October 2020

Skadden

The Distributed Ledger

Blockchain, Digital Assets and Smart Contracts

Recent and significant regulatory and legislative events in the digital asset space demonstrate the evolving and expanding approach by U.S. and international regulators to the burgeoning digital asset markets. These developments implicate the jurisdiction of numerous regulatory bodies, whose recent actions (described in this issue) illustrate their sharpening focus on the legal issues that this emerging asset class may present.

DOJ Issues First-Ever Cryptocurrency Enforcement Framework

On October 8, 2020, the Department of Justice (DOJ) issued its Cryptocurrency Enforcement Framework, the first comprehensive public statement of the DOJ's approach to investigating and prosecuting cryptocurrency-related crimes. The framework sets as its goals to: "describe how cryptocurrency technology" is currently used and misused; identify legal authorities and agency relationships on which the DOJ has relied to prosecute cryptocurrency-related offenses; and discuss potential DOJ approaches to "growing public safety challenges related to cryptocurrency." Given the DOJ's natural focus on illicit activity, the framework takes a somewhat skeptical view of cryptocurrency's value as a legitimate asset and stakes out a broad vision for U.S. enforcement and U.S. jurisdiction in this area.

The introduction to the framework acknowledges the importance of blockchain innovation but asserts that without appropriate safeguards and oversight, innovation can "facilitate great human suffering." Part I of the framework, "Threat Overview," addresses the use and misuse of cryptocurrency. The framework identifies and provides detailed examples of three categories of cryptocurrency-related crimes: using cryptocurrency to commit crimes; using cryptocurrency to hide illicit financial activity; and crimes against the cryptocurrency marketplace itself, such as hacks of cryptocurrency exchanges.

In Part II of the framework, the DOJ sets out federal statutes and regulations that have been and can be used to pursue cryptocurrency-related violations. The list includes what most have recognized as the key legal levers: the federal fraud statutes, money laundering statutes and the statutes governing underlying criminal activity that cryptocurrency can facilitate. The framework also points out that the civil forfeiture statute allows the government to seize virtual assets derived from or involved in criminal activity, a tool

that has been used extensively in recent years, including in cases of terrorist financing and hacks of cryptocurrency exchanges. Notably, the framework does not identify shortfalls in existing law or propose any new legislation or regulations.

In addition, Part II identifies the DOJ's partners, both domestic and international, in the cryptocurrency enforcement space. Here, too, the list includes the U.S. entities that those involved in this space would identify: Financial Crimes Enforcement Network (FinCEN); the Office of Foreign Assets Control, the Office of the Comptroller of the Currency (OCC), the Securities and Exchange Commission (SEC), the Commodity Futures Trading Commission (CFTC) and the Internal Revenue Service, as well as state authorities. On the international front, the DOJ acknowledges that cryptocurrency's global nature poses particular challenges for U.S. law enforcement and urges international implementation of the Financial Action Task Force's (FATF) recommendation to bring virtual asset activity within the FATF's anti-money laundering (AML) and countering the financing of terrorism standards.

Part III of the framework, which is focused on "Ongoing Challenges and Future Strategies," provides some insight into the DOJ's priorities and strategies. In particular, the DOJ identifies "business models and activities that may facilitate criminal activity": cryptocurrency exchanges; peer-to-peer (P2P) exchangers and platforms; cryptocurrency ATMs and kiosks; virtual currency casinos; anonymity-enhanced cryptocurrencies (AECs); and mixers, tumblers and chain hopping. Within this group, the DOJ seems especially concerned with P2P exchangers and AECs:

- The framework asserts that although "P2P exchangers are considered [money services businesses] and are subject to FinCEN record keeping and reporting requirements," "many P2P exchangers fail to register with FinCEN as MSBs or to comply with [Bank Secrecy Act] obligations, and some even conduct transactions without requiring any form of identification from the customer."
- Perhaps more starkly, the framework states that "[t]he Department considers the use of AECs to be a high-risk activity that is indicative of possible criminal conduct." The framework calls out certain cryptocurrencies by name, stating that "[c]ompanies that choose to offer AEC products should consider the increased risks of money laundering and financing of criminal activity" and notes that such companies should evaluate "whether it is possible" to address such risks, suggesting it might not be.

The framework appears similarly skeptical of privacy concerns in the enforcement arena: It devotes a page to the European Union's General Data Protection Regulation (GDPR), a privacy law that some exchanges have cited in resisting U.S. grand jury subpoenas. The framework suggests GDPR objections generally lack merit and signals a willingness to take the fight to the courts, including "pursu[ing] motions to compel as needed."

Finally, the framework makes clear that the DOJ is prepared to exercise expansive jurisdiction over cryptocurrency-related crimes, noting that the agency "has robust authority" to prosecute individuals and entities outside the United States. In addition, it asserts that U.S. regulations apply to cryptocurrency businesses abroad if they serve U.S. customers: "[A]ll entities, including foreign-located exchanges, that do business wholly or in substantial part within the United States, such as by servicing U.S. customers, must also register with FinCEN and have an agent in the United States for [Bank Secrecy Act] reporting and for accepting service of process."

Although there is much in the framework that will be familiar to those well versed in the cryptocurrency space, it is a significant development. It is a clear signal that the DOJ has devoted resources to understanding cryptocurrency, that it is watching how cryptocurrency can be used to commit and facilitate crimes, and that it will take action when cryptocurrency is involved in criminal activity almost anywhere around the globe.

US Enforcement Activity

CFTC and DOJ Actions Against Off-Shore Cryptocurrency Derivatives Exchange

On October 1, 2020, the CFTC and the DOJ brought actions against BitMEX, a cryptocurrency exchange and derivatives trading platform owned and operated by Seychelles-based HDR Global Trading Limited. The CFTC filed a civil action against BitMEX for failing to register with the CFTC while offering products that allegedly fall within the CFTC's regulatory jurisdiction.[1] The DOJ simultaneously announced the indictment of four founders and executives of BitMEX for alleged violations of AML requirements under the Bank Secrecy Act (BSA).

Specifically, the CFTC's complaint alleges that BitMEX violated the Commodity Exchange Act (CEA) by offering cryptocurrency derivatives (leveraged retail commodity transactions, futures,

[1] Complaint, *CFTC v. HDR Global Trading Ltd.*, No. 1:20-cv-08132-MKV (S.D.N.Y. Oct. 1, 2020), ECF No. 1; *see also, e.g.*, Complaint, *CFTC v. Laino Group Ltd.*, No. 4:20-cv-03317 (S.D. Tex. Sept. 24, 2020), ECF No. 1.

options and swaps) to U.S. retail customers and accepted their funds to margin derivatives transactions without registering as a futures commission merchant (FCM) under the CEA. The CFTC has determined that virtual currencies are commodities under the CEA, and an entity must register with the CFTC as an FCM "if it solicits or accepts orders for commodity futures contracts, swaps, or retail commodity transactions (among other specified products), and in connection with such activity accepts any money or property to margin, guarantee, or secure any trades or contracts that result or may result therefrom."[2]

As an FCM, BitMEX is a covered financial institution under the BSA and must maintain an AML compliance program that meets certain requirements, including but not limited to the maintenance of policies, procedures and controls reasonably designed to prevent the FCM from being used for money laundering or terrorist financing; independent testing of the compliance program; the designation of personnel responsible for overseeing the compliance program; ongoing training for appropriate personnel; risk-based procedures for conducting ongoing customer due diligence; and the filing of suspicious activity reports (SARs).[3]

The DOJ's indictment alleges that the BitMEX executives solicited and accepted customers and operated in the United States without complying with U.S. AML requirements. The DOJ alleges that the defendants understood that these requirements applied to BitMEX if it operated in the United States and that they "took affirmative steps purportedly designed to exempt BitMEX" from the application of these laws, including by incorporating the company outside the United States, in the Seychelles, "a jurisdiction they believed had less stringent regulation."[4] The indictment alleges that the defendants caused BitMEX to reject the adoption of the AML requirements required of it as an FCM and, as a result, "BitMEX made itself available as a vehicle for money laundering and sanctions violations."[5] The indictment specifically highlights allegations that the trading platform was used by customers located in Iran, which is subject to U.S. economic sanctions.

These actions by the CFTC and DOJ against BitMEX are the latest in the U.S. government's steady stream of enforcement actions against individuals and entities that deal in digital assets. It is also an example of increasing cross-agency collaboration — both in guidance and enforcement — as multiple regulators police the digital assets markets, seeking to provide regulatory certainty for the operators of digital asset trading platforms and other businesses, and enhanced protection for retail customers. An important refrain in recent regulatory guidance — and a central theme in the BitMEX case — is that those companies and individuals that operate, or provide services to customers, in the United States will be subject to the reach of U.S. regulators, regardless of where they are based.

FinCEN Imposes $60 Million Civil Monetary Penalty on Operator of 'Mixers'

On October 19, 2020, FinCEN assessed a $60 million civil monetary penalty[6] against Larry Dean Harmon, the founder and operator of two convertible virtual currency (CVC) exchangers, Helix and Coin Ninja, for willful violations of the BSA and FinCEN's implementing regulations.

According to FinCEN, Helix was an unregistered money services business (MSB) that operated as a bitcoin "mixer" or "tumbler" — a provider of anonymizing services that accepts CVCs and retransmits them in a manner designed to prevent others from tracing the transmission back to its source. In its civil penalty assessment, FinCEN asserted that Helix would receive bitcoin from its customers and, for a fee, subsequently send bitcoin from a different Helix account to a destination account specified by its customer. FinCEN noted that Coin Ninja also operated as an unregistered MSB, and its website indicated it also provided "mixing" services.

FinCEN has clarified in guidance that anonymizing services providers are MSBs because they accept and transmit CVCs.[7] MSBs have a range of obligations under the BSA, including a requirement to register with FinCEN, to implement an effective AML compliance program and to file SARs. According to FinCEN, with respect to Helix, Mr. Harmon never implemented an AML compliance program and failed to develop internal policies,

[2] Sealed Indictment at 3, *United States v. Hayes*, No. 1:20-cr-00500-JGK (S.D.N.Y. Sept. 21, 2020), ECF No. 2; *see also* 7 U.S.C. § 1a(28).

[3] 31 C.F.R. § 1026.210; 31 C.F.R. § 1026.320.

[4] Sealed Indictment at 9, *United States v. Hayes*, No. 1:20-cr-00500-JGK (S.D.N.Y. Sept. 21, 2020), ECF No. 2.

[5] *Id.* at 11.

[6] In the Matter of Larry Dean Harmon d/b/a Helix, Assessment of Civil Monetary Penalty.

[7] Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies (FIN2019-G001), May 9, 2019, p.19-20.

procedures and internal controls; appoint a compliance officer; train personnel; conduct independent testing; or file SARs.[8] Significantly, FinCEN noted that Helix "openly flaunted existing regulatory requirements and went out of its way to create ways for darknet customers and vendors to avoid law enforcement detection."[9] FinCEN emphasized that Mr. Harmon openly advertised Helix as a service that did not conduct customer due diligence[10] and that Helix asserted even the minimal customer information collected was being deleted.[11] According to FinCEN, "from June 2014 through December 2017, Helix conducted over 1,225,000 transactions for its customers and was associated with virtual currency wallet addresses that sent or received over $311 million dollars."[12] FinCEN noted that of that amount, bitcoin transactions valued at over $121 million were transferred to darknet-associated addresses by, through or to Helix. FinCEN concluded that as "a sophisticated enterprise, Helix worked in conjunction with darknet marketplaces to launder illicit bitcoin proceeds and actively marketed its services as an anonymity-enhancing service to launder bitcoin from illicit activity."[13]

FinCEN determined that the maximum penalty in this matter was $209.14 million. FinCEN stated it was authorized to impose a civil monetary penalty in the amount of $57,317 for each willful violation of the AML program requirements and $8,457 for each violation of the requirement to register as an MSB. Under the BSA, each day a violation continues can be considered a separate violation. In determining the final penalty in the amount of $60 million, FinCEN weighed a number of factors, including the nature and seriousness of the violations and their harm to the public, the impact on FinCEN's mission to safeguard the financial system, the pervasiveness of the wrongdoing at Helix, the financial gain resulting from the violations and the fact that Helix agreed to two statute of limitations tolling agreements.

FinCEN also noted that it provided Helix with a pre-assessment notice, which included an outline of the violations, the factors FinCEN considered and the proposed civil monetary penalty amount. According to FinCEN, Helix responded through counsel denying that it operated as an MSB and requested additional time to respond. However, after eight months of failing to respond to the allegations or provide additional information, FinCEN concluded Helix decided not to submit any new facts or explanations and moved forward with the civil penalty assessment.[14]

In addition to FinCEN's civil enforcement action, Mr. Harmon is being prosecuted in the U.S. District Court for the District of Columbia on charges of conspiracy to launder monetary instruments and the operation of an unlicensed money transmitting business in connection with his operation of Helix.

SEC Granted Summary Judgment in Kik Enforcement Action

On September 30, 2020, Judge Alvin Hellerstein of the U.S. District Court for the Southern District of New York granted summary judgment in favor of the SEC in the closely watched enforcement action *SEC v. Kik*, 19-cv-5244(AKH)(S.D.N.Y.). The SEC brought suit in June 2019, asserting that Kik's offering of its digital tokens, called Kin, violated the federal securities laws. Kik offered the tokens through a private pre-sale to a limited number of accredited investors and later through a public distribution. The court held that, in evaluating compliance with the securities laws, the two offerings should be integrated into a single public offering and concluded that "Kik offered and sold securities without a registration statement or exemption from registration, in violation of Section 5 [of the Securities Act of 1933]." Judge Hellerstein held that there were no material issues of fact warranting trial as to any prong of the "investment contract" test set forth in *SEC v. W.J. Howey*, 328 U.S. 293 (1946), including whether Kik's sales gave rise to a "horizontal common enterprise" and an "expectation of profits based on the efforts of others."

Regarding the common enterprise prong, the court found that the funds raised through Kik's sale of Kin were pooled into "a single bank account" and used by Kik "for its operations, including the construction of the digital ecosystem it promoted." While Kik expressly disclaimed any ongoing obligations to develop the ecosystem, Judge Hellerstein held that "an ongoing contractual obligation is not a necessary requirement for a finding of a common enterprise." The court disregarded that Kin purchasers could sell their tokens independently at any time, stating that "the key feature [of a common enterprise] is not that investors must reap their profits at the same time; it is that investors' profits at any given time are tied to the success of the enterprise."

[8] *See* 31 U.S.C. § 5318(h).

[9] In the Matter of Larry Dean Harmon d/b/a Helix, Assessment of Civil Monetary Penalty, at 5.

[10] In the Matter of Larry Dean Harmon d/b/a Helix, Assessment of Civil Monetary Penalty Attachment A – Statement of Facts, at. 4.

[11] In the Matter of Larry Dean Harmon d/b/a Helix, Assessment of Civil Monetary Penalty, at 4-5

[12] *Id.* at 2.

[13] *Id.* at 4.

[14] *Id.*

Regarding the expectation of profits prong, the court found that Kik "extolled Kin's profit-making potential" and "allow[ed] purchasers to buy more Kin to speculate on any increase in value." Judge Hellerstein further found that "none of [Kin's] 'consumptive use' was available at the time of the distribution" of the tokens, and any argument that market forces would drive the value of Kin "ignores the essential role of Kik in establishing the market" through its efforts to develop the ecosystem. On this point, the court contrasted cases involving real estate, stating that "Kin have no inherent value and will generate no profit absent an ecosystem that drives demand," and "[i]t is undisputed that Kik had to be the primary driver of that ecosystem."

Finally, the court rejected Kik's argument that the *Howey* test is unconstitutionally vague as applied to the facts of the case, ruling that *Howey* provides " a clearly expressed test for determining what constitutes an investment contract."

On October 21, 2020, the court approved the parties' agreed-upon final judgment whereby Kik (i) is permanently enjoined from violating Section 5 of the Securities Act, (ii) for a period of three years, will provide 45 days' notice to the SEC before offering, selling or transferring any "covered assets" (which includes the 3 trillion Kin tokens issued by Kik to itself in 2017); and (iii) will pay a $5 million civil penalty.

Although the *Kik* decision may be viewed by some as providing clarity in an area dominated by uncertainty, its broader influence remains to be seen. As a trial-level opinion, it is not binding on any other court or matter, though courts are free to follow its reasoning to the extent it is found persuasive in the context of sales of other digital currencies. It bears noting that, in rejecting Kik's constitutional defense, Judge Hellerstein emphasized that "every cryptocurrency, along with the issuance thereof, is different and requires a fact-specific analysis." Thus, one of the very grounds upon which the court ruled against Kik may supply the decision's own limiting principle.

SEC Brings Enforcement Action Against McAfee for Alleged Illegal ICO 'Touts'

On October 5, 2020, the SEC filed an enforcement action against the computer programmer and entrepreneur John David McAfee for allegedly leveraging his fame to make more than $23.1 million in undisclosed compensation by recommending at least seven initial coin offerings (ICOs) to his thousands of Twitter followers. The SEC accused Mr. McAfee of violating Sections 17(a) and 17(b) of the Securities Act and Section 10(b) of the Securities Exchange Act.

The complaint also named Mr. McAfee's bodyguard, Jimmy Gale Watson, Jr., who allegedly negotiated the deals with the ICO issuers, helped Mr. McAfee monetize the proceeds of his promotions and directed his then-wife to tweet fake interest in an ICO that Mr. McAfee was promoting at the behest of the offeror.

According to the SEC, in 2017, Mr. McAfee allegedly gained hundreds of thousands of Twitter followers and fame in the digital asset community by tweeting predictions about the rise in trading prices of bitcoin. ICO issuers began contacting Mr. McAfee to ask him to promote their digital asset offerings, and from November 2017 to February 2018, Mr. McAfee unlawfully "touted" seven ICOs by promoting them through at least 40 tweets and replies without disclosing that he was being paid to do so. Additionally, the SEC accused Mr. McAfee of falsely claiming to be an investor and/or a technical adviser to certain ICO issuers.

On February 8, 2018, a blogger on an online messaging board posted a message speculating that Mr. McAfee had promoted an unsuccessful project to unwitting investors for compensation and that the SEC should be alerted. In response to this blog post, Mr. McAfee allegedly admitted to being paid for promotions while falsely claiming to have reviewed and picked the best ICOs to recommend and provided advice to the issuers. Further, Mr. McAfee allegedly orchestrated a scheme to pay a separate promoter to tout certain of the tokens without disclosing the arrangement. The SEC claims Mr. McAfee did so in order to increase the price of those digital assets and cash them out.

Finally, Mr. McAfee is accused of "scalping" for at least one of the digital assets, a practice whereby someone (i) obtains securities for his or her own account prior to recommending or touting it to others, (ii) fails to disclose the complete truth about the ownership of the securities and plans to sell them, and then (iii) sells the securities. "Scalping" generally allows promoters to sell their securities holdings quickly and profitably through market interest that they deceptively generate.

In addition to the SEC enforcement action, the Tax Division of the Department of Justice unsealed an indictment filed in June 2015 against Mr. McAfee for failing to file an income tax return and willfully attempting to evade and defeat income tax due on, *inter alia*, income received from 2017 through 2018 for promoting cryptocurrencies.

Unikrn Agrees To Disable Token in SEC Consent Order

Unikrn, Inc., an operator of an online esports gaming and gambling platform, entered into a September 15, 2020, consent order with the SEC under which it agreed to permanently disable its digital token UnikoinGold (UKG) after the SEC alleged that the token was sold in an unregistered securities offering in which Unikrn raised $31 million.

In the consent order, the findings of which Unikrn neither admitted nor denied, the SEC found that UKG tokens were securities under the *Howey* test, concluding that purchasers in the offering of UKG tokens had a reasonable expectation of obtaining a future profit based upon Unikrn's efforts to create applications for tokens. The SEC came to this conclusion despite the terms of the public token sale agreement, which required purchasers to agree that they were buying UKG tokens for their utility and not as an investment.

The SEC also focused on Unikrn's alleged promotional efforts, including its description to investors that the company's efforts to expand the UKG tokens' functionality would increase their value, and that as the company added and improved the products and services for use with the UKG tokens, the betting volume and turnover of the UKG tokens on Unikrn's platform would increase. Unikrn further allegedly represented that it would facilitate a secondary trading market for the tokens and that its efforts to increase the uses for the UKG token would increase the demand for and, in turn, the value of the tokens. Additionally, the SEC pointed to Unikrn's alleged statements to purchasers that it was committed to maintaining a "stable ecosystem" for UKG, and that the company would limit the number of tokens sold in the offering in order to "maintain value in UnikoinGold and limit the number of tokens in the market."

In addition to agreeing to permanently disable UKG and to request its removal from digital asset trading platforms, Unikrn agreed to pay a civil money penalty in the amount of $6.1 million to the SEC. A Fair Fund would also be created pursuant to Section 308(a) of the Sarbanes-Oxley Act, as amended by the Dodd-Frank Act, to be used to compensate harmed investors for losses resulting from the violations determined in the consent order.

Salt Blockchain Enters Into SEC Consent Order

Salt Blockchain Inc., a company formed in 2016 with plans to offer U.S. dollar-denominated loans secured by blockchain assets, entered into a September 30, 2020, order instituting cease-and-desist proceedings with the SEC, under which it agreed to register its Salt Tokens.

The SEC claimed that Salt violated Sections 5(a) and 5(c) of the Securities Act by offering and selling Salt Tokens without a registration statement or qualifying for an exemption from registration. Starting in June 2017, Salt conducted a "membership token sale" or ICO in which it offered and sold the Salt Tokens and raised approximately $47 million.

The SEC found that Salt Tokens were offered and sold as investment contracts under *Howey*, determining that purchasers had a reasonable expectation of profits because the proceeds of the offering were intended to improve Salt's lending business and the development of associated technology that would increase demand for Salt Tokens and thus their value. The SEC further found that Salt told investors that the company would launch the lending platform and take various steps to increase the price of Salt Tokens, including limiting the number of Salt Tokens created and sold, managing the price at which Salt continued to sell the Salt Token and managing the value at which Salt allowed the Salt Tokens to be redeemed for various benefits.

Further, both before and after the ICO, Salt sought to have Salt Tokens listed on various secondary trading platforms and stated in communications that it would support secondary market sales by setting the price at which it would sell its remaining Salt Tokens above the prevailing secondary market price.

Under the consent order, Salt agreed to: register the Salt Tokens as a class of securities under Section 12(g) of the Securities Exchange Act; inform all persons and entities that purchased Salt Tokens from it before or on December 31, 2019, of their potential claims under Section 12(a) of the Securities Act, including the right to sue to recover the consideration paid for the tokens upon tender; and pay a civil money penalty of $250,000. Salt neither admitted nor denied the findings in the order.

OCC Permits Banks To Hold Reserves for Certain Stablecoins

The OCC has continued its support for the cryptocurrency industry, publishing a September 21, 2020, letter clarifying that national banks and federal savings associations (FSA) have the authority to hold reserves as a service to bank customers who issue certain types of stablecoins and to engage in activities incidental to receiving deposits from stablecoin issuers.[15]

[15] OCC Chief Counsel's Interpretation on National Bank and Federal Savings Association Authority To Hold Stablecoin Reserves. In July 2020, the OCC published a letter clarifying national banks' and federal savings associations' authority to provide cryptocurrency custody services for customers.

Stablecoins, in contrast to cryptocurrencies such as bitcoin or ether, which can be volatile, are designed to be stable, either because they are backed by a fiat currency, a commodity such as gold or another cryptocurrency, or because they are stabilized through a computer algorithm.

The OCC letter focuses on the holding of fiat reserves that back stablecoins where those coins are held in "hosted wallets." These are cryptocurrency wallets where the wallet provider custodies the keys of the account holder and typically conducts diligence on the customer as required by applicable law. The letter notes that the OCC is not currently addressing the authority to support stablecoin transactions involving unhosted wallets in which the holder custodies their own keys and there can be no assurances that any checks were done on the holder.

Th letter is directed toward stablecoins that are backed by a single fiat currency (as opposed to a basket of currencies) and on a one-to-one basis. Banks and FSAs are also required to verify on at least a daily basis that the reserve account balance held by the bank or FSA is greater than or equal to the number of the issuer's outstanding stablecoins.

While the OCC letter is supportive of providing this service, it cautions that banks need to comply with their other legal requirements — an important admonition, given the wide range of stablecoin issuers. For example, the letter notes that banks and FSAs must ensure that they have "instituted appropriate controls and conducted sufficient due diligence commensurate with the risks associated with maintaining a relationship with a stablecoin issuer." This due diligence process includes understanding the risks of cryptocurrency and a compliance review of applicable laws such as those related to the BSA and anti-money laundering. In addition, a national bank or FSA is required to ensure that it establishes and maintains procedures reasonably designed to assure and monitor its compliance with the BSA.

In connection with risk management, the OCC letter notes that reserves associated with stablecoins could entail significant liquidity risks, and therefore banks must manage liquidity risk "with sophistication equal to the risks undertaken and complexity of exposures."

The OCC letter also reminds banks and FSAs that they must comply with applicable federal securities laws. In a footnote, the letter refers to a statement by the staff of the SEC encouraging stablecoin issuers to contact the SEC staff with questions as to whether a stablecoin is structured, marketed and operated in compliance with the federal securities laws. The OCC letter cites the SEC FinHub Staff Statement on OCC Interpretation that was issued the same day. In that statement, the SEC explains that whether a particular digital asset, including a stablecoin, is a security is "inherently a facts and circumstances determination. This determination requires a careful analysis of the nature of the instrument, including the rights it purports to convey, and how it is offered and sold."

The OCC letter could be an important step toward fostering the growth and adoption of stablecoins.

CFTC Issues Futures Commission Merchant Virtual Currency Guidance

On October 21, 2020, the CFTC Division of Swap Dealer and Intermediary Oversight (DSIO) published an advisory (the Advisory) for FCMs regarding the segregation of virtual currency in customer accounts.[16]

The Advisory was published in response to requests from market participants for DSIO to explain how the customer protection provisions of the CEA and the CFTC regulations[17] apply to virtual currencies deposited by futures customers or cleared swaps customers with FCMs to margin futures, options on futures and cleared swaps.[18] In the Advisory, DSIO observes that "virtual currencies present a degree of custodian risk that is beyond what is currently present with depositories, such as banks and trust companies" and, in light of this concern, provides guidance to FCMs regarding how to hold and report certain virtual currency deposited by customers in connection with physically delivered virtual currency futures or swaps, including with respect to:

- Where and how virtual currency held as customer funds by an FCM must be deposited.
- Requirements for virtual currency to be made available for withdrawal from a depository on an FCM's demand.
- Requirements for the FCM's preparation of daily and month-end segregation statements.
- Prohibitions on commingling of an FCM's own virtual currency in customer accounts, and on the investment of segregated customer funds in virtual currency.

[16] *See* CFTC Staff Letter No. 20-34 (Oct. 21, 2020) [hereinafter "Advisory"].

[17] *See, e.g.*, 7 U.S.C. 6d(a)(2), 6d(f), 17 C.F.R. §§ 1.11, 190.01 et seq.

[18] *See* Advisory at 1. The Advisory makes clear that it does not address virtual currency held by FCMs on behalf of customers trading futures or options on futures on foreign markets, or virtual currency assets held by FCMs on their own behalf, such as in proprietary accounts. *Id.*

The Advisory also provides guidance with respect to FCM risk management programs concerning the acceptance of virtual currency as customer funds, including regarding:

- How an FCM should limit the acceptance of virtual currency into segregated accounts.
- Restrictions on using virtual currency as margin (*i.e.*, as collateral to support open contracts).
- Circumstances under which an FCM that holds virtual currency for a customer should initiate a return of the virtual currency to the customer.
- Timing for completion of withdrawals of virtual currency from a depository by an FCM in order to liquidate customer accounts or return customer funds.
- Notice that an FCM must provide to futures and cleared swaps customers, prior to accepting virtual currency into segregated accounts, regarding the date on which the FCM will begin accepting virtual currency.

CFTC Chairman Heath P. Tarbert remarked that the Advisory is intended to advance the CFTC's goal of "clarity" by providing "additional certainty" to market participants as the CFTC "works to establish a holistic framework for digital asset derivatives."[19]

International Developments

UK Imposes Restrictions on Sale of Crypto-Assets and Related Products

The U.K. Treasury and Financial Conduct Authority (FCA) have taken steps to restrict the sale of crypto-assets and ban the sale of derivatives referencing crypto-assets (crypto-derivatives) to U.K. retail investors. In the U.K., marketing and distributing financial instruments and the provision of related services are governed by the U.K. financial promotion regime. The U.K. Treasury has proposed new legislation expanding the financial promotion regime to cover unregulated crypto-assets. This will affect the ability of service providers to distribute crypto-assets and market-related services in the U.K.

On October 6, 2020, the FCA published a policy statement confirming that it had implemented an outright ban on the marketing, distribution and sale of crypto-derivatives in or from the U.K. to retail customers. The ban means that service providers will not be able to rely on limited exemptions from the financial promotion regime to market crypto-derivatives to retail clients, and even FCA-regulated service providers will not be able to sell these products to retail clients.

[19] *See* Press Release, "CFTC Staff Issues Advisory on Virtual Currency for Futures Commission Merchants," CFTC (Oct. 21, 2020).

Proposed Extension of the UK Financial Promotion Regime

Under the Financial Services and Markets Act 2000, promotions of "controlled investments" and related "controlled activities" (*i.e.*, investment services) are permissible only if made or approved by entities that are regulated in the U.K. subject to certain exemptions set out in the Financial Promotion Order 2005 (FPO). The U.K. Treasury's proposals extend this general restriction on promotions, and the related framework of exemptions, to certain "unregulated cryptoassets."

The U.K. Treasury's consultation defines a "cryptoasset" as "a cryptographically secured digital representation of value or contractual rights that uses some type of distributed ledger technology and can be transferred, stored or traded electronically." The family of crypto-assets captured by this broad definition is further subdivided into "security tokens" and "unregulated cryptoassets." Confusingly, the term "security tokens" captures both instruments that replicate features of traditional financial instruments (such as shares and bonds) and e-money tokens, which are by definition not financial instruments but types of e-money. "Unregulated cryptoassets" are any type of crypto-asset that is not a security token, such as payment tokens and utility tokens.

Under the U.K. Treasury's proposals, "qualifying" unregulated crypto-assets would be deemed "controlled investments" and therefore be made subject to the financial promotion regime. The characteristics of fungibility and transferability exclude some unregulated crypto-assets from the scope of the proposed changes. Instruments that can be redeemed only by the issuer, such as a loyalty points scheme arranged on the basis of a distributed ledger technology system, would not be regarded as transferable. Additionally, central bank digital currencies are specifically excluded.

The U.K. Treasury proposal also extends the scope of certain existing "controlled activities" to encompass "qualifying" unregulated crypto-assets. Under the proposal, the following activities, when carried out in respect of qualifying unregulated crypto-assets, would amount to a controlled activity:

- dealing in securities and contractually based investments;
- arranging deals in investments;
- managing investments; and/or
- advising on investments.

Marketing of unregulated crypto-assets to U.K. investors will be curtailed as a result of the extension of the definitions of "controlled investment" and "controlled activity" described above. Service providers seeking to distribute such crypto-assets in the

U.K. will (if the proposal is adopted) be required to either rely on an exemption specified in the FPO and have their marketing material approved by an FCA-authorized entity before distribution or obtain authorization themselves before carrying out the marketing activity.

Prohibition of Sale of Crypto-Derivatives to UK Retail

The FCA's prohibition of the marketing, sale and distribution of crypto-derivatives to retail investors will be implemented in the U.K. by the Conduct of Business (Cryptoasset Products) Instrument 2020 (FCA 202/34), with the final rules coming into force on January 6, 2021. Crypto-derivatives are already subject to the U.K. financial promotion regime, so the FCA's policy statement is intended to prohibit any use of exemptions from the regime that may enable the sale of crypto-derivatives to U.K. retail clients by unregulated service providers, and to prohibit FCA-regulated service providers from marketing such instruments to U.K. retail investors.

The result of the legislative and regulatory change is to significantly curtail access to the U.K. retail market for issuers and distributors of crypto-assets and crypto-derivatives. Given the ongoing proposals to develop a bespoke crypto-assets licensing and supervisory regime at an international level by the Financial Stability Board and the EU,[20] we can expect further developments in this area in the U.K.

OECD Report Sheds Light on Current Taxation Practices and Issues Related to Cryptocurrencies

On October 12, 2020, the Organization for Economic Co-operation and Development (OECD) published a report titled "Taxing Virtual Currencies: An Overview of Tax Treatments and Emerging Tax Policy Issues." The report was prepared with the participation of over 50 jurisdictions and aims to address certain tax policy challenges raised by digital financial assets based on distributed ledger technology (referred to in the report as "crypto-assets"), with a focus on virtual currency. The report is based to a significant extent on responses received from a questionnaire sent to participating governments to identify the current approaches being taken with respect to the income, value-added and property taxation of crypto-assets.

The report describes the various ways in which crypto-assets can be created (such as airdrops, initial token offerings, mining and forging), summarizes the common ways of storing (in various types of "wallets") and transferring (through exchanges or brokers) crypto-assets, and also provides an overview of hard forks and soft forks. The report attempts to provide readers with a basic understanding of the terminology in this area, which may make the report of particular use to anyone who is first exploring the tax issues inherent in crypto-assets. While the focus of the report is on the taxation of crypto-assets, topics addressed also include the legality of virtual currencies, the accounting treatment for crypto-assets and the energy usage associated with virtual currencies.

For purposes of analyzing and suggesting tax treatment of crypto-assets, the report divides such assets into three categories:[21]

- Payment tokens/virtual currencies (such as bitcoin and ether) that are usable as a means of exchange for goods or services, and may also be a store of value.
- Security tokens, which are tradable assets that are classified as a security under applicable laws and held for investment purposes.
- Utility tokens, which may allow access to specific goods or services, or effectively serve as a license.

The remainder of the report largely focuses on crypto-assets in the first of these categories. The report confirms that most OECD jurisdictions, like the United States, have explicitly laid out a view that such virtual currencies are not "currencies" for tax purposes.[22] The stated justification for this treatment comes in part from political views whereby a currency is linked to a country's sovereignty and trust, and in part from the fact that virtual currencies, unlike "real" currencies, are issued in private transactions, are not widely recognized as legal tender, may have price volatility and generally have no intrinsic value.

While these arguments may be compelling for some more "traditional" crypto-assets (such as bitcoin) that fluctuate in value and are not backed by underlying assets, they do not apply nearly as neatly to so-called "stablecoins" that are backed by or linked to a set amount of fiat currency. Such crypto-assets would

[20] Proposals include the draft Markets in Crypto-Assets Regulation, Sept. 24, 2020, and the Financial Stability Board's "Crypto-Assets: Work Underway, Regulatory Approaches and Potential Gaps," May 31, 2019.

[21] The report acknowledges that certain crypto-assets may fit into more than one of the above categories or may share characteristics of multiple categories.

[22] *See* Notice 2014-21, 2014-16 I.R.B. 938, laying out the IRS' view. ("Under currently applicable law, virtual currency is not treated as currency that could generate foreign currency gain or loss for U.S. federal tax purposes.")

certainly have intrinsic value, at least to the extent that a holder is generally able to exchange the stablecoin for the underlying fiat currency. For the same reason, these assets would generally not bear price volatility beyond that of the underlying "real" fiat currency. Stablecoins may also become more and more widely recognized as legal tender over time; this is certainly often the intent of issuers of such crypto-assets. And if such assets begin to become widely accepted as a means of payment, it would seem that the sole justification (at least based on the arguments advanced in the report) for differentiating them from traditional currencies would be that they are issued by a private rather than a governmental entity.

The report acknowledges the unique nature of stablecoins and seems to encourage or at least set the stage for disparate treatment, noting in a later section that "as the stablecoin markets develop, tax policymakers may wish to consider giving more attention to the applicable tax rules, and whether these should vary depending on the nature of a stablecoin." Notably, a handful of jurisdictions (Belgium, the Ivory Coast, Italy and Poland) have indicated that virtual currencies should be taxed in a manner akin to foreign currency, contrary to the U.S. view.

After discussing the general characterization of crypto-assets, the report analyzes the manner in which jurisdictions tax transactions involving such assets for purposes of income tax, value-added tax (VAT) and property tax. While there are many distinctions and nuances among jurisdictions, which the report explores in some detail, the general themes highlighted include:

- There is significant divergence as to whether mining a new token is itself a taxable event (as under the U.S. approach), or whether the taxable event should occur only upon disposal of such token.
- A large majority of jurisdictions, like the United States, view an exchange of virtual currency for fiat, for other crypto-assets or for goods and services as a taxable event, though a handful of respondent countries (Chile, France, Latvia and Poland) indicated that they do not view an exchange for another crypto-asset as a taxable event.
- A small number of countries (Grenada, Italy, the Netherlands, Portugal and Switzerland) indicated that they do not view any exchange of virtual currency as a taxable event for individuals.
- For VAT purposes, an exchange of fiat currency for virtual currency, or vice versa, is generally exempt from VAT taxation. Supplies of goods or services paid for with virtual currency, however, may be subject to VAT in some jurisdictions. It is worth noting that this treatment derives in part from a 2015 European Court of Justice decision, which held that virtual currencies should generally be viewed and treated in the same manner as fiat currencies for purposes of applying the EU's VAT Directive.
- For countries that impose inheritance or estate taxes, or impose wealth taxes, virtual currencies are generally regarded as property and hence subject to such taxes.

The later portions of the report focus on particular challenges, including those posed by valuation, by the taxation of hard forks, by stablecoins (as noted above) and by digital currencies issued by central banks. After analyzing these issues, the report concludes with a list of recommendations for policymakers. The recommendations generally do not push for specific substantive conclusions on the issues presented, but rather flag considerations that jurisdictions should take into account.

Notable among the recommendations is to have clear, comprehensive guidance that is adapted or updated frequently as the market and technologies further develop. This recommended approach would seem to contrast with the U.S. approach to date, where one Notice from six years ago and a brief Revenue Ruling targeted solely at "forks" constitute the totality of the official guidance targeted at the tax treatment of crypto-assets.

Other Developments

New US Digital Asset Legislation Introduced

Securities Clarity Act

On September 24, 2020, Rep. Tom Emmer, R-Minn., introduced the Securities Clarity Act, a bill aimed at clarifying the legal and regulatory landscape around digital assets and the manner in which they are offered and sold. According to the bill, its purpose is "to clarify and codify that an asset sold pursuant to an investment contract, whether tangible or intangible (including an asset in digital form), that is not otherwise a security under the Act, does not become a security as a result of being sold or otherwise transferred pursuant to an investment contract."

Although the bill purports to refine the application of the *Howey* investment contract analysis to digital assets, the law before now has never treated underlying assets as securities simply because they were offered and sold pursuant to an investment contract. The bill nevertheless appears to be a reaction to the SEC's activity in this space, which, as SEC Commissioner Hester M. Peirce acknowledged earlier this year, has been criticized for eliding "the distinction between the token and

the investment contract." As Commissioner Peirce explained, a "'contract, transaction or scheme' by which the token is sold may constitute an investment contract; but, the object of the investment contract — the token — may not bear the hallmarks of a security. Conflating the two concepts has limited secondary trading and has had disastrous consequences for the ability of token networks to become functional."

The Securities Clarity Act is still in its initial stages but was drafted with input from expert legal practitioners and marks a noteworthy step toward mitigating the uncertainty around application of the *Howey* test to digital tokens. The bill holds open the possibility that a digital token may be a security in some circumstances but focuses the *Howey* inquiry on the token itself rather than the manner in which it might initially be sold. This approach could have favorable implications for blockchain projects that become more functional (and more "decentralized") over time, including where digital tokens do not independently meet the *Howey* test when divorced from their initial sale in connection with a capital-raising event.

In this regard, further clarity may still be needed regarding whether and under what circumstances a digital token may be deemed a security in its own right — a question that the Securities Clarity Act leaves for another day, possibly through other legislative efforts. One such possibility remains: legislative codification of Commissioner Peirce's safe harbor proposal or some version thereof.

Digital Commodity Exchange Act

On the same day that the Securities Clarity Act (see above) was introduced, Rep. Michael Conaway, R-Texas, introduced the Digital Commodity Exchange Act (DCEA), which proposes to create a single, opt-in federal regulatory scheme for digital asset trading platforms under the exclusive jurisdiction of the CFTC. The proposed framework, based on the regulatory model for traditional commodity exchanges, aims to remove major regulatory roadblocks for innovators in developing new digital asset projects and provide regulatory certainty in cash markets for digital assets while protecting retail consumers.

Digital asset trading platforms today are subject to a complex and uncertain web of state and federal regulations. At the state level, trading platforms must generally follow money transmitter rules that apply to the sale or exchange of digital assets in each state in which they operate. But not all states have rules that clearly apply to digital asset transactions and, to the extent they do, those rules are not necessarily identical or even comparable. At the federal level, digital asset trading platforms are potentially subject to numerous different regulatory schemes.

The DCEA aims to address these issues by (i) providing an option for digital asset trading platforms to register with the CFTC as a "digital commodity exchange" (DCE),[23] which would provide regulatory certainty by preempting regulation by any state or other federal authority, and (ii) allowing trading on DCEs of certain digital assets that would otherwise be subject to trading restrictions under federal securities laws.

A DCE would be subject to exclusive and comprehensive regulatory oversight by the CFTC and permitted to list for trading any digital commodity[24] that is "not readily subject to manipulation," among other conditions. Similar to the CFTC's regulation of trading facilities in traditional commodity markets (known as designated contract markets), a DCE would be subject to principles-based registration requirements. This means that a DCE would need to comply with 14 core principles that address, for example, monitoring of trading activity, prohibition of abusive trading practices, minimum capital requirements, public reporting of trading information, conflicts of interest, governance standards and cybersecurity.

Each DCE would be required to segregate customer assets in its possession and entrust them with a "qualified digital commodity custodian" that would be regulated by a state, federal or international banking regulator, subject to minimum regulatory standards set by the CFTC. This requirement is intended to provide another layer of protection for retail customers, similar to the segregation requirements applicable to the trading regime in traditional commodity markets.

Importantly, DCE registration would be an option, not a requirement, for digital commodity trading platforms. Registration does not mean, however, that the CFTC would be the only regulator for all digital commodity transactions. The DCEA explicitly provides that relevant state and federal regulators would retain their jurisdiction over custodial or depository activities for a digital asset, or any promise or right to a future digital asset, and that entities raising money for a digital commodity project may be subject to securities laws.

The DCEA also proposes to provide a regulatory safe harbor of sorts for certain digital assets obtained through ICOs. Under the DCEA's approach, retail customers could trade digital assets initially offered through an ICO on a DCE subject to CFTC

[23] The DCEA defines a DCE as "a trading facility that lists for trading at least one digital commodity."

[24] The DCEA defines "digital commodity" as "any form of fungible intangible personal property that can be exclusively possessed and transferred person to person without necessary reliance on an intermediary, and which does not represent a financial interest in a company, partnership, or investment vehicle." "Digital commodity" would thus include cryptocurrencies, such as bitcoin and ether, and many other forms of digital assets.

regulation. The DCEA defines the delivery or promise of a digital commodity in exchange for participating in a securities offering or investment contract under federal securities laws as a "digital commodity presale." The digital asset obtained through the presale would remain subject to trading restrictions on securities under federal securities laws, unless the asset meets the DCEA's definition of digital commodity.

If the digital asset obtained through the presale qualifies as a digital commodity, transactions involving that asset would be permitted in the following instances:

- on a registered DCE;
- with another person who would have been eligible for the original securities offering;
- to utilize the digital asset for its intended purpose; or
- under a limited CFTC-provided public interest exemption.

Before listing any digital commodity for trading, a DCE would be required to determine that the digital commodity is "not readily susceptible to manipulation" by considering the digital commodity's (i) purpose and use, (ii) governance structure, (iii) participation, (iv) distribution, (v) intended, current and proposed functionality, (vi) other relevant factors determined by the exchange, and (vii) any other factor required by the CFTC. The DCEA would also add certain safeguards for retail customers' digital commodity transactions.

As with the proposed Securities Clarity Act, it remains to be seen whether this bill will become law. But regardless of whether it does, the introduction of the bill itself will likely spark more discussions and suggestions on how to improve the current regulatory landscape for cash markets in digital assets and for innovators of digital asset projects.

Contacts

Gary DiBianco
Partner / Washington, D.C.
202.371.7858
gary.dibianco@skadden.com

Alexander C. Drylewski
Partner / New York
212.735.2129
alexander.drylewski@skadden.com

Eytan J. Fisch
Partner / Washington, D.C.
202.371.7314
eytan.fisch@skadden.com

Nathan W. Giesselman
Partner / Palo Alto
650.470.3182
nathan.giesselman@skadden.com

Stuart D. Levi
Partner / New York
212.735.2750
stuart.levi@skadden.com

Jessie K. Liu
Partner / Washington, D.C.
202.371.7340
jessie.liu@skadden.com

Peter B. Morrison
Partner / Los Angeles
213.687.5304
peter.morrison@skadden.com

Simon Toms
Partner / London
44.20.7519.7085
simon.toms@skadden.com

Jonathan Marcus
Of Counsel / Washington, D.C.
202.371.7596
jonathan.marcus@skadden.com

Jeongu Gim
Associate / Washington, D.C.
202.371.7223
jeongu.gim@skadden.com

Daniel B. O'Connell
Associate / Washington, D.C.
202.371.7003
daniel.oconnell@skadden.com

Kasonni Scales
Associate / Los Angeles
213.687.5657
kasonni.scales@skadden.com

Skadden, Arps, Slate, Meagher & Flom LLP
One Manhattan West
New York, NY 10001
212.735.3000

skadden.com