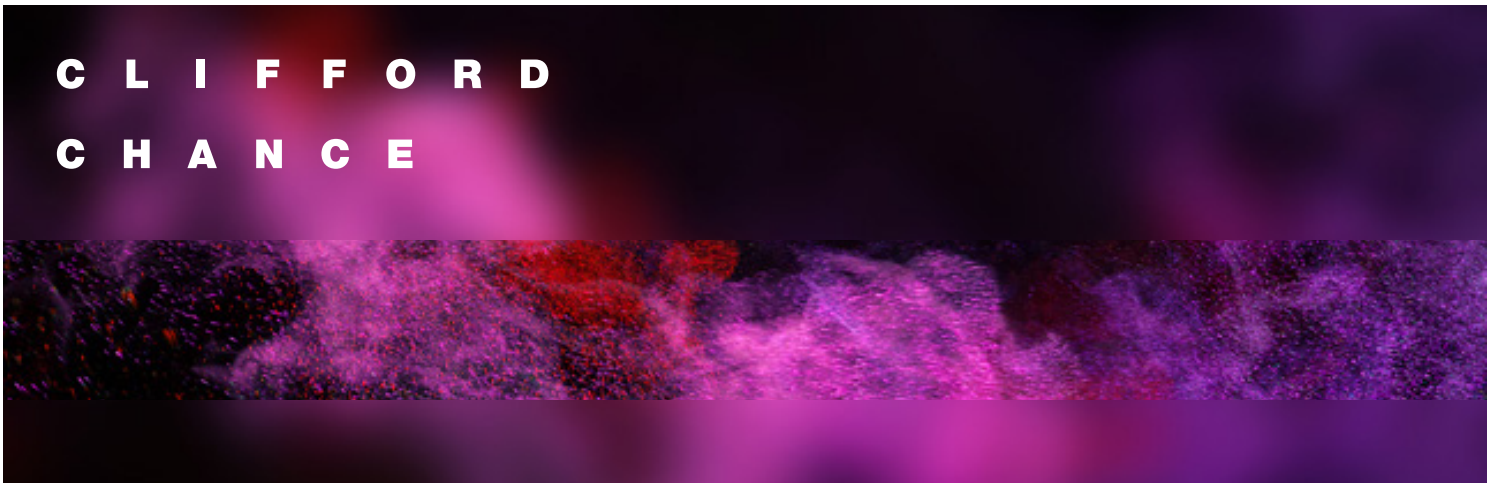

FINCEN AND DOJ SIGNAL INCREASED SCRUTINY OF CRYPTOCURRENCIES

US authorities are closely scrutinizing the anti-money laundering (AML), terrorist financing, and sanctions compliance risks associated with the use of cryptocurrencies. While US authorities including the Financial Crimes Enforcement Network of the US Treasury (FinCEN) and the US Department of Justice (DOJ) have been tracking the rise in use (and potential for misuse) of cryptocurrencies for years, 2020 saw a flurry of new developments that indicate that cryptoassets are now center stage. Recent guidance and enforcement actions against companies and private individuals make clear the need for US and non-US cryptocurrency sponsors, trading platforms and other intermediaries that facilitate cryptocurrency transactions involving US persons to adhere to applicable US legal and regulatory requirements, including registration.

Virtually all cryptocurrencies permit users to transact without revealing their identities. From the beginning, blockchain protocols underlying cryptocurrencies like Bitcoin (BTC) have allowed users to create "wallets" to hold their digital assets without going through a centralized exchange or other regulated intermediary, such as a traditional financial institution. This system provided a structure that allowed users to hold and transmit cryptocurrencies outside of the traditional financial system that requires financial services providers to conduct KYC checks and to comply with AML and terrorist financing regulations. This anonymity provides an opportunity for criminals to transact anonymously in cryptocurrencies which has naturally attracted the attention of US enforcement authorities.

FinCEN 2019 Cryptocurrency Guidance

In May 2019, the FinCEN issued guidance on how its regulations apply to certain crypto-related businesses and activities (the 2019 Guidance). FinCEN defined currency as "[t]he coin and paper money of the United States or of any other country that is designated as legal tender and that circulates and is customarily used and accepted as a medium of exchange in the country of issuance." In contrast to real currency, FinCEN concluded that "virtual" currency is a medium of exchange that operates like a currency in some environments, but does not have all the attributes of real currency and does not have legal tender status in any jurisdiction.[1]

1. *See* Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies, FIN-2019-G001 (May 9, 2019); Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, FIN-2013-G001 (Mar. 18, 2013); *see also* Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, FIN-2013-G001 (Mar. 18, 2013); Bank Secrecy Act Regulations – Definitions and Other Regulations Relating to Money Services Businesses, 76 FR 43585 (July 21, 2011).

FinCEN also defined "Convertible Virtual Currency" (CVC) as virtual currency that has either an equivalent value in real currency or acts as a substitute for real currency, and explained that it considers most established virtual currencies to be CVCs. Entities that facilitate transactions in CVC for US customers generally must register with FinCEN as money services businesses (MSBs). For example, CVC exchangers like centralized and de-centralized virtual currency trading platforms must generally register as MSBs. While FinCEN generally recognizes an exemption from its registration requirements for pure software developers, most DApps require one or more persons to not only write the code on which they run, but to also deploy/operate them, particularly at inception. When decentralized applications perform money transmission as discussed above, the definition of money transmitter may apply to the decentralized application itself, its owners/operators, or both, depending on the facts and circumstances. CVC administrators, which typically include a CVC's issuer, must also generally register as MSBs, because they are the only person authorized to issue and redeem the new units of CVC at the time of issuance. This remains true even if the issuer declines to exercise its authority through contract or otherwise.

US law requires entities registered as MSBs, or required to be registered based on their activities, to implement a dedicated AML compliance program, to submit suspicious activity reports and currency transaction reports to FinCEN, and to maintain adequate records. Platforms that fail to satisfy these requirements may expose themselves, their owners, and key executives or smart contract developers to the potentially existential threat of a FinCEN civil enforcement action, website seizure, and/or criminal prosecution by the DOJ.

DOJ Cryptocurrency Enforcement Framework & Recent FinCEN Statements

In October 2020, the DOJ published a cryptocurrency enforcement framework[2] (the Framework) laying out its enforcement priorities and its jurisdictional reach. The Framework identifies key categories of illicit use of cryptocurrency, including: (i) financial transactions associated with the commission of crimes; (ii) money laundering and the shielding of legitimate activity from tax, reporting, or other legal requirements; and (iii) crimes, such as theft, directly implicating the cryptocurrency marketplace itself. Under the Framework, the DOJ asserts broad jurisdiction to prosecute entities and individuals engaged in illicit cryptocurrency transaction, ***even when located outside the United States,*** if the crypto transactions "touch financial, data storage, or other computer systems within the United States." The Framework emphasizes DOJ's jurisdiction to prosecute actors located outside the United States that use a cryptocurrency to "provide illicit services to defraud or steal from U.S. residents."

FinCEN officials also stressed the importance of AML measures in the crypto context in 2020. In doing so, FinCEN sought to put MSBs and other financial institutions on notice of the enforcement risks associated with failing to comply with US legal and regulatory requirements. For example, FinCEN Director, Kenneth Blanco, in remarks[6] in May 2020, stated *"We expect each financial institution to have appropriate controls in*

2. Report of the Attorney General's Cyber Digital Task Force: Cryptocurrency Enforcement Framework (Oct. 2020).

place based on the products or services it offers, consistent with the obligation to maintain a risk-based AML program. This means we are taking a close look at the AML/CFT controls you put on the types of virtual currency you offer—whether it be Monero, Zcash, Bitcoin, Grin, or something else—and you should too."

Recent DOJ & FinCEN Actions

DOJ and FinCEN are backing up their messaging with aggressive AML-related enforcement activity. Recent enforcement actions have targeted both those using cryptocurrency to facilitate or conceal nefarious activities, and others that have failed to meet their legal obligations to counter illicit activity.

For example, the DOJ and FinCEN recently imposed civil penalties and proceeded criminally against the founder and operator of Helix, an unregistered MSB. In an October 2020 press release, FinCEN stated that the founder "operated Helix as a bitcoin mixer . . . and advertised its services in the darkest spaces of the internet" as a means for users to anonymously pay for nefarious activities.

FinCEN fined the founder $60 million for violations of AML laws, including failing to register Helix as an MSB and failing to implement and maintain an AML program or meet other AML requirements. The DOJ is also prosecuting him criminally on charges of conspiracy to launder monetary instruments and operating an unlicensed money transmission business.[3]

The Helix case raises additional questions about platforms that facilitate transactions in cryptocurrencies like Monero, Zcash, and Grin, which are also referred to as anonymity enhanced coins (or AECs). AECs operate on blockchain protocols specifically designed to help preserve the anonymity of their users and to obscure the identity of transaction participants. FinCEN officials have expressed specific concerns about AECs in the past and cautioned MSBs that they can "count on" being asked about AECs during examinations. MSBs facilitating transactions in AECs should consider the risks they pose in light of the Helix "mixer case," and adopt specific policies and procedures to mitigate these risks.

Advances in Blockchain Surveillance

DOJ and other US authorities are also increasingly able to use blockchain transactions, given their public nature, to identify bad actors, to "blacklist" their wallets, or to even "unmask" them by identifying wallets associated with illegal activity and mapping out wallets that sent/received cryptocurrency to/from them. This is possible because even though users can anonymously create cryptocurrency wallets, all transactions with a user's wallet are publicly, and permanently, recorded on blockchain protocols like BTC.

3. First Bitcoin "Mixer" Penalized by FinCEN for Violating Anti-Money Laundering Laws, FinCEN Press Release (Oct. 19, 2020). DOJ also recently filed a criminal indictment against the founders and one employee of a centralized non-US cryptocurrency trading platform and arrested its Chief Technology Officer. Previously, FinCEN and other US authorities took action against and ultimately shut down the online cryptocurrency platform BTC-e. *See e.g., FinCEN Fines BTC-e Virtual Currency Exchange $110 Million for Facilitating Ransomware, Dark Net Drug Sales, FinCEN Press Release (July 26, 2017); In re BTC-E et. al, FinCEN Assessment of Civil Money Penalty No. 2017-03 (July 26, 2017).*

For example, in August 2020, DOJ announced civil forfeiture actions against 280 cryptocurrency accounts implicated in laundering cryptocurrency stolen by North Korean actors. "Despite the highly sophisticated laundering techniques used" US regulators could still track the stolen funds and identify the crypto accounts engaged in laundering the funds. Similar techniques have been used in counterterrorism efforts.[4] Both DOJ and FinCEN have recommended that the blockchain industry (e.g., cryptocurrency exchanges) use similar technology and software to avoid transacting with bad actors (see our briefing **here**). Accordingly, we expect to see increased pressure on financial institutions and crypto businesses to utilize these types of technologies in their AML procedures.

FinCEN's Travel Rule & Recordkeeping Rule Proposals

DOJ and FinCEN's recent pronouncements and enforcement activity focus largely on operators of unregistered MSBs who facilitate (or directly engage in) money laundering and other illegal activity. FinCEN and the Federal Reserve Board also published a joint notice of proposed rulemaking on October 27, 2020 (the Proposed Rule) which, if implemented, would increase the compliance burden on cryptocurrency companies registered as MSBs.[5]

The Proposed Rule would lower the dollar value threshold that triggers certain regulatory requirements from $3,000 to $250 for cross-border transmittals of funds by MSBs. The requirements triggered by the lower threshold would include recordkeeping and verification obligations (the Recordkeeping Rule), and the obligation to transmit certain information to the recipient's or an intermediary financial institution (the Travel Rule). The lower $250 threshold would only apply to transmittals of funds that begin or end outside the United States.

The Proposed Rule would also amend the definition of "money" used in both the Travel Rule and Recordkeeping Rule to expressly extend to CVCs and other digital assets. This would be accomplished by amending the definition of "money" "to make explicitly clear that both payment orders and transmittal orders include any instruction by the sender to transmit CVC or any digital asset having legal tender status to a recipient." FinCEN takes the position in the Proposed Rule that the new definition codifies FinCEN's existing expectations, (i.e., that transactions in CVC are subject to both the Recordkeeping Rule and Travel Rule). FinCEN nevertheless acknowledges industry concerns that the existing definition of "money" is tied to the one used in the Uniform Commercial Code (UCC), and that the UCC's definition of "money" is limited to "legal tender," which does not include CVCs.

---

4. *See, e.g.*, United States Files Complaint to Forfeit 280 Cryptocurrency Accounts Tied to Hacks of Two Exchanges by North Korean Actors, DOJ Press Release (Aug. 27, 2020); U.S. Seizes Bitcoin Said to Be Used to Finance Terrorist Groups, New York Times Article (Aug. 12, 2020) (stating that law enforcement officials obtained court orders to seize about 300 cryptocurrency wallets held by bank-like institutions, and that they blacklisted privately held accounts containing several million dollars of virtual currency);
5. Threshold for the Requirement To Collect, Retain, and Transmit Information on Funds Transfers and Transmittals of Funds That Begin or End Outside the United States, and Clarification of the Requirement To Collect, Retain, and Transmit Information on Transactions Involving Convertible Virtual Currencies and Digital Assets With Legal Tender Status, 85 F.R. 68005 (Oct. 27, 2020).

What's next?

FinCEN and DOJ's recent activities highlight their increasing focus on cryptocurrencies and their broad assertion of extraterritorial jurisdiction in these markets. Their actions also highlight the increasing sophistication of US blockchain surveillance techniques, and the importance of ensuring compliance with US law, including by assessing the relevant risks and establishing effective risk mitigation and compliance programs. In the wake of these developments, both US and non-US cryptocurrency issuers, cryptocurrency platforms, and others involved in facilitating cryptocurrency transactions should closely assess their US law compliance and take steps to ensure compliance, including, as necessary, by registering in an appropriate capacity and implementing AML and other compliance programs. FinCEN-registered MSBs should also examine the adequacy of their AML compliance programs and policies and procedures. This examination may result in increased surveillance of transactions in AECs or in restricting their use, enhanced customer identification practices, the use of new software or service providers to identify blacklisted wallets, stricter white listing protocols, or other steps.

CLIFFORD

CHANCE

CONTACTS

Steven Gatti
Partner
Washington DC
T: +1 202 912 5095
E: steven.gatti@cliffordchance.com

Megan Gordon
Partner
Washington DC
T: +1 202 912 5021
E: megan.gordon@cliffordchance.com

Robert Rice
Partner
New York
T: +1 212 878 8529
E: robert.rice@cliffordchance.com

Joshua Berman
Partner
Washington DC
T: +1 202 912 5174
E: joshua.berman@cliffordchance.com

Glen Donath
Partner
Washington DC
T: +1 202 912 5138
E: glen.donath@cliffordchance.com

Celeste Koeleveld
Partner
New York
T: +1 212 878 3051
E: celeste.koeleveld@cliffordchance.com

Philip Angeloff
Counsel
Washington DC
T: +1 202 912 5111
E: philip.angeloff@cliffordchance.com

David Adams
Associate
Washington DC
T: +1 202 912 5067
E: davidg.adams@cliffordchance.com

Jesse Overall
Associate
New York
T: +1 212 878 8289
E: jesse.overall@cliffordchance.com

Holly Bauer
Associate
Washington DC
T: +1 202 912 5132
E: holly.bauer@cliffordchance.com

Find more of our global fintech team at
www.cliffordchance.com/fintech

2011-001501