only become more involved and cooperate more extensively in the regulation and oversight of this space. And just because violative conduct goes uninvestigated for a period of time, that does not mean federal authorities will not notice the conduct eventually, and may come knocking. As federal law enforcement and regulatory authorities ramp up enforcement actions, businesses — particularly those issuing, selling, or providing a platform for the issuance or sale of digital currencies — are wise to consider how recent guidance and enforcement actions should inform changes and improvements to their own platforms and operations. As federal regulators continue to flex their intertwined enforcement muscle in this area, investment in "an ounce of prevention" to ensure regulatory and legal compliance will certainly be "worth a pound of cure."

ABOUT KING & SPALDING

Celebrating more than 130 years of service, King & Spalding is an international law firm that represents a broad array of clients, including half of the Fortune Global 100, with 1,200 lawyers in 22 offices in the United States, Europe, the Middle East and Asia. The firm has handled matters in over 160 countries on six continents and is consistently recognized for the results it obtains, uncompromising commitment to quality, and dedication to understanding the business and culture of its clients.

ABU DHABI	CHARLOTTE	GENEVA	MOSCOW	RIYADH	TOKYO
ATLANTA	CHICAGO	HOUSTON	NEW YORK	SAN FRANCISCO	WASHINGTON, D.C.
AUSTIN	DUBAI	LONDON	NORTHERN VIRGINIA	SILICON VALLEY	
BRUSSELS	FRANKFURT	LOS ANGELES	PARIS	SINGAPORE	

[1] *See e.g.*, Anna Irrera & Tom Wilson, *Paypal to Open Up Network to Cryptocurrencies*, REUTERS (Oct. 21, 2020), https://www.reuters.com/article/us-paypal-cryptocurrency/paypal-to-open-up-network-to-cryptocurrencies-idUSKBN2761L6; Penny Crosman, *JPMorgan Chase reorganizes blockchain units*, AMERICAN BANKER (Oct. 28, 2020), https://www.americanbanker.com/news/jpmorgan-chase-reorganizes-blockchain-units.
[2] Press Release, Dep't of Justice, United States Files A Civil Action To Forfeit Cryptocurrency Valued At Over One Billion U.S. Dollars (Nov. 5, 2020), https://www.justice.gov/usao-ndca/pr/united-states-files-civil-action-forfeit-cryptocurrency-valued-over-one-billion-us.
[3] *Id.*
[4] ATTORNEY GENERAL'S CYBER-DIGITAL TASK FORCE, DEP'T OF JUSTICE, CRYPTOCURRENCY: ENFORCEMENT FRAMEWORK (Oct. 2020), https://www.justice.gov/ag/page/file/1326061/download [hereinafter FRAMEWORK].
[5] FRAMEWORK, *supra* note 4, at 6–16.
[6] MSBs are statutorily defined as individuals or entities engaged in one or more of the following activities: (1) currency dealer or exchanger; (2) check casher; (3) issuer of traveler's checks, money orders, or stored value; (4) seller or redeemer of traveler's checks, money orders, or stored value; (5) money transmitter; or (6) the U.S. Postal Service. 31 C.F.R. § 1010.100(ff). The Framework notes that "[i]n the United States, individuals and entities that offer money transmitting services involving virtual assets, such as cryptocurrency exchanges and kiosks, as well as certain issuers, exchangers, and brokers of virtual assets, are considered MSBs. Like brick-and-mortar financial institutions, MSBs are subject to AML/CFT regulations as well as certain licensing and registration requirements." FRAMEWORK, *supra* note 4, at 22.
[7] While VASPs are not an independent legal category of business in the United States, certain international frameworks identify them and prescribe particular legal treatment. For example, the Financial Action Task Force ("FATF") — the global standard-setter for anti-money laundering ("AML") and combatting the financing of terrorism ("CFT") standards, of which the United States is a founding member and participant — identifies VASPs as individuals or entities operating as a business to conduct one or more of the following activities for or on behalf of another entity or individual: (1) exchanges between virtual assets and fiat currency; (2) exchanges between one or more forms of virtual assets; (3) transfers of virtual assets; (4) safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; or (5) participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset. *The FATF Recommendations: International Standards on Combatting Money Laundering and the Financing of Terrorism & Proliferation*, FATF 130 (June 2019), http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf.
[8] FRAMEWORK, *supra* note 4, at 37–44.
[9] FRAMEWORK, *supra* note 4, at 44.
[10] FRAMEWORK, *supra* note 4, at 23, 44.
[11] FRAMEWORK, *supra* note 4, at 38–41.
[12] *First Bitcoin "Mixer" Penalized by FinCEN For Violating Anti-Money Laundering Laws*, FINCEN (Oct. 19, 2020), https://www.fincen.gov/news/news-releases/first-bitcoin-mixer-penalized-fincen-violating-anti-money-laundering-laws.
[13] FRAMEWORK, *supra* note 4, at 10.
[14] FRAMEWORK, *supra* note 4, at 11.
[15] FRAMEWORK, *supra* note 4, at 17.
[16] FRAMEWORK, *supra* note 4, at 44–52.
[17] DOJ has broad authority to investigate and bring charges against criminal activity involving cryptocurrency. As discussed in the Framework, DOJ has a wide variety of federal statutes at its disposal, including charges for (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 BSA requirements. FRAMEWORK, *supra* note 4, at 20–21. The Department can also use criminal and civil forfeiture statutes to seize the cryptocurrency or other property connected to the illegal activity. FRAMEWORK, *supra* note 4, at 21–22.

[18] Jonathan Stempel, *U.S. Charges BitMEX Cryptocurrency Founders with Failing to Prevent Money Laundering*, REUTERS (Oct. 1, 2020), https://www.reuters.com/article/us-usa-crime-bitmex-idUSKBN26M6SE.

[19] *CFTC Charges BitMEX Owners with Illegally Operating a Cryptocurrency Derivatives Trading Platform and Anti-Money Laundering Violations*, CFTC (Oct. 1, 2020), https://www.cftc.gov/PressRoom/PressReleases/8270-20.

[20] The CFTC has jurisdiction under the Commodity Exchange Act ("CEA") over "transactions involving swaps or contracts of sale of a commodity for future delivery," 7 U.S.C. § 2(a)(1)(A), with certain virtual currencies considered a "commodity." *See* FRAMEWORK, *supra* note 4, at 67 n.124.

[21] Nathaniel Popper, *Owners of BitMEX, a Leading Bitcoin Exchange, Face Criminal Charges*, THE NEW YORK TIMES (Oct. 1, 2020), https://www.nytimes.com/2020/10/01/technology/bitmex-bitcoin-criminal-charges.html.

[22] *Id*.

[23] Daniel Palmer, *BitMEX Exchange Hires First Compliance Chief After US Charges*, COINDESK (Oct. 12, 2020), https://www.coindesk.com/bitmex-exchange-hires-compliance-chief-after-us-charges.

[24] Robert Hackett, *Binance CEO: BitMex Indictment Is 'Wake-up Call' for Cryptocurrency Industry*, FORTUNE (Oct. 21, 2020), https://fortune.com/2020/10/21/binance-bitmex-indictment-cryptocurrency-industry/.

[25] *Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments*, FINCEN (Oct. 2020), https://www.fincen.gov/sites/default/files/advisory/2020-10-01/Advisory%20Ransomware%20FINAL%20508.pdf [hereinafter *FinCEN Ransomware Advisory*].

[26] *Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments*, OFAC (Oct. 2020), https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf [hereinafter *OFAC Ransomware Advisory*].

[27] *FinCEN Ransomware Advisory*, *supra* note 25, at 2.

[28] *OFAC Ransomware Advisory*, *supra* note 26, at 1–2.

[29] *FinCEN Ransomware Advisory*, *supra* note 25, at 3.

[30] *FinCEN Ransomware Advisory*, *supra* note 25, at 3.

[31] *OFAC Ransomware Advisory*, *supra* note 26, at 2.

[32] *OFAC Ransomware Advisory*, *supra* note 26, at 3.

[33] *OFAC Ransomware Advisory*, *supra* note 26, at 4.