Skadden

The Distributed Ledger

Blockchain, Digital Assets and Smart Contracts

1 *My Big Coin* Gives Big Boost to CFTC's Virtual Currency Enforcement Efforts

3 New York Attorney General Report Criticizes Virtual Asset Trading Platforms for Failing to Adequately Protect Customers

4 Ohio Statute Facilitates Development of Blockchain-Based Business

My Big Coin Gives Big Boost to CFTC's Virtual Currency Enforcement Efforts

In a recent case alleging virtual currency fraud, a Massachusetts federal district court handed the Commodity Futures Trading Commission (CFTC) a significant victory in its efforts to police fraud in virtual currency markets.

In *CFTC v. My Big Coin Pay, Inc.*,[1] the U.S. District Court for the District of Massachusetts ruled that a virtual currency fell within the Commodity Exchange Act's (CEA) definition of "commodity" and was subject to CFTC anti-fraud enforcement authority under CEA Section 6(c)(1) and CFTC Rule 180.1, even though no futures contracts for the virtual currency existed.[2]

The CFTC alleged that the defendants fraudulently offered the sale of a virtual currency called "My Big Coin."[3] According to the CFTC, the defendants made untrue or misleading statements and material omissions in touting My Big Coin as a "fully-functioning virtual currency," when in fact My Big Coin was never a functional, traded virtual currency.[4] The defendants moved to dismiss, primarily arguing that the CFTC failed to state a claim for relief because My Big Coin is not a "commodity" within the meaning of the CEA and therefore the CFTC's authority did not apply to the allegedly fraudulent scheme.[5]

The court explained that while the CEA grants the CFTC exclusive jurisdiction over commodity futures contracts and the exchanges where they are traded, it also grants the CFTC anti-fraud and anti-manipulation enforcement authority over any sale of a "commodity in interstate commerce."[6] The CEA defines "commodity" as including a number of enumerated agricultural products, as well as "all other goods and articles ... and all services, rights, and interests ... in which contracts for future delivery are presently or in the future dealt in."[7]

[1] No. 1:18-cv-10077-RWZ, 2018 WL 4621727 (D. Mass. Sept. 26, 2018).

[2] The court also ruled that Section 6(c)(1) and Rule 180.1 reached the pure fraud that the CFTC alleged in its complaint, and that the CFTC did not need to additionally allege manipulation. *See* Skadden's October 1, 2018, client alert.

[3] *See My Big Coin Pay, Inc.*, 2018 WL 4621727, at *1.

[4] *See id.*; *see also* Compl. at ¶ 2, *CFTC v. My Big Coin Pay, Inc.*, No. 1:18-cv-10077-RWZ (D. Mass. Jan. 16, 2018), ECF No. 1.

[5] *See My Big Coin Pay, Inc.*, 2018 WL 4621727, at *1, *3.

[6] *See id.* at *2 (citing Section 6(c)(1) and Rule 180.1(a)).

[7] CEA Section 1a(9).

The defendants argued that because no My Big Coin futures are "dealt in," My Big Coin is not a commodity under the CEA.[8] But the CFTC pleaded that both My Big Coin and bitcoin are virtual currencies, and the court noted that it was undisputed that bitcoin futures contracts are currently traded.[9] The CFTC argued that My Big Coin and bitcoin were "sufficiently related," in light of certain characteristics common to virtual currencies, so as to justify treatment as part of the same commodity category.[10]

The court agreed with the CFTC's argument that the term "commodity" is "broader than *any particular type or brand* of commodity."[11] The court observed that the CEA "defines 'commodity' generally and categorically," rather than "by type, grade, quality, brand, producer, manufacturer, or form," highlighting congressional intent to focus on categories of commodities rather than specific items.[12] The court further noted that the CEA should be construed "flexibly to effectuate [its] remedial purposes."[13] Finally, the court found support in cases holding that the CEA covered certain natural gas contracts for which there were no futures contracts because futures contracts existed on other types of natural gas and natural gas is "fungible" and "may move freely throughout a national pipeline system."[14] Thus, the court concluded, the CEA "only requires the existence of futures trading within a certain class ... in order for all items within that class ... to be considered commodities."[15]

The decision lends further support to the CFTC's view that virtual currency is properly within the scope of its regulatory and enforcement purview. The CFTC first took the position that virtual currency is a commodity subject to the agency's authority in a 2015 order settling charges against virtual currency firm Coinflip, Inc.[16] Since then, the CFTC has remained firm on that position in statements from commissioners,[17] guidance and interpretations[18] and enforcement actions.[19]

James McDonald, director of the CFTC Division of Enforcement, stated that the *My Big Coin* decision "recognizes the broad definition" of the term "commodity" under the CEA, as well as the CFTC's authority to prosecute fraud in the virtual currency space.[20] Director McDonald likened the *My Big Coin* decision to that in *CFTC v. McDonald*, a recent New York federal district court decision that held that the CFTC could pursue a pure anti-fraud action under Section 6(c)(1) and Rule 180.1 against defendants who allegedly operated a fraudulent virtual currency trading scheme and misappropriated money from investors.[21]

The CFTC will no doubt view the *My Big Coin* decision as a green light to press forward with its virtual currency enforcement efforts regardless of whether the particular type of virtual currency is subject to a futures contract. And in light of the CFTC's recent focus on virtual currency fraud, and continued growth and development in virtual currency products and markets,[22] those efforts are likely to remain vigorous.

[8] *See My Big Coin Pay, Inc.*, 2018 WL 4621727, at *3.

[9] *See id.* at *3 & n.6, *5 & n.8.

[10] *See id.* at *5 & n.8. The CFTC described virtual currency in its complaint as a "digital representation of value that functions as a medium of exchange, unit of account, and/or a store of value," which "does not have legal tender status in any jurisdiction." Am. Compl. ¶ 25, *CFTC v. My Big Coin Pay, Inc.*, No. 1:18-cv-10077-RWZ (D. Mass. Apr. 20, 2018). The CFTC cited as common characteristics of virtual currency the use of "cryptographic protocols to secure transactions," use of "decentralized networks to track transactions between persons who are denominated only by publicly visible strings of characters" and transactions that are "captured in single blocks at a time" that are "confirmed by 'miners'" who "perform[] algorithmic proofs of work ... for which they are usually awarded a sum of the virtual currency." *Id.*

[11] *See My Big Coin Pay, Inc.*, 2018 WL 4621727, at *3 (emphasis added). However, the court rejected the CFTC's argument that My Big Coin is a "good" or "article" and that the commodity definition's "dealt in" clause does not apply to goods and articles. *See id.* & n.5.

[12] *See id.* at *4.

[13] *See id.* (citing *SEC v. Zandford*, 535 U.S. 813, 819 (2002)).

[14] *See id.* (citing *United States v. Brooks*, 681 F.3d 678 (5th Cir. 2012); *United States v. Futch*, 278 F. App'x 387, 395 (5th Cir. 2008); *United States v. Valencia*, No. CR.A. H-03-024, 2003 WL 23174749, at *8 (S.D. Tex. Aug. 25, 2003), *order vacated in part on reconsideration*, No. CRIM.A. H-03-024, 2003 WL 23675402 (S.D. Tex. Nov. 13, 2003), *rev'd and remanded on other grounds*, 394 F.3d 352 (5th Cir. 2004)).

[15] *See id.*

[16] *See In re Coinflip, Inc.*, CFTC No. 15-29 (Sept. 17, 2015) (finding that Coinflip unlawfully offered bitcoin options and ran an unregistered facility for trading or processing swaps).

[17] *See, e.g.*, "Written Testimony of Chairman J. Christopher Giancarlo Before the Senate Banking Committee, Washington, D.C.," CFTC (Feb. 6, 2018); "Remarks of Chairman J. Christopher Giancarlo to the ABA Derivatives and Futures Section Conference, Naples, Florida," CFTC (Jan. 19, 2018); "Chairman Giancarlo Statement on Virtual Currencies," CFTC (Jan. 4, 2018); "Giancarlo Commends SEC Chairman Clayton on ICO Statement," CFTC (Dec. 11, 2017); "Testimony of Chairman Timothy Massad Before the U.S. Senate Committee on Agriculture, Nutrition & Forestry," CFTC (Dec. 10, 2014).

[18] *See, e.g.*, "Retail Commodity Transactions Involving Virtual Currency," 82 Fed. Reg. 60,335 (Dec. 20, 2017) (proposed guidance); CFTC, "CFTC Backgrounder on Oversight of and Approach to Virtual Currency Futures Markets" (Jan. 4, 2018); CFTC, "Customer Advisory: Understand the Risks of Virtual Currency Trading" (Dec. 15, 2017); CFTC, "CFTC Backgrounder on Self-Certified Contracts for Bitcoin Products" (Dec. 1, 2017); *see also* Skadden's December 26, 2017, client alert.

[19] *See, e.g.*, Compl., *CFTC v. Blue Bit Banc*, No. 2:18-cv-02247-SJF-ARL (E.D.N.Y. Apr. 16, 2018) (alleging virtual currency fraud); Compl., *CFTC v. Dean*, No. 2:18-cv-00345 (E.D.N.Y. Jan. 18, 2018) (same); Compl., *CFTC v. Gelfman Blueprint, Inc.*, No. 1:17-cv-07181 (S.D.N.Y. Sept. 21, 2017) (same); *In re Bitfinex*, CFTC No. 16-19 (June 2, 2016) (finding that bitcoin exchange unlawfully offered off-exchange financed retail commodity transactions and failed to register as a futures commission merchant); *In re TeraExchange, LLC*, CFTC No. 15-33 (Sept. 24, 2015) (finding that swap execution facility failed to enforce prohibitions on wash trading and prearranged trading of a bitcoin swap).

[20] Press Release, "Federal Court Finds That Virtual Currencies are Commodities," CFTC (Oct. 3, 2018).

[21] *See CFTC v. McDonnell*, No. 18-CV-361, 2018 WL 3435047 (E.D.N.Y. July 16, 2018), *denying reconsideration in CFTC v. McDonnell*, 287 F. Supp. 3d 213 (E.D.N.Y. 2018). *See also* Skadden's October 1, 2018, client alert.

[22] *See, e.g.*, Sarah Hansen, "Guide to Top Cryptocurrency Exchanges," Forbes (June 20, 2018) (noting that there are over 1,600 different virtual currencies).

New York Attorney General Report Criticizes Virtual Asset Trading Platforms for Failing to Adequately Protect Customers

On September 18, 2018, the Office of the New York State Attorney General (the OAG) released a report criticizing virtual currency trading platforms for insufficiently protecting customers (the Report), following a fact-finding inquiry by the Virtual Markets Integrity Initiative.[23] The Report's key conclusion is that "[V]irtual asset trading platforms now in operation have not registered under state of federal securities or common laws. Nor have they implemented common standards for security, internal controls, market surveillance protocols, disclosures, or other investor and consumer protections. Accordingly, customers of virtual asset trading platforms face significant risks."

The OAG launched its Virtual Markets Integrity Initiative in April 2018 by sending letters and questionnaires to 13 cryptocurrency exchanges requesting information regarding their policies and practices. Nine of the 13 exchanges participated in the inquiry.[24] The four exchanges that declined to participate claimed that they did not allow trading from New York state.[25] Following an investigation into whether these exchanges accepted trades from within New York state, OAG referred three of the platforms (Binance, Gate.io and Kraken) to the New York State Department of Financial Services for possible violations of New York state's virtual currency regulations.[26]

The Report comes on the heels of a March 2018 public statement by the Securities and Exchange Commission warning investors about potentially unlawful online trading platforms for virtual currencies.[27] It is unlikely to be the last word on such exchanges by regulators who are facing increased calls to regulate cryptocurrencies.

The Report identified three broad areas of concern: conflicts of interest, susceptibility to abusive trading practices, and limited or illusory protections for consumer funds.

Conflicts of Interest

- The OAG found that there is little information available regarding how the exchanges determine whether or not to list a particular virtual currency on their respective platforms, and none of the responding exchanges conveyed a consistent methodology used to make this determination. The Report also highlighted that cryptoexchanges typically do not disclose whether they receive compensation for listing a particular virtual currency.
- Several of the participating exchanges indicated that they allow owners and employees to trade directly on their platforms. The Report cautioned that if employees have access to nonpublic information, they may be engaging in insider trading at the expense of everyday investors.
- A number of the participating exchanges indicated that they engage in proprietary trading on their own platform, to varying degrees. The Report noted that exchanges may thereby be acting as "market makers," and to the extent that a significant volume of trades are attributable to proprietary trading, this could mask the true liquidity of the exchange.

Susceptibility to Abusive Trading Practices

- The OAG found that most of the cryptoexchanges do not have a formal policy to monitor and prevent abusive trading. Unlike traditional exchanges, they lack robust market surveillance capabilities to spot and halt suspicious trading patterns, and fail to monitor pump-and-dump schemes.
- The Report noted that few of the participating cryptoexchanges prohibit "bots" or the use of automated algorithmic trading or trading using application programming interfaces.

Protection of Consumer Funds

- The OAG explained that there are no generally accepted auditing methods for virtual assets, and cryptoexchanges generally do not have a transparent or consistent approach to independent auditing. Several exchanges indicated that they do not hire independent auditors to conduct audits of their virtual currency holdings. The Report cautions that lack of independent audits makes it difficult to determine whether such cryptoexchanges are responsibly protecting the virtual assets over which they have custody.
- Most but not all of the participating cryptoexchanges reported that they conduct penetration testing to identify security flaws in their platform. The Report notes that in the event of a hack or unauthorized withdrawal, customers are highly vulnerable.
- The Report notes that insurance products for virtual currencies are underdeveloped and not well understood.

[23] The full text of the report is available here.

[24] Companies that participated in the Virtual Markets Integrity Initiative are: Bitfinex (operated by iFinex Inc.), bitFlyer USA, Inc. , Bitstamp, Ltd., Bittrex, Inc., Coinbase, Inc., Gemini Trust Company, itBit (operated by Paxos Trust Company), Poloenix (owned by Circle Internet Financial Limited), Tidex (operated by Elite Way Developments LLP) and HBUS (the U.S. strategic partner of Huobi Inc.).

[25] Four exchanges declined to participate: Binance Limited, Gate.io (operated by Gate Technology Incorporated), Huobi Global Limited and Kraken (operated by Payward, Inc.).

[26] The regulations are available here.

[27] The public statement is available here.

- The OAG found that most exchanges do not have formal policies in place to protect customers during outages or trading suspensions, and customers have often been locked out of their accounts and unable to trade. According to the Report, cryptoexchanges have failed to adequately notify customers of any such outages.

Questions Customers Should Be Asking

The Report concludes with a list of questions that customers should consider before transacting with a virtual asset trading platform:

1. What security measures are in place to stop hackers from unlawfully accessing the platform or particular customer accounts?
2. What insurance or other policies are in place to make customers whole in the event of a theft of virtual or fiat currency?
3. What guardrails or other policies does the platform maintain to ensure fairness for retail investors in trading against professionals?
4. What controls does the platform maintain to keep unauthorized or abusive traders off the venue?
5. What policies are in place to prevent the company and its employees from exploiting nonpublic information to benefit themselves at the expense of customers?
6. How does the platform notify customers of a site outage or suspension, the terms under which trading will resume and how customers can access funds during an outage?
7. What steps does the platform take to promote transparency and to subject its security, virtual and fiat accounts, and controls to independent auditing or verification?
8. Is the platform subject to, and registered under, banking regulations or a similar regime — for instance, the New York BitLicense regulations?

Ohio Statute Facilitates Development of Blockchain-Based Business

Several states have introduced legislation to facilitate the use of blockchain technology in an effort to attract new technology initiatives to their state. While many such bills remain in committee, or states simply pass a mandate to study the issue, Ohio recently joined Arizona, California, Delaware, Nevada, Tennessee and Vermont by enacting somewhat more substantive statutes.[28] Although the Ohio statute did not go as far as Arizona in specifically recognizing the enforceability of "smart contracts," the statute nonetheless benefits developers by recognizing the use of blockchain technology to store and transmit electronic records.

The statute is actually a minor amendment to its version of the Uniform Electronic Transactions Act (UETA). Forty-seven states have enacted a version of the UETA, the language of which varies somewhat across states. The UETA generally states the following with respect to "electronic records" and other documents in an "electronic form":

- A record or signature may not be denied legal effect or enforceability solely because it is in electronic form.
- A contract may not be denied legal effect or enforceability solely because an electronic record was used in its formation.
- If a law requires a record to be in writing, an electronic record satisfies the law.

Ohio's amendment to its version of the UETA states that a record or contract that is secured through blockchain technology is considered to be in an "electronic form" and to be an "electronic record." Therefore, records and contracts secured through blockchain technology may not be denied legal effect or enforceability solely because they are in electronic form or because an electronic record was used in the formation of the contract. Similarly, blockchain-based records satisfy written record-keeping requirements under the amended Ohio statute.

Ohio notably omitted language regarding the enforceability of smart contracts in its recent amendment. The term "smart contract" refers to computer code that automatically executes all or parts of an agreement and is stored on a blockchain-based platform. An earlier version of Ohio's amendment suggested that the enforceability or legal effect of electronic contracts cannot be denied simply because a contract contains a "smart contracts term." The enacted version does not include this language. However, this smart contracts-specific language may have been omitted on the theory that smart contracts are already enforceable under Ohio's version of the UETA — which theory has not been tested or conclusively decided in Ohio state courts.

Key Takeaways

Given that contract law is ordinarily a function of state law in the United States, we will likely see further statutory developments regarding the legal effect of blockchain-based records and contracts at the state level. Some have asserted, however, that statutes like those in Ohio and Arizona are primarily marketing ploys to attract blockchain businesses, since blockchain-based systems likely already fell within the UETA's definition of "electronic record."

[28] The full text of the Ohio statute is available here.

Contacts

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

Ryan J. Dzierniejko
Partner / New York
212.735.3712
ryan.dzierniejko@skadden.com

Gregory A. Fernicola
Partner / New York
212.735.2918
gregory.fernicola@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

Alex Jupp
Partner / London
44.20.7519.7224
alex.jupp@skadden.com

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

James A. McDonald
Partner / London
44.20.7519.7183
james.mcdonald@skadden.com

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

Danny Tricot
Partner / London
44.20.7519.7071
danny.tricot@skadden.com

Mark D. Young
Partner / Washington, D.C.
202.371.7680
mark.d.young@skadden.com

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

Skadden, Arps, Slate, Meagher & Flom LLP
Four Times Square
New York, NY 10036
212.735.3000