Portfolio Media. Inc. | 111 West 19th Street, 5th floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

3 Critical Events For Cryptocurrency Exchanges: Part 2

By **John Reed Stark and David Fontaine** (March 13, 2018, 1:22 PM EDT)

John Reed Stark

David Fontaine

Notice to all cryptocurrency exchanges: Be prepared for a relentless U.S. regulatory onslaught.

That seems to be the clear warning embodied in three events last week involving the U.S. Securities and Exchange Commission, the Financial Crimes Enforcement Network at the U.S. Department of the Treasury, and the U.S. Commodity Futures Trading Commission:

1. The SEC's "Statement on Potentially Unlawful Online Platforms for Trading Digital Asset," jointly issued by the SEC's enforcement division and its trading and markets division, on March 7, 2018;

2. FinCEN's response to a congressional request by Democratic Sen. Ron Wyden, ranking member on the U.S. Senate Committee on Finance, sent on Feb. 13, 2018, and made public on March 6, 2018; and

3. The CFTC's March 6, 2018, litigation victory in U.S. federal district court against defendants Patrick K. McDonnell and CabbageTech Corp., d/b/a Coin Drop Markets, or CDM, which confirmed that virtual currencies are goods exchanged in a market for a uniform quality and value and fall well within the common definition of "commodity."

The confluence of these events, which all occurred during the same 24-hour window, is more than a mere harbinger. These three powerful, essential and historically respected U.S. federal enforcement agencies are no longer content with generating regulatory headwinds or publicizing menacing saber rattling. Instead, the SEC, FinCEN and the CFTC have now unleashed the perfect storm — and cryptocurrency exchanges, trading platforms and the like currently reside right smack in the eye of it.

In this two-part series, we unpack the SEC statement, the Wyden response and the CDM order, extrapolating key takeaways from each, scrutinizing their underlying legal theories, and forecasting their ultimate impact. **Part one** of our series addressed the SEC statement. Part two now addresses the Wyden response and the CDM order.

Cryptocurrency Exchanges and FinCEN

FinCEN was one of the first federal regulators out of the gate with respect to cryptocurrency exchanges, and on March 18, 2013, issued certain interpretive guidance at the federal level to clarify the applicability of the regulations implementing the Bank Secrecy Act to persons creating, exchanging and transmitting virtual currencies.

A year later, on Oct. 27, 2014, in a response to twin letters submitted in late 2013, FinCEN explained that bitcoin exchanges may be money transmitters, even if they only match buyers and sellers on their platform. Further, the letters suggest that this is true, even if the exchanges behave more like traditional securities or commodities exchanges, where no money is transferred between the company and any counterparty.

Congress has begun to take notice of FinCEN's posture and encourage further FinCEN enforcement efforts. Specifically, in December 2017, Sen. Ron Wyden, D-Ore., sent FinCEN a request for answers to a series of questions on cryptocurrency tokens, including one asking how FinCEN will apply the BSA framework to participants in the initial coin offering market, like token developers, and when FinCEN will issue guidance regarding its enforcement intentions regarding digital token exchanges and ICOs. The Wyden response was delivered on Feb. 13, 2018, and made public on March 6, 2018.

With respect to ICOs, FinCEN expressed the view that a person or developer that sells convertible virtual currency, including in the form of tokens sold in an ICO, in exchange for real currency or a substitute for currency, is engaged in a money services business and, therefore, must register with FinCEN and comply with anti-money laundering requirements. Categorization as an MSB also brings with it potential state licensing and related regulatory requirements. Indeed, under federal law, an MSB that fails to secure requisite state licensure can be subject to federal criminal prosecution under 18 U.S.C. § 1960.

With respect to cryptocurrency exchanges, the Wyden response reiterated its March 18, 2013, guidance, in which FinCEN stated that exchangers and administrators of "convertible virtual currency" are money transmitters. That response defined "convertible virtual currency" as either having an equivalent value in real currency or acting as a substitute for real currency. An "administrator" engaged in the business of issuing or putting convertible virtual currency into circulation, and which can withdraw it from circulation, is a money transmitter.

Exchanges can also qualify as MSBs, according to FinCEN:

> An exchange that sells ICO coins or tokens, or exchanges them for other virtual currency, fiat currency, or other value that substitutes for currency, would typically also be a money transmitter.

Anti-Money Laundering and Cryptocurrency Generally

Theoretically, anyone with an internet connection and a digital wallet can be part of an ICO or cryptocurrency exchange — which, of course, opens the door for those with criminal motives. Given that cryptocurrency transactions are pseudonymous, encrypted and decentralized by nature, virtual currencies offer a convenient method of transferring funds obtained from illegal activities without an audit trail, thereby making it harder for any central authority or law enforcement agency to track each of the transactions made, and to identify the individuals behind any of them. On the other hand, transactions involving traditional financial firms, such as banks, brokers and dealers, and money service businesses are subject to strict U.S. anti-money laundering laws and regulations aimed at detecting and reporting suspicious activity, including money laundering and terrorist financing, as well as securities fraud and market manipulation.

Not surprisingly, the notion of terrorists and criminals being able to launder money anonymously has not escaped the attention of U.S. law enforcement agencies, which have vowed to crack down on the virtual currency exchanges that serve criminals, even those operating outside the United States. Along those lines, the U.S. Department of Justice, acting in cooperation with FinCEN, has become increasingly active in policing criminals exploiting cryptocurrencies, leveraging AML statutes and regulations as the preferred statutory prosecutorial weapon.

For instance, as far back as 2015, in addition to being charged for conspiracy to commit bank fraud and conspiracy to obstruct an examination of a financial institution, Anthony Murgio, a bitcoin exchange operator, also pled guilty to operating as a money transmitter without a license, and was sentenced to 5 ½ years in prison.

Federal prosecutors alleged Murgio and his co-conspirators benefited from transactions providing victims with bitcoin to pay off ransomware demands. The indictment states:

> As part of the unlawful Coin.mx scheme, Anthony P. Murgio, the defendant, and his co-conspirators knowingly processed and profited from numerous Bitcoin transactions conducted on behalf of victims of ransomware schemes … By knowingly permitting ransomware victims to exchange currency for Bitcoins through Coin.mx, Murgio and his co-conspirators facilitated the transfer of ransom proceeds to the malware operators while generating revenue for Coin.mx.

Not just a part of the ransomware payment process, Murgio allegedly facilitated the ransomware transactions with unclean hands — possessing the kind of nefarious intent required for money laundering criminal liability, which is probably why the Murgio prosecution also addresses AML liability.

Specifically, the issues relate to the failure of Murgio and his cohorts to:

- Register with FinCEN;
- Maintain an effective AML program;
- Comply with AML record-keeping requirements; and
- File with FinCEN suspicious activity reports regarding customers who use cryptocurrencies for nefarious purposes.

The Murgio indictment also alleges that Murgio and another defendant had undue influence on a federally insured credit union that handled the exchange's banking operations for a period of time, and that they tried to "trick" major financial institutions about the nature of their business.

The Murgio defendants allegedly exchanged at least $1.8 million bitcoins for cash for certain customers who claimed they were ransomware attack victims needing bitcoins to "pay off" ransomware attackers.

FinCEN, MSBs and Cryptocurrency

MSBs have been required to register with FinCEN since 1999, when the MSB regulations first went into effect. MSBs have historically been recognized by FinCEN to include (1) currency dealers or exchangers; (2) check cashers; (3) issuers of traveler's checks, money orders or stored value; (4) sellers or redeemers of traveler's checks, money orders or stored value; and (5) money transmitters.

An entity acting as an MSB that fails to register (by filing a registration of money services business, and renewing the registration every two years per 31 U.S.C. § 5330 and 31 C.F.R. § 1022.380), is subject to civil money penalties and possible criminal prosecution.

The registration of the MSB serves as a first step in establishing the compliance framework for applicable FinCEN regulations designed to help mitigate the risks of criminal abuse of MSBs for money laundering and terrorist financing as the MSB seeks to provide financial services to customers for legitimate purposes. There is no cost for registration, which is a simple procedure explained in detail on FinCEN's website.

The BSA and its implementing regulations require an MSB to develop, implement and maintain an effective, written AML program that is reasonably designed to prevent the MSB from being used to facilitate money laundering and the financing of terrorist activities. For ICOs and cryptocurrency exchanges, this would require, among other things, meticulously

recording transactions, definitively knowing who customers are, and reporting suspicious activity to law enforcement.

FinCEN's MSB Expansion

Recently, FinCEN has begun to expand its definition of an MSB even further, to include not only virtual currency exchanges but also cryptocurrency platforms that act as enablers/financial intermediaries for criminal schemes.

For instance, in a July 2017 AML enforcement action, FinCEN, in a joint prosecution by the U.S. Attorney's Office for the Northern District of California, assessed a $110 million civil money penalty against BTC-e, aka Canton Business Corp., for willfully violating U.S. AML laws. Russian national Alexander Vinnik, one of the operators of BTC-e, was also arrested in Greece, and FinCEN assessed a $12 million penalty against him for his role in the violations.

BTC-e is an internet-based, foreign-located money transmitter that exchanges fiat currency as well as the convertible virtual currencies Bitcoin, Litecoin, Namecoin, Novacoin, Peercoin, Ethereum and Dash. By volume, BTC-e is one of the largest virtual currency exchanges in the world. In so doing, the exchange facilitated numerous transactions connected to a variety of criminal activities ranging from illegal drug sales on dark web markets like Alpha Bay to public corruption.

FinCEN asserted jurisdiction because BTC-e conducts business as an MSB in substantial part within the United States (including $296 million of U.S. customer transactions through U.S servers.) The BTC-e FinCEN action marks just the second case by FinCEN involving a cryptocurrency exchange and the first FinCEN action against a foreign-based exchange that did substantial business in the United States.

In announcing the AML fines and prosecutions, Jamal El-Hindi, acting director for FinCEN, stated:

> We will hold accountable foreign-located money transmitters, including virtual currency exchangers, that do business in the United States when they willfully violate U.S. anti-money laundering law. This action should be a strong deterrent to anyone who thinks that they can facilitate ransomware, dark net drug sales, or conduct other illicit activity using encrypted virtual currency. Treasury's FinCEN team and our law enforcement partners will work with foreign counterparts across the globe to appropriately oversee virtual currency exchangers and administrators who attempt to subvert U.S. law and avoid complying with U.S. AML safeguards.

The response to Wyden also expands upon the 2013 FinCEN guidance, taking the position that under existing FinCEN rules and interpretations, a developer that sells convertible currency, including in the form of ICO coins or tokens, in exchange for another type of value that substitutes for currency, is a money transmitter. Money transmitters must comply with the BSA and its implementing regulations issued by FinCEN that apply to MSBs.

FinCEN recognizes that ICO structures may vary, and may be structured as an offering or sale of securities or derivatives that are subject to the jurisdiction of the SEC and CFTC. In such cases, the Wyden response states that the SEC or CFTC regulations implementing the BSA, and imposing AML and CFT requirements, would apply to the covered parties involved in an ICO.

Key AML/Crypto Takeaways

Some key crypto takeaways from FinCEN's response to Wyden (together with the FinCEN/DOJ fines, prosecutions, and overall regulatory and enforcement posture toward the alleged "criminal design" of cryptocurrency exchanges) are as follows:

- By becoming increasingly sophisticated at co-opting a cryptocurrency network to establish an AML jurisdictional nexus, FinCEN and DOJ have laid the groundwork to link and prosecute both the masterminds and the foot soldiers of unregistered ICOs and cryptocurrency exchanges;
- The SEC has become increasingly aggressive in its policing of ICOs, but now, with FinCEN clearly entering the fray, ICOs are in for an even rougher ride, which will translate into more cryptocurrency investigations and prosecutions. If what FinCEN is saying holds merit, anyone who sells tokens to U.S. residents while, at the same time, failing to register with FinCEN as an MSB and failing to perform the "know your customer" and AML compliance obligations could also face several years in prison under a felony conviction. Employees and investors of ICO companies and cryptocurrency exchanges could be held criminally liable, too. Worse, the federally related offense of wire fraud, which includes sending money over the internet to avoid reporting requirements, could even be bootstrapped to the AML and KYC charges;
- FinCEN is actively mining BSA data to develop leads on cyberthreats who may be involved in ICOs and cryptocurrency exchanges, and coordinating with an alphabet soup of criminal investigative agencies by sharing critical analytics and by providing tactical and strategic intelligence reports associated with these threats;
- U.S. regulators and prosecutors could take action against persons or entities associated with an ICO or cryptocurrency exchange under the auspices that they are MSBs who fail to keep BSA/AML controls or know their customers — or even for avoiding or neglecting reporting requirements or not properly registering as money transmission businesses (like Murgio);
- When an offshore person or entity intentionally and maliciously participates and profits within the financial machinations of a ransomware scheme (such as the alleged money laundering by BTC-e and its senior management via a cryptocurrency exchange), a company or person's location overseas is not necessarily a defense to AML charges;

- AML rules and regulations also could affect the sponsor of a token offering or token exchange indirectly to the extent it relies on banks, exchanges or other financial institutions for clearing, settlement, custody or other functions; and

- Companies involved with ICOs and cryptocurrency exchanges should carefully review FinCEN's guidance on the "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies" and obtain compliance advice and counsel when necessary. If cryptocurrency exchanges conduct business with shady characters, their actions could nonetheless raise AML red flags by facilitating such transactions.

Cryptocurrency Exchanges and the CFTC

Along with FinCEN and the SEC, the CFTC is similarly mobilizing rapidly to declare its jurisdiction and intention to enforce cryptocurrency regulation.

The CFTC has issued several customer protection fraud advisories, including its "Customer Advisory: Risks of Virtual Currency Trading," which describes the risks of trading virtual currencies and warns customers about a number of virtual currency exchange scams.

The CFTC's interest in cryptocurrency exchanges dates back to September 2015, when the CFTC issued an order filing and simultaneously settling charges against Coinflip Inc., d/b/a Derivabit, and its chief executive officer, Francisco Riordan. The CFTC brought its charges against Coinflip and Riordan for conducting activity related to commodity options transactions without complying with the Commodity Exchange Act and CFTC regulations, specifically, by operating a facility for the trading or processing of commodity options without complying with the CEA or CFTC regulations otherwise applicable to swaps or conducting the activity pursuant to the CFTC's exemption for trade options.

The CFTC order found that, from in or about March 2014 to at least August 2014, Coinflip and Riordan operated an online cryptocurrency platform named Derivabit, offering to connect buyers and sellers of bitcoin option contracts. Aitan Goelman, the CFTC's enforcement director at the time, commented:

> While there is a lot of excitement surrounding Bitcoin and other virtual currencies, innovation does not excuse those acting in this space from following the same rules applicable to all participants in the commodity derivatives markets.

Fast forward to Jan. 19, 2018, when the CFTC reinforced this notion in a joint statement with the SEC, affirming bluntly that cryptocurrencies were commodities. Then, a few days later, CFTC Chairman Christopher Giancarlo and SEC Chairman Jay Clayton took to the Wall Street Journal editorial pages to proclaim their stand regarding cryptocurrencies, while the CFTC concurrently announced its third fraud enforcement action in a week. In the WSJ op-ed, the dynamic federal regulatory duo of Clayton and Giancarlo wrote portentously:

> In recent months we have seen a wide range of market participants, including retail investors, seeking to invest in DLT [distributed ledger technology] initiatives, including through cryptocurrencies and so-called ICOs, initial coin offerings. Experience tells us that while some market participants may make fortunes, the risks to all investors are high. Caution is merited ... The SEC is devoting a significant portion of its resources to the ICO market. Through statements, reports and enforcement actions the SEC has made it clear that federal securities laws apply regardless of whether the offered security — a purposefully broad and flexible term — is labeled a "coin" or "utility token" rather than a stock, bond or investment contract. Market participants, including lawyers, trading venues and financial services firms, should be aware that we are disturbed by many examples of form being elevated over substance, with form-based arguments depriving investors of mandatory protections.

Next, on Feb. 6, 2018, the Senate Banking, Housing and Urban Affairs Committee held a hearing on virtual currencies. The chairmen of the SEC and CFTC testified together on their agencies' respective oversight and regulatory actions concerning cryptocurrencies, as well as what they thought should be a broader coordinated effort by federal agencies to monitor and regulate cryptocurrencies and to educate the public and investors about potential associated risks.

The CDM Order

Most recently, on March 6, 2018, the CFTC's cryptocurrency jurisdiction was confirmed when Judge Jack B. Weinstein of the U.S. District Court for the Eastern District of New York entered an order against defendants Patrick K. McDonnell and CabbageTech Corp., d/b/a Coin Drop Markets.

The CDM order stemmed from the CFTC's Jan. 18, 2018, complaint charging the defendants with fraud and misappropriation in connection with purchases and trading of the virtual currencies bitcoin and litecoin. At issue in the case was whether the CFTC had the authority to regulate cryptocurrency as a commodity and whether the law permitted the CFTC to exercise its jurisdiction over fraud that does not directly involve the sale of futures or derivative contracts. According to the order:

> Virtual currencies are "goods" exchanged in a market for a uniform quality and value ... [and] ... They fall well within the common definition of "commodity."

Specifically, Judge Weinstein found that the CFTC had shown a reasonable likelihood that the defendants would continue to violate the Commodity Exchange Act. The CDM order prohibits the defendants from engaging in fraud in violation of the CEA, requires defendants to preserve books and records, and requires defendants to provide expedited discovery. In its continuing litigation, the CFTC seeks, among other relief, a permanent injunction against future violations of federal commodities laws, restitution to defrauded customers, disgorgement of benefits from violations of the Commodity Exchange Act and CFTC regulations, civil monetary penalties, and trading bans, as charged.

The CDM order resulted from the efforts of the CFTC Division of Enforcement Virtual Currency Task Force, the first cousin of the SEC's new cyber unit, which signifies that both the CFTC and SEC are approaching crypto issues with the same committed, concentrated and specialized approach.

Looking Ahead

The SEC statement, the FinCEN Wyden response and the CDM order clearly evidence that cryptocurrency exchanges are now squarely in the sights of federal regulators.

Interestingly, the FinCEN Wyden response references that FinCEN, the SEC and the CFTC are working together to clarify and enforce anti-money laundering and anti-terrorism funding regulations. This noted inter-agency cooperation is also a likely nod to cryptocurrency joint operations within the U.S. Treasury — involving the CFTC, SEC, FinCEN and others — aimed at coordinating the various agencies' patrolling of the cryptocurrency industry. This effort was also described by Giancarlo during his Feb. 6, 2018, testimony before the U.S. Senate.

All of the most powerful U.S. regulatory players are talking and collaborating — having now become strategically aligned to execute their rigorous scrutiny of all things crypto, including and especially cryptocurrency exchanges. These coordinated federal initiatives may be viewed as alarming by entrepreneurs and their advisers, who are breaking new ground within the exciting and promising world of blockchain. But we believe such concerns are largely misguided.

Whatever cryptocurrency marketplace survives the SEC's, FinCEN's and CFTC's crypto crackdowns will provide the same customer protections and capital safeguards often taken for granted in the context of the traditional trading of securities and rendering of financial transactions. This not only makes for good business, but for a more robust and resilient blockchain-related marketplace.

Bear this in mind: In U.S. capital markets, when an investor orders 100 shares of his or her favorite stock, a transparent and meticulously recorded transaction occurs. That's because — and this is no coincidence — U.S. markets, in addition to being the most heavily regulated, are also the most efficient, most robust, most trusted and most secure in the world.

ICOs and cryptocurrency exchanges have turned this traditional notion of safety and confidence on its head. But if crypto-markets are here to stay, we believe regulation is inevitable and ultimately will lead to a more transparent and effective business model with the potential to endure.

While the U.S. government should not discourage modernization or technological advances like the many possible benefits and applications of blockchain technology, it makes sense for the SEC, FinCEN and CFTC to ferret out the abuses. Although innovation and creativity have made U.S. securities markets the best capital formation system in the world, thoughtful government intervention has ensured that U.S. markets also have the highest level of integrity, reliability and safety.

After the dust settles from the SEC, FinCEN and CFTC initiatives, what will result in the short run admittedly won't be pretty — there will be some blood on the floor in the form of lost investments from honest wide-eyed investors caught up in the current cryptocurrency frenzy. Even the so-called cryptocurrency "gatekeepers," such as the lawyers who have helped facilitate unlawful ICO offerings and promotions, will perhaps take a hit.

But what will follow in the long run (if possible) will be a more fulsome, more transparent, more reliable, more efficient and far healthier cryptocurrency/blockchain marketplace. Not a bad result for Main Street investors — whose lifetime or retirement savings are at risk. And not a bad result for everyday American citizens — whose safety is at risk by pseudo-anonymous crypto-transactions, which can conceal money laundering and other illicit activity, thereby fostering the activities of drug dealers, terrorist organizations or other bad actors intent on doing harm.

John Reed Stark is the president of John Reed Stark Consulting LLC, a data breach response and digital compliance firm. Formerly, Stark served for almost 20 years in the Enforcement Division of the U.S. Securities and Exchange Commission, including 11 years as the chief of its Office of Internet Enforcement. He was recently a senior lecturing fellow at Duke University Law School and will be teaching a cyber law course there in spring 2019. He also worked for 15 years as an adjunct professor of law at the Georgetown University Law Center. He is the author of "The Cybersecurity Due Diligence Handbook."

David Fontaine is the chief executive officer of Kroll Inc. and its parent company, Corporate Risk Holdings LLC. Previously, he held senior leadership roles and served as the chief legal officer, chief risk officer, chief administrative officer and corporate secretary at several public and private companies, including Travelex Global Business Payments Inc., American Management Systems Inc. and Proxicom Inc.