Katten

Financial Markets and Regulation

2020 Year-End Crypto Assets Legal and Regulatory Developments:

It Wasn’t Just Bitcoin Breaking $29,000 (It’s Even Higher Now)!

Gary DeWaal, Chair, Financial Markets and Regulation
Carl Kennedy, Partner, Financial Markets and Regulation

January 21, 2021

Table of Contents

I. SEC, CFTC and OCC Guidance 3

SEC – Statement regarding Special Purpose Broker-Dealers Eligible to Custody Digital Asset Securities (Statement) 3

CFTC – Advisory on Virtual Currency for Futures Commission Merchants 6

OCC – National Banks Authorized to Participate in Independent Node Verification Networks and Use Stablecoins for Payment Activities 8

II. Decisions/Settlements in SEC, CFTC and OFAC Enforcement Matters 10

SEC v. Kik Interactive Inc.: 10

CFTC v. Monex Credit Company et al 14

OFAC/BitGo, Inc. – Settlement 17

III. Pending CFTC, SEC Material Litigation 18

CFTC v. HDR Global Trading Limited et al (BitMEX) 18

SEC v. Ripple Labs, Inc. et al 20

IV. Miscellaneous Developments 23

FinCEN Proposed Rule Aimed at Closing AML Regulatory Gaps 23

Attorney General's Cyber Digital Task Force – Cryptocurrency Enforcement Framework 25

FCA – Prohibiting the Sale to Retail Clients of Investment Products That Reference Cryptoassets 25

1. SEC, CFTC and OCC Guidance

SEC – Statement regarding Special Purpose Broker-Dealers Eligible to Custody Digital Asset Securities (Statement): https://www.sec.gov/rules/policy/2020/34-90788.pdf

- On December 23, 2020, the Securities and Exchange Commission (SEC) said that, for a five-year period, it would not take enforcement action against a special purpose broker-dealer (SPBD) on the basis that the SPBD "deems itself to have obtained and maintained physical possession or control of customers' fully paid for digital asset securities" subject to certain enumerated conditions—namely, that the SPBD:

    1. has access to the digital asset securities and has the capability to transfer them on the relevant blockchain;
    2. limits its business to effectuating transactions in, maintaining custody of or operating an alternative trading system for digital asset securities with limited exceptions for handling traditional securities for certain enumerated proprietary purposes;
    3. establishes, maintains and follows policies and procedures requiring it to:
        - conduct and document whether each digital asset security it offers is offered pursuant to an effective registration statement or an available exemption from registration and that the SPBD can effect transactions in the relevant security;
        - evaluate the characteristics of each relevant blockchain, including, among other things, its scalability, resiliency, security, and governance;
        - maintain exclusive control over each digital asset security consistent with "industry best practices to protect against the theft, loss, and unauthorized and accidental use of the private keys";
        - identify in advance steps it will take in response to (i) events that could affect its exclusive control over each digital asset security, (ii) a court ordered freeze or seizure, or (iii) a need to transfer digital asset securities to another SPBD in case it can no longer continue in business;
    4. does not try to maintain custody if the SPBD is concerned with the relevant blockchain's security;
    5. provides written disclosures to prospective customers regarding certain enumerated risks of digital asset securities and explaining that it will consider itself in possession or control of each digital asset security; and
    6. enters into a written agreement with each customer covering certain relevant matters.

- The SEC also requested responses to seven questions (Request) by 60 days after publication of the Statement in the *Federal Register*.

- **Observations**

1. An SPBD must comply with all traditional requirements of a broker-dealer (BD), including financial responsibility rules, obligations under the Bank Secrecy Act and obligation to be a member of the Financial Industry Regulatory Authority (FINRA).
2. Traditional BD business must be conducted through a traditional BD.
3. The SEC does not at this time contemplate a SPBD accepting stablecoins or any other non-security digital assets for payment of digital asset securities because they are not expressly covered by the SEC's customer protection rule, SEC Rule 15c3-3: https://www.sec.gov/rules/policy/2020/34-90788.pdf. However, in its Request, the SEC expressly asks for comment on the question "Should [the SEC permit] the use of non-security digital assets as a means of payment for digital asset securities, such as by incorporating a *de minimis* threshold for non-security digital assets?"
4. In a liquidation of an SPBD, customers holding digital asset securities may be treated as general creditors and not preferred creditors if the securities are not deemed securities as defined under the Securities Investor Protection Act (e.g., non-registered "investment contracts" under *SEC v. W.J. Howey Co.*: https://supreme.justia.com/cases/federal/us/328/293/).
5. There has been no guidance yet issued by FINRA regarding the new member application process for an SPBD.
6. The Statement followed the September 25, 2020 No-Action Letter (NAL) issued by the SEC's Division of Trading and Markets (T&M) to FINRA regarding an alternative trading system's (ATS) role in the settlement of digital asset security trades: https://www.sec.gov/divisions/marketreg/mr-noaction/2020/finra-ats-role-in-settlement-of-digital-asset-security-trades-09252020.pdf.

SEC – Statement regarding Special Purpose Broker-Dealers Eligible to Custody Digital Asset Securities (Statement): (Cont'd)

- In the NAL, SEC T&M staff indicated that a three-step process proposed by several BDs handling digital asset securities would not result in the recommendation of an enforcement action:
    i. a buyer and seller submit their orders to an ATS, notify their respective custodians of their respective orders, and instruct their respective custodians to settle transactions pursuant to the terms of their orders when the ATS notifies the custodians of a match;
    ii. the ATS matches the order; and
    iii. the ATS notifies the buyer and seller and their respective custodians of the matched trade and the custodians carry out the conditional instructions.
- BDs operating ATSs seeking to take advantage of this relief would:
    i. not guarantee or otherwise have responsibility for settling trades. This would be "clearly stated" in agreements between the BD and its customers;
    ii. not at any time exercise any level of control over the digital asset securities being sold or cash being used to make the purchase;
    iii. maintain minimum capital of US $250,000;
    iv. establish, maintain and follow policies and procedures requiring it to conduct and document whether each digital asset security it offers is offered pursuant to an effective registration statement or an available exemption from registration and whether any secondary transactions of a digital asset security are made pursuant to an effective registration statement or an available exemption from registration; and
    v. ensure the transactions in digital asset securities otherwise comport with federal securities laws.

- The NAL built upon the July 8, 2019 Joint Staff Statement on Broker-Dealer Custody of Digital Asset Securities by T&M and FINRA's Office of General Counsel: https://www.sec.gov/divisions/marketreg/mr-noaction/2020/finra-ats-role-in-settlement-of-digital-asset-security-trades-09252020.pdf.

CFTC – Advisory on Virtual Currency for Futures Commission Merchants(Advisory): https://www.cftc.gov/csl/20-34/download

- On October 21, 2020, the then Division of Swap Dealer and Intermediary Oversight (now the Market Participants Division) of the Commodity Futures Trading Commission (CFTC) issued an Advisory on how a futures commission merchant (FCM) could hold for customers virtual currency underlying a physicallydelivered futures contract (or option thereon) or swap cleared through a derivatives clearing organization (DCO).[1] To address the risks of virtual currencies, FCMs desiring to hold virtual currencies as specially protected "customer funds":

    1. must hold such funds only with a bank, a trust company, another FCM or a DCO that clears derivatives on the relevant virtual currencies in an account that clearly identifies the account as holding customer funds and states they are "segregated" as required by the Commodity Exchange Act (CEA) and CFTC regulations. The FCM must also obtain an appropriate written acknowledgment letter from each depository (not from a DCO, however);
    2. must reflect the virtual currency on its daily and month-end segregation statements at fair market value in US dollars reflecting the FCM's "reasoned judgment" based on spot market or other "appropriate market transactions";
    3. may not offset a debit or deficit in a futures or cleared swaps customer account by the value of any virtual currency held in the same account. However, if a customer defaults for any reason, the FCM may use any virtual currency held for the customer to cover the default;
    4. may not deposit its own virtual currencies in any futures or cleared swaps customer segregated account for any reason, including to meet targeted or residual interest requirements; and
    5. may not invest any segregated futures or cleared swaps customer funds in virtual currencies.

- Any virtual currencies held at a Depository for futures or cleared swaps customers must be available on demand by the FCM. Each withdrawal of virtual currencies from a depository should be completed within a time that is "technologically and operationally possible" but ordinarily longer than one day.

[1] The Advisory noted it was not addressing virtual currency held by FCMs for customers trading futures (or options thereon) on non-US markets.

- FCMs must also limit acceptance of virtual currency:

    1. into segregated futures or cleared swaps customer accounts to virtual currencies that are subject to cleared physical delivery derivatives and are an acceptable form of collateral for such contracts by the relevant DCO; and
    2. to an amount for each customer that "reasonably relates" to the customer's level of trading in the relevant derivatives during each calendar quarter. This correlation must be documented in the FCM's books and records pursuant to its risk management policies and procedures.

- An FCM must contact a customer to initiate a return of virtual currency if the customer has stopped trading the relevant derivatives contracts and there are no open derivatives contracts. The notice and return must occur within 30 days after the customer has ceased trading for 90 days.
- Prior to accepting virtual currency into segregation, an FCM should provide at least 45 days' advance written notice to all its futures and cleared swaps customers that it will begin accepting virtual currencies as margin as of a designated date.

- **Observations**

    1. A single FCM can hold both traditional futures and cleared swaps and physically deliverable futures and cleared swaps for its customers and use the virtual currencies as collateral for the customers' related physically deliverable futures and cleared swaps open positions or hold the virtual currencies for a limited period of time for customers without related positions.
    2. The CFTC contemplates that an FCM may hold customer virtual currencies in wallets it establishes for customers; however, it would have to demonstrate that it could satisfy the CFTC's segregation requirements "including retaining the appropriate possession and control of the virtual currencies and the safeguarding of the virtual currencies."

OCC – National Banks Authorized to Participate in Independent Node Verification Networks and Use Stablecoins for Payment Activities: https://www.occ.gov/news-issuances/news-releases/2021/nr-occ-2021-2.html

- On January 4, 2021, the Office of Comptroller of the Currency (OCC) said in an Interpretive Letter that national banks and federal savings associations (Banks) may validate, store and record payment transactions on independent node verification networks (INVN) such as blockchains and use stablecoins to engage in payment activities and other bank-approved activities.
    1. A stablecoin is a type of virtual currency designed to have a stable value compared to other types of virtual currency. Some stablecoins are pegged to the US dollar, but others may be designed to achieve a stable value by being pegged to other fiat currencies, virtual currencies, commodities or assets, or by being algorithmically stabilized.
    2. Under the Interpretative Letter, Banks may buy, sell or issue stablecoins, and exchange an issued stablecoin for fiat currency.
    3. Banks must conduct the approved activities in accordance with applicable law and "safe and sound banking practices." They need to be aware of potential risks, including operational risk, compliance risk (e.g., money laundering), and fraud risk. In particular, stablecoin arrangements "should have the capability to obtain and verify the identity of all transacting parties, including those using unhosted wallets." (The OCC quoted from the President's Working Group on Financial Markets Statement on Key Regulatory and Supervisory Issues Relevant to Certain Stablecoins (December 23, 2020: https://home.treasury.gov/system/files/136/PWG-Stablecoin-Statement-12-23-2020-CLEAN.pdf.))
    4. Banks issuing stablecoins also should have strong reserve management practices to ensure a 1:1 reserve ratio and sufficient financial resources to deal with losses and meet liquidity needs.
    5. Prior to engaging in the approved activities, Banks should consult with their OCC supervisors.

- **Observations**
    1. The OCC has been active in 2020, and so far in 2021, in accommodating virtual currency use by Banks under Acting Comptroller Brian Brooks. However, Mr. Brooks resigned as Acting Comptroller on January 14, 2021.

OCC – National Banks Authorized to Participate in Independent Node Verification Networks and Use Stablecoins for Payment Activities: (Cont'd)

2. For the OCC, the January Interpretative Letter providing for use of INVNs and stablecoins was materially the same as allowing for the use of debit cards, checks and electronically stored value systems.
3. Previously in 2020, OCC authorized Banks to:
   - hold reserves on behalf of customers who issued stablecoins (September 21, 2020: https://www.occ.gov/topics/charters-and-licensing/interpretations-and-actions/2020/int1172.pdf); and
   - conduct cryptocurrency custody services, including holding unique cryptographic private keys, on behalf of customers and provide any permissible banking services to any lawful businesses, including cryptocurrency businesses (July 22, 2020: https://www.occ.gov/topics/charters-and-licensing/interpretations-and-actions/2020/int1170.pdf).
4. In addition, on January 13, 2021, the OCC conditionally approved the application of Anchorage Trust Company of South Dakota (Anchorage Trust) to convert to a national trust bank under the name "Anchorage Digital Bank, National Association" subject to satisfaction of a number of enumerated conditions.
   - Anchorage Trust engaged in the custody of digital assets and fiat currency and provided governance, staking and settlement services.
   - As a national bank, the bank will engage in the same fiduciary activities. It will limit its activities to the operations of a trust company and related activities, and will engage in no activities causing it to be considered a "bank" under the Bank Holding Company Act: https://www.occ.gov/news-issuances/news-releases/2021/nr-occ-2021-6a.pdf.

II. Decisions/Settlements in SEC, CFTC and OFAC Enforcement Matters

SEC v. Kik Interactive Inc.:
https://law.justia.com/cases/federal/district-courts/new-york/nysdce/1:2019cv05244/516941/88/

- On September 30, 2020, the Hon. Alvin K. Hellerstein of the US District Court for the Southern District of New York held that Kik Interactive Inc. (Kik) offered and sold securities without a registration statement or exemption from registration in violation of Section 5 of the Securities Act of 1933 (Securities Act) (https://www.law.cornell.edu/uscode/text/15/77e). He ruled on cross-motions for summary judgment filed by both parties in response to an initial SEC enforcement action against Kik on June 4, 2019.
- **Background (as set forth in the Court Opinion and Order)**

1. Kik determined to develop a virtual currency — “Kin” — on the Ethereum blockchain that could be used to buy and sell digital products through many applications, including applications not run by Kik.
2. In connection with this, Kik staged a private offering from June 2017 through September 11, 2017, and a public offering beginning September 12, 2017, termed by Kik a “token distribution event” (TDE).
    - The private offering was effectuated by Kik entering into simple agreements for future tokens (SAFTs) for Kin with 50 sophisticated persons and receiving US $50 million in exchange. These investors bought Kin at a 30 percent discount and expected to receive 50 percent of their Kin tokens at the time of the network launch and 50 percent one year later. These investors also acknowledged in their SAFTs that their right to acquire Kin was a security and not registered with the SEC.
    - During the TDE, approximately 10,000 persons purchased Kin in exchange for ether worth US $49.2 million.
    - One trillion Kin were distributed to private and public purchasers of Kin on September 26, 2017. Additionally, Kik retained three trillion Kin and six trillion Kin were provided to the Kik Foundation, a not-for-profit entity created by Kik.
3. According to the Court, “As of …September 26, 2017, no goods or services were available for sale to holders of Kin. They had only Kik’s ‘Minimum Viable Product,’ that is a digital wallet showing the holder’s balance, and digital stickers of undefined use or purpose.”

    4. Kik used the proceeds from its public and private sale to develop the Kin ecosystem and other projects.

- Applying the *Howey* tests (https://supreme.justia.com/cases/federal/us/328/293/), the Court held that Kik's sale of Kin to the TDE purchasers involved an (i) investment of money (ii) in a common enterprise (iii) with the expectation of profits solely from the efforts of the promoter or a third party and thus constituted an investment contract (i.e., a security). According to the Court,

    1. Kik conceded the TDE involved in an investment of money;
    2. Kik established a common enterprise. It deposited all funds received from purchasers in a single bank account and used the funds for its operations; and
    3. TDE purchasers had a reasonable expectation of profits through the efforts of Kik.
        - It was not relevant that the form of the profits would be appreciation in the value of Kin rather than a distribution of profits.
        - Among other things, Kik's CEO in public statements "extolled" Kin's profit-making potential. He noted that Kik was offering only a limited amount of Kin, so as demand increased, its value would increase, benefitting early purchasers.

- The Court rejected Kik's argument that, because Kin was intended to be a medium for consumptive use, it was not an investment contract. The Court said that "none" of Kin's supposed consumptive use was available at the time of the TDE.
- The Court held that the presale and the TDE were part of a single integrated plan of financing and "made for the same general purpose." Proceeds from both were dedicated to operations. As a result, both the presale and TDE were sales to the general public and constituted an unregistered securities offering that did not qualify for an exemption under SEC Rule 506(c): https://www.law.cornell.edu/cfr/text/17/230.506.
    1. Moreover, said the Court, private-offering and TDE purchasers received the same class of securities.
    2. The timing of the presale and the TDE were so close they were "interdependent," held the Court.

- The Court rejected Kik's affirmative defense that the term "investment contract" was unconscionably vague, saying *Howey* provided "a clearly expressed test" and that an "extensive body of case law" has interpreted *Howey* in connection with varied fact patterns.

- **Observations**

1. The SEC's Report of Investigation related to the DAO, setting forth the SEC's views that DAO token sales to the public constituted sales of investment contracts, was published after Kik announced its plans for issuance of Kin on May 25, 2017, and commenced its presale. (The DAO report was issued on July 25, 2017: https://www.sec.gov/litigation/investreport/34-81207.pdf. *See also* the SEC Staff Statement of April 3, 2019, on "Framework for Investment Contract Analysis of Digital Assets": https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets.)
2. Following the Opinion and Order, Kik settled the SEC enforcement action against it by agreeing to pay a fine of US $5 million and, for three years, to provide notice to the SEC prior to engaging in enumerated future issuances, offers, sales and transfers of digital securities. Kik also was permanently enjoined from violation of registration provisions of the Securities Act.
3. As part of its settlement, Kik was not obligated to register its Kin tokens with the SEC or to return investors' money. This was the same approach the SEC took in connection with its September 30, 2019 settled charges against Block.one in connection with its initial coin offering/token distribution:
    - The SEC alleged that Block.one conducted an unregistered initial offering of 900 million ERC-20 tokens between June 2017 and June 2018 that raised in excess of "several billion dollars' worth of Ether." The token sale was meant to fund the development of the EOSIO software and the launch of EOSIO-blockchains, said the SEC.
    - The SEC claimed that the ERC-20 tokens were securities applying the *Howey* tests." Among other things, the SEC noted, the ERC-20 tokens were transferable on secondary marketplaces through the end of Block.one's ICO, and purchasers reasonably expected profits through the efforts of Block.one. At the end of the ICO, the ERC-20 tokens became fixed and not transferable; holders had to register their ERC-20 through a smart contract on the Ethereum blockchain to receive native EOSIO-based blockchain tokens (EOS).
    - The SEC and Block.one agreed to payment of a $24 million fine by Block.one to settle the SEC's allegations and agreed not to violate securities' registration requirements going forward.
    - There was no requirement for Block.one to register the ERC-20 or EOS tokens or buy-back tokens from initial investors.
4. The SEC's approach in settling against Kik was different than in settlements of most other alleged unregistered ICO-type actions, where the defendants were required to disgorge proceeds and/or disable or register the relevant digital assets, among other penalties. For

example, earlier in 2020, on March 24, in response to another SEC civil complaint, a different judge of the US District Court for the Southern District of New York — the Hon. P. Kevin Castel — enjoined Telegram Group Inc. and TON Issuer Inc. (Telegram) from distributing “Grams,” a new purported cryptocurrency, concluding that such a distribution would also constitute an unlawful, unregistered offering of securities (https://law.justia.com/cases/federal/district-courts/new-york/nysdce/1:2019cv09439/524448/227/). The SEC initially filed a complaint against Telegram on October 11, 2019. According to the Court:

- In 2018, Telegram sold interests in approximately 2.9 billion Grams to 175 entities and high-net-worth individuals in two rounds of sales from which it raised US $1.7 billion, including US $424.5 million from 39 US purchasers. It intended to deliver the Grams upon the launch of Telegram’s new blockchain, the Telegram Open Network Blockchain. The Grams sold as part of the first round would be subject to some resale restrictions at launch, but the Grams sold as part of the second round would be subject to no resale restrictions.
- Additionally, upon network launch, 4 percent of Grams were to be provided to four Telegram developers (including the two Telegram principals), 10 percent of Grams would be reserved for post-launch incentive programs, and other Grams would be allocated to a reserve pool that could end up being transferred to a foundation Telegram would set up — the TON Foundation (with the two Telegram principals serving on its board). Telegram promoted that the TON Foundation had the power to support the market price of Grams.
- Telegram used the proceeds of its alleged private sale to develop the TON blockchain and Grams, as well as to maintain and expand Telegram Messenger.
- Telegram argued that its initial private sales constituted lawful private placements exempt from registration. It also argued that the proposed distribution of Grams in a “wholly-unrelated transaction” would not constitute an offering of securities. The SEC claimed that the initial purchasers were underwriters, and that the initial sale and proposed redistribution of Grams were an integrated transaction that would constitute an unlawful public sale of securities.
- The Court, applying *Howey*, found “an implicit (though formally disclaimed) intention on the part of Telegram to remain committed to the success of the TON Blockchain post-launch.” For this and other reasons, it found each of the *Howey* tests satisfied and that Grams were securities.
- Following the Opinion and Order, Telegram settled with the SEC by agreeing to return more than $1.2 billion to investors and to pay an $18.5 million fine. Telegram also agreed, for the next three years, to give notice to the SEC prior to participating in the issuance of any digital securities

CFTC v. Monex Credit Company et al.

8:17-cv-01868-JVS-DFMx (December 28, 2020)

- On December 28, 2020, the Hon. James V. Selna of the US District Court of the Central District of California granted the CFTC a preliminary injunction against Monex Credit Company (Monex), ordering the firm to cease offering leveraged retail commodity transactions as part of its “Atlas” program. Although this action involved Monex’s leveraged trading program for precious metals, it entailed analysis of a CEA provision that also applies to certain leveraged, margined, or financed transactions involving other commodities (including virtual currencies) to non-eligible contract participants where actual delivery of the relevant commodity does not occur within 28 days. *See* 7 U.S.C. § 2(c)(2)(D)(ii)(III)(aa): https://www.law.cornell.edu/uscode/text/7/2.

  1. The CFTC initially filed its enforcement action against Monex in September 2017. The CFTC alleged that, in connection with the Atlas program’s precious metals transactions, retail clients purchased and sold precious metals, paid only a portion of the purchase price, and either borrowed the difference (for purchases) or borrowed the metal (for sales). Although Monex delivered customers' precious metals to an independent warehouse and transferred title to the customers, it retained control over the commodities to protect itself in case a customer defaulted on his/her repayment or margin obligations.
  2. The CFTC charged that these leveraged purchases and sales to retail clients constituted prohibited off-exchange futures contracts, and that Monex operated as an FCM without required registration. In making this claim, the CFTC relied on provisions of law that require all contracts for commodities for future delivery to be executed on or be subject to the rules of a DCM and offered and sold through a licensed broker (e.g., an FCM). *See* 7 U.S.C. § 2(c)(2)(D(i)): https://www.law.cornell.edu/uscode/text/7/2l; 7 U.S.C. § 6(a)(1): https://www.law.cornell.edu/uscode/text/7/6; and 7 U.S.C. § 6d(a)(1): https://www.law.cornell.edu/uscode/text/7/6d.
  3. Although the CFTC conceded these requirements did not apply to outright sales of commodities to retail persons, it said the requirements apply when the sales are financed or on leverage and a firm retains control over its customers' commodities beyond 28 days – even if to protect itself in connection with its financing – because actual delivery has not occurred within 28 days. See 7 U.S.C § 2(c)(2)(D)(ii)(III)(aa).
  4. In its first substantive opinion on the CFTC’s action, the Court dismissed the CFTC’s complaint, claiming, among other things, that actual delivery of precious metals in financed transactions to retail persons falls outside the CFTC’s authority when ownership of real metals is legally transferred to such persons within 28 days — the so-called “Actual Delivery Exception” — even if the seller retains control over the commodities because of financing

beyond 28 days. *See* "California Federal Court Dismissal of CFTC Monex Enforcement Action Upsets Stable Legal Theories" by Gary DeWaal, *Bridging the Week* (May 6, 2018): https://bridgingtheweek.com/Commentary/PrintCommentary/2513.

5. The Ninth Circuit Court of Appeals overturned the District Court's opinion. Monex claimed that the relevant CEA provision would have no practical meaning if "actual delivery" required possession or control by a customer "because such a reading would clash with 'margin,' which means 'cash or collateral required to be paid to a securities broker by an investor to protect the broker against losses from securities bought on credit.'" However, the appeals court rejected this view, writing that "[w]hile permitting customers to obtain significant control over or possession of metals might be practically difficult here, that fact does not displace the statute's plain meaning." *See* "Federal Appeals Court Upholds Expansive CFTC View of Prohibition Against Manipulative or Deceptive Device and Restrictive View of Actual Delivery" by Gary DeWaal, *Bridging the Week* (July 28, 2019): https://www.bridgingtheweek.com/Commentary/PrintCommentary/2569.

- Applying the Ninth Circuit decision and the record before it, the Court, in the instant decision, determined that the CFTC would likely prevail on the merits of its claim that Monex failed to make actual delivery of its metals in connection with its Atlas program. According to the Court:
  1. although customers of Monex can use any of three depositories chosen by Monex, only Monex and not the customers have a contractual relationship with the depositories, even though Monex has no affiliation with the depositories. The customers do not have an effective choice;
  2. although customers of Monex receive title transfer to metals at the depositories, it is not "actual delivery." Monex maintains a control over the metals that is "inconsistent with the metals ever changing hands"; and
  3. Monex may liquidate a customer's entire portfolio should certain circumstances arise (e.g., the value of the portfolio declines below Monex's equity requirement) and may sell off with or without notice to a customer "the whole or any part of the Collateral," and a customer must obtain Monex's prior approval before moving any collateral from any depository. As a result "the absence of any meaningful customer control does not meet the test for 'at least some degree of possession or control by the customer'" (citing the Ninth Circuit opinion).

- The Court said its determination was in accord with two CFTC releases relating to actual delivery:
  1. the 2013 interpretation regarding retail commodity transactions (Commodity Guidance) under the CEA (https://www.govinfo.gov/content/pkg/FR-2013-08-23/pdf/2013-20617.pdf); and

2. the 2020 interpretive guidance regarding retail commodity transactions involving certain digital assets (Virtual Currency Guidance) under the CEA (https://www.govinfo.gov/content/pkg/FR-2020-06-24/pdf/2020-11827.pdf). In this guidance, the CFTC said that actual delivery occurs for virtual currency when a customer obtains:
   - "[p]ossession and control of the entire quantity of the commodity, whether it was purchased on margin, or using leverage, or any other financing arrangement; and
   - the ability to use the entire quantity of the commodity freely in commerce (away from any particular execution venue) no later than 28 days from the date of the last transaction;" as well as when
   - the offeror or counterparty seller does "not retain any interest in, legal right, or control over the commodity."

- The Court concluded that, not only is the CFTC likely to win on its claim that Monex's Atlas program does not satisfy the actual delivery exception of the CEA, but because of that, the CFTC is likely to prevail on its claim that Monex's transactions should be conducted on a DCM, and that the firm is likely to continue its violations.
- The Court rejected Monex's claims that imposing a preliminary injunction would violate Monex's due process rights.
- **Observations**
  1. The Commodity Guidance and the Virtual Currency Guidance are materially consistent, except that the Virtual Currency Guidance contemplates the possibility that a customer's virtual currency could be held at a depository that is an affiliate of the offeror (as agent for the customer), provided that certain enumerated conditions are met, including that the depository is (i) a separate legal entity from the offeror and any offeror execution platform; (ii) "predominantly operated for the purpose of providing custodial services for virtual currency or other digital assets;" and (iii) is licensed to conduct such custodial activities.
  2. In its initial decision, the Court did not accept the Commission's view that Monex's leveraged metals transactions were like futures contracts and thus subject to provisions of law that imposed registration requirements on brokers of such contracts. The CFTC had claimed that, although Monex transferred physical metals to independent depositories for the account of the retail clients, its retention of control over the precious metals negated that it made actual delivery of the commodities. However, said the court, if this view was correct, "every financed transaction would violate Dodd-Frank… and the result would be to eliminate the Actual Delivery Exception from the [relevant law]." The Ninth Circuit's dismissal of this argument seems cavalier. However, on June 29, 2020, the Supreme Court denied hearing Monex's appeal of the Ninth Circuit's opinion: https://www.cftc.gov/PressRoom/PressReleases/8192-20
  3. The Court's instant Order was temporarily stayed until January 19, 2021.

OFAC/BitGo, Inc. – Settlement
https://home.treasury.gov/system/files/126/20201230_bitgo.pdf

- On December 30, 2020, the Department of Treasury's Office of Foreign Assets Control (OFAC) announced it had entered into a settlement with BitGo, Inc. (BitGo) related to 183 alleged violations of multiple sanction programs by BitGo from approximately March 10, 2015 through December 11, 2019, in connection with its processing of digital currency transactions. BitGo agreed to pay a fine of $98,830 to resolve its potential civil liability.
    1. According to OFAC, during the relevant time, BitGo did not prevent persons located in Cuba, Iran, Sudan, Syria and the Crimea region of Ukraine from utilizing its "hot-wallet" non-custodial secure digital wallet management services. OFAC claimed that BitGo had reason to be aware of the sanctioned locations of the relevant users because of the Internet Protocol (IP) address data associated with devices they used to access the BitGo platform. However, during the relevant time, BitGo did not have controls to prevent access by such users although it used the IP addresses for security purposes related to account logins.
    2. OFAC also claimed that BitGo did not self-report its violations.
    3. According to OFAC, BitGo adopted an OFAC sanctions compliance program in January 2020 and implemented "significant remedial measures," including IP address blocking and email restrictions for sanctioned jurisdictions.
- **Observations**
    1. As part of its settlement release, OFAC noted that "[c]ompanies that facilitate or engage in online commerce or process transactions using digital currency are responsible for ensuring that they do not engage in transactions prohibited by OFAC sanctions, such as dealings with blocked persons or property, or engaging in prohibited trade or investment-related transactions."
    2. Decentralized applications (dApp), to the extent they are deemed a US person, would be expected to comply with OFAC sanctions. Could a dApp be deemed a US person?

CFTC v. HDR Global Trading Limited et al (BitMEX)
https://www.cftc.gov/media/4886/enfhdrglobaltradingcomplaint100120/download

USA v. Arthur Hayes, Benjamin Delo, Samuel Reed and Gregory Dwyer

https://www.justice.gov/usao-sdny/press-release/file/1323316/download

- On October 1, 2020, the CFTC announced the filing of a civil complaint in the federal court in the Southern District of New York against five entities (including HDR Trading Limited) and three individuals (Arthur Hayes, Ben Delo and Samuel Reed) that own and operate the BitMEX trading platform. The CFTC charged that BitMEX failed to register as a designated contract market (DCM) or swap execution facility (SEF), as well as an FCM, and failed to implement various anti-money laundering (AML) procedures, as required, under the Bank Secrecy Act (BSA).
- On the same day, the US Department of Justice separately indicted the same three individuals (arresting one, Mr. Reed) and one additional executive of BitMEX, claiming they caused a financial institution to violate the BSA by not establishing, implementing and following a required AML program.
- Although most of the BitMEX enterprises were organized outside the United States, the CFTC alleged that BitMEX conducted a significant portion of its business and maintained a significant presence in the United States.
- The CFTC alleged that, from November 2014 to the present, the BitMEX enterprises have:
    1. offered off-exchange commodity futures and options products on virtual currencies to US persons that were not eligible contract participants in violation of applicable provisions of the CEA and CFTC rules. According to the CFTC, “BitMEX offers the leveraged trading of cryptocurrency derivatives; BitMEX does not actually deliver the cryptocurrencies whose prices underlie the various contracts and transactions BitMEX offers”;
    2. acted as an unregistered FCM;
    3. operated a facility for the trading or processing of swaps without having registered as a DCM or SEF;
    4. failed to supervise as required for certain CFTC registrants (e.g., FCMs); and
    5. failed to comply with applicable provisions of the BSA. The CFTC claimed that BitMEX did not implement “know your customer” or customer identification program as required under the CFTC rules for FCMs.

- The CFTC claimed that the principals of BitMEX were aware of regulatory requirements applicable to financial institutions like FCMs "but made conscious decisions …to avoid and evade them."
- The CFTC also charged that Messrs. Hayes, Delo and Reed controlled and operated BitMEX as a "common enterprise."
- The indictment by the DOJ charged the four defendants with violating the BSA and conspiracy to violate the BSA in connection with their roles in causing BitMEX, as an FCM, to violate the BSA.
- BitMEX has filed no answers or substantive motions as of January 17, 2021, in response to the CFTC's and the DOJ's legal proceedings; it has issued the following statement, in part:

  "We strongly disagree with the U.S. government's heavy-handed decision to bring these charges, and intend to defend the allegations vigorously. From our early days as a start-up, we have always sought to comply with applicable U.S. laws, as those laws were understood at the time and based on available guidance.

  In the meantime, the BitMEX platform is operating as normal and all funds are safe."

  For BitMex's complete statement see: https://blog.bitmex.com/united-states-cftc-doj-filing/.
- **Observations**
  1. The CFTC's rule dealing with an obligation to supervise, CFTC Rule 166.3, applies on its face solely to CFTC registrants: https://www.law.cornell.edu/cfr/text/17/166.3. The CFTC charged that "BitMEX is and has been acting as an FCM, and therefore [the relevant rule] applies to BitMEX, as if it were a Commission registrant." This is an aggressive approach.
  2. Compare and contrast this with the CFTC's BSA charge that relies on CFTC Rule 42.2: https://www.law.cornell.edu/cfr/text/17/42.2. This provision also applies on its face to every FCM and introducing broker. However, the definition of an FCM under the CFTC's rules includes any person that is registered as an FCM or any individual or entity that performs functions of an FCM. See the definition of FCM in 17 C.F.R. Part 1: https://www.law.cornell.edu/cfr/text/17/part-1.

SEC v. Ripple Labs, Inc. et al.

https://www.sec.gov/litigation/complaints/2020/comp-pr2020-338.pdf

- On December 22, 2020, the SEC filed a civil complaint against Ripple Labs, Inc. (Ripple), as well as Bradley Garlinghouse (Garlinghouse), Ripple's current chief executive officer, and Christian Larsen (Larsen), Ripple's current executive chairman of the firm's board of directors. The SEC claims that, since 2013, the firm and the individual defendants have engaged in unregistered sales of Ripple's XRP digital asset token. Specifically, the SEC claims, the defendants have sold over 14.6 billion units of XRP in exchange for cash or other consideration valued over US $1.38 billion.
- The SEC alleges that:
    1. Ripple engaged in this "illegal securities offering" despite receiving legal advice as early as 2012 from an "international law firm" that, under the circumstances, there was "some risk" that XRP could be considered an investment contract, and thereby a security and was unlikely to be regarded as a currency. Larsen, according to the SEC, was aware of this advice by at least 2012.
    2. Ripple used the US $1.38 billion it raised to fund operations without disclosing how it was doing so, how it was paying others to develop a use for XRP, or how it was maintaining secondary markets.
    3. Garlinghouse and Larsen organized Ripple's sales of XRP and personally profited US $600 million from their unregistered sales of XRP.
    4. Garlinghouse never disclosed his sales of XRP despite repeatedly stating publicly he was "very long" XRP, implying he expected the price of the digital asset to rise.
- According to the SEC:
    1. At the time the XRP Ledger was completed in December 2012, Larsen and another unnamed Ripple co-founder transferred 20 billion XRP to themselves and one agent. Larsen received 9 billion XRP. Ripple retained 80 billion XRP.
    2. Ripple began making unregistered offers and sales of XRP in August 2013.
    3. Ripple engaged in market sales both on the XRP ledger and on digital asset trading platforms. It also engaged in institutional sales, typically offering discounts. The institutional sales typically did not require any restrictions on resales other than short lockup periods. "By selling at a discounts to market prices, Ripple incentivized these buyers to seek to sell their XRP into the public markets in order to realize what was essentially a guaranteed profit."

4. Throughout the offering period, Garlinghouse and Larsen "undertook significant efforts to monitor, manage and impact the XRP trading markets, including the trading prices and volume of XRP." They also "were instrumental" in creating an XRP escrow to help place 55 billion to "secure speculative liquidity" and increase XRP volume and liquidity in the marketplace, and thus its price.
5. Relying on *Howey*, XRP is an investment contract and therefore a security subject to registration requirements.
    - Ripple employees said the purpose of XRP was speculative.
    - Ripple sold XRP as an investment into a common enterprise that included "significant entrepreneurial and managerial efforts," including to create a liquid market for XRP, which would in turn increase demand for XRP and therefore its price.
    - "From the onset of the Offering, Defendants publicly promised significant, meaningful entrepreneurial efforts with respect to XRP."
6. Not until mid-2018 did Ripple begin "earnestly" testing a product relying on XRP to help synthetically transfer fiat currency between jurisdictions — its On Demand Liquidty (ODL) product. ODL was commercially launched in October 2018.

- Ripple and the two individual defendants have not yet answered the SEC's complaint. They publicized their "Wells" submission submitted to the SEC's Division of Enforcement prior to the filing of the SEC complaint: https://ripple.com/wp-content/uploads/2020/12/Ripple-Wells-Submission-Summary.pdf. Among other things, Ripple claimed that:
    1. XRP is not an investment contract. It is a "bridge currency" that does not rely on Ripple's efforts for its functionality or price. It is like bitcoin which the SEC has said is not a security.
    2. Ripple does not control "anywhere near a supermajority of validators" on the XRP Ledger, and changes have been adopted "despite Ripple's dissent."
    3. XRP is used as a currency by approximately 150 third-party commercial and consumer applications.
    4. It would be "unprecedented" to bring a case against Ripple for XRP sales that occurred prior to publication of the DAO Report, as well as for circumstances where there are no contract or privity between a buyer and seller; the vast majority of Ripple trading has taken place on secondary markets, independent of Ripple. Moreover there is no "pooling" of proceeds from sales (either vertically or horizontally), as is required by *Howey*.
    5. Ripple's holdings do not convert XRP into an investment contract. Many entities own large amounts of commodities and "no one credibly argues that those substantial holdings convert those commodities or currencies into securities."

SEC v. Ripple Labs, Inc. et al.: (Cont'd)

- **Observations**

1. Numerous regulators have regarded XRP as a currency and not a security. For example:
   - XRP is greenlisted on the New York Department of Financial Services website as a coin approved for custody: https://www.dfs.ny.gov/apps_and_licensing/virtual_currency_businesses/virtual_currencies.
   - On May 5, 2015, FinCEN assessed a US $700,000 penalty against Ripple for acting as a money service business (MSB) without registration in connection with its selling of XRP and by failing to implement and maintain an adequate AML Program. FinCEN claimed this violated the BSA: https://www.fincen.gov/news/news-releases/fincen-fines-ripple-labs-inc-first-civil-enforcement-action-against-virtual.
     i. In its October 2020 "Cryptocurrency – Enforcement Framework" report, the US Department of Justice's Cyber Digital Task Force lauded its success working with FinCEN to penalize Ripple Labs in 2015 for facilitating transfers of "a virtual currency known as XRP" without registering as an MSB and failing to implement and maintain an adequate AML program: https://www.justice.gov/opa/pr/attorney-general-william-p-barr-announces-publication-cryptocurrency-enforcement-framework.
   - In March 2020, an affiliate of Ripple was granted an exemption from holding a license under Singapore's Payment Services Act ("PS Act") to provide digital token payment services through July 2020: https://www.mas.gov.sg/regulation/payments/entities-that-have-notified-mas-pursuant-to-the-ps-esp-r.
   - On January 13, 2021, the Japan Financial Services Agency said XRP was not a security: https://www.coindesk.com/japans-fsa-says-xrp-not-a-security-report.
2. Is it relevant that SEC staff, including its former chairperson, have stated that ether likely was once a security but is now a virtual currency?

   William Hinman: https://www.sec.gov/news/speech/speech-hinman-061418

   Jay Clayton: https://4actl02jlq5u2o7ouq1ymaad-wpengine.netdna-ssl.com/wp-content/uploads/2019/03/Budd-et-al-Digital-Tokens-ES157408-Response-002.pdf

   - Consider the terms of the Kik and Block.one settlements.

IV. Miscellaneous Developments

FinCEN Proposed Rule Aimed at Closing AML Regulatory Gaps:
https://public-inspection.federalregister.gov/2020-28437.pdf
https://home.treasury.gov/system/files/136/2020-12-18-FAQs.pdf
Extension of time for comment: https://www.govinfo.gov/content/pkg/FR-2021-01-15/pdf/2021-01016.pdf

- On December 18, 2021, FinCEN proposed amendments to existing rules that would require banks and registered MSBs to maintain certain records and/or report certain transactions to FinCEN involving convertible virtual currencies (CVC) or legal tender digital assets (LDTA). Generally:

  1. one or more transactions within a 24-hour period between a hosted wallet maintained for a customer and a non-hosted wallet (or hosted wallet in a jurisdiction identified by FinCEN) with value equal to or greater than $3,000 would require the financial institution to obtain and maintain records regarding the transaction (including transaction hash) and holder of the non-hosted wallet (including the counterparty's name and physical address), and verify and record the identity of its own customer.
     - Outgoing transactions should not occur prior to this information being obtained, and the required information should be obtained as soon as practicable after incoming transactions.
     - Additionally, financial institutions would have to implement policies "tailored to their respective business models" addressing what the institution would do if it could not obtain the required information (e.g., terminating its customer's account "in appropriate circumstances"); and
  2. one or more transactions within a 24-hour period between a hosted wallet maintained for a customer and a non-hosted wallet (or hosted wallet in a jurisdiction identified by FinCEN) with value equal to or greater than $10,000 would require the financial institution to report certain information to FinCEN regarding the transaction and the holder of the non-hosted wallet (or hosted wallet in a jurisdiction identified by FinCEN). This is in addition to complying with the recordkeeping requirements.
     - The reporting obligation would exist even if the user of the unhosted or otherwise controlled wallet is a customer for whom the financial institution holds a hosted wallet.

- FinCEN's proposed obligations would not apply to transactions between hosted wallets (unless otherwise covered).

FinCEN Proposed Rule Aimed at Closing AML Regulatory Gaps: (Cont'd)

- Initially, comments to FinCEN were due by January 4, 2021. However, FinCEN reopened the comment period on January 15, 2021, and agreed to accept comments through February 1, 2021, for comments regarding the proposed reporting requirements, and through March 1, 2021, for all other aspects of the rule.
- **Observations**
    1. These proposals are controversial. They generated at least 7,506 responses by January 8, 2021.
    2. As proposed by FinCEN, financial institutions might have to obtain more information regarding their customers' counterparties other than just the counterparty's name and physical address. According to FinCEN, "Banks and MSBs would, under the proposed rule, continue to follow risk-based procedures, consistent with their AML/[Combatting the Financing of Terrorism] (MSB) program, to determine whether to obtain additional information about their customer[s'] counterparties or take steps to confirm the accuracy of counterparty information." This could be an onerous undertaking.
    3. At a minimum, FinCEN must provide sufficient time to enable financial institutions to implement any new requirements.

Attorney General's Cyber Digital Task Force — Cryptocurrency Enforcement Framework: https://www.justice.gov/opa/pr/attorney-general-william-p-barr-announces-publication-cryptocurrency-enforcement-framework

- On October 8, 2020, the US Department of Justice's (DOJ) Cyber Digital Task Force issued a comprehensive report outlining legitimate and illicit uses of cryptoassets, summarizing relevant law and regulation, and providing insight into business models that might facilitate criminal activity. The report also identified a number of successful prosecutions by the DOJ.
- **Observations**
    1. The DOJ did not provide any novel insights in its report. It did indicate, however, that it regards the use of anonymity enhanced cryptocurrencies that use nonpublic or private blockchains (e.g., Monero, Zcash and Dash) as a "high risk activity that is indicative of possible criminal conduct."
    2. The DOJ also acknowledged that while so-called "P2P" (peer to peer) exchanges are considered MSBs, "[i]n practice, …many P2P exchanges failed to register with FinCEN as MSBs or to comply with BSA obligations, and some even conduct transactions without requiring any form of identification from the customer."

FCA – Prohibiting the Sale to Retail Clients of Investment Products That Reference Cryptoassets: https://www.fca.org.uk/publication/policy/ps20-10.pdf

- In October 2020, the UK Financial Conduct Authority (FCA) adopted rules banning the sale, marketing and distribution to retail persons of any derivatives or exchange-traded notes that reference unregulated virtual assets (e.g., non-security tokens including cryptocurrencies) by firms acting in or from the United Kingdom:
    1. Affected derivatives include contracts for differences, futures and options.
    2. The ban went into effect on January 6, 2021.
- **Observations**
    1. FCA received 527 responses to its initial proposal published in July 2019. The FCA conceded that most (97 percent) of the commentators opposed the FCA's proposal. Generally, FCA rejected commentators' arguments that: cryptocurrencies had intrinsic value and could be valued reliably; derivatives based on virtual currencies served a legitimate investment need; and less restrictive measures (other than an absolute ban) could address FCA's concerns, among other arguments.

UK Regulatory Approach to Cryptoassets and Stablecoins (Consultation and Call for Evidence):

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/950206/HM_Treasury_Cryptoasset_and_Stablecoin_consultation.pdf

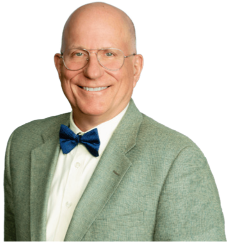
President's Working Group on Financial Markets — Statement on Key Regulatory and Supervisory Issues Relevant to Certain Stablecoins:

https://home.treasury.gov/news/press-releases/sm1223

European Commission: Proposal for a Regulation of the European Parliament and of the Council on a pilot regime for market infrastructure based on distributed ledger technology:

https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020PC0594&from=EN

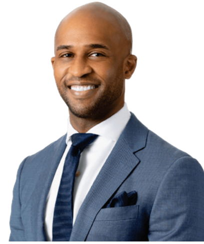
Contacts



Gary DeWaal

Special Counsel

New York
+1.212.940.6558
gary.dewaal@katten.com



Carl E. Kennedy

Partner

New York
+1.212.940.8544
carl.kennedy@katten.com

Offices

USA Offices

Charlotte

550 South Tryon Street
Suite 2900
Charlotte, NC 28202-4213

Chicago

525 West Monroe Street
Chicago, IL 60661-3693

Dallas

2121 North Pearl Street
Suite 1100
Dallas, TX 75201

Los Angeles – Century City

2029 Century Park East
Suite 2600
Los Angeles, CA 90067-3012

Los Angeles – Downtown

515 South Flower Street
Suite 4150
Los Angeles, CA 90071-2212

New York

575 Madison Avenue
New York, NY 10022-2585

Orange County

100 Spectrum Center Drive
Suite 1050
Irvine, CA 92618-4960

Washington, DC

2900 K Street NW
North Tower - Suite 200
Washington, DC 20007-5118

International Offices

London

Paternoster House
65 St Paul's Churchyard
London, EC4M 8AB
United Kingdom

Shanghai

Suite 4906 Wheelock Square
1717 Nanjing Road West
Shanghai, 200040
P.R. China

©2021 Katten Muchin Rosenman LLP. All rights reserved.
Katten refers to Katten Muchin Rosenman LLP and the affiliated partnership as explained at katten.com/disclaimer
Attorney advertising. Published as a source of information only. The material contained herein is not to be construed as legal advice or opinion.