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

Crypto Developments Are Indeed Alarming

By **John Reed Stark and David Fontaine** (April 3, 2018, 5:43 PM EDT)

John Reed Stark

David Fontaine

In a **recent rebuttal** to our **two-part Law360 guest column**, which cautioned cryptocurrency exchanges to be "prepared for relentless U.S. regulatory oversight," Sarah Auchterlonie and Emily Garnett advise instead that cryptocurrency financiers are at no greater risk today than they have been over the last few years — and should not be alarmed by recent regulatory and law enforcement activities.

We could not disagree more. Here's are a few quick reasons why:

1. Auchterlonie and Garnett claim that certain cryptocurrency tokens are not securities and that U.S. Securities and Exchange Commission jurisdiction is "murky" — but the definition of security is extraordinarily broad with a presumptive, rich and storied history favoring SEC jurisdiction.

Historically, the courts and the SEC have taken an extremely broad view of whether any kind of investment is a security. Indeed, the definition of "security" under Section 2(a)(1) of the Securities Act of 1933 (and the nearly identical definition under Section 3(a)(10) of the Exchange Act of 1934) includes not only a number of specific types of financial instruments, such as notes, bonds, debentures and stock, but also broad categories of financial instruments, such as evidences of indebtedness and investment contracts.

Plainly crafted to contemplate not only known securities arrangements at the time — but also any prospective instruments created by those who seek the use of the money of others on the promise of profits — the definition of "security" is broad, sweeping and designed to be flexible to capture new instruments that share the common characteristics of stocks and bonds.

Consider for example, so-called prime bank notes, which have been promoted for decades as sound and safe investments — but are instead bogus financial instruments purporting to derive their value from European secondary markets for stand-by letters of credit, a wholly fictional concoction.

In the seminal prime bank case SEC v. Lauer (1995), the purveyors of prime bank notes argued that the prime bank notes were not securities because they were wholly fictional. The Seventh Circuit disagreed, noting that the so-called Howey test did not require that the securities actually existed, but rather whether the investment, as described, had the characteristics of a security, highlighting just how broad the definition of security is.

While it is an interesting academic exercise to debate the Howey test, the reality is that be it an Article III judge or an SEC administrative law judge, the SEC will be granted tremendous latitude with respect to its jurisdiction, and betting against the SEC with a "not a security" defense would be a highly risky gamble. This is probably why SEC Chairman Jay Clayton has asserted confidently that, "I believe every ICO I have ever seen is a security ... ICOs should be regulated like securities offerings. End of Story."

Auchterlonie and Garnett also offer no reason why the SEC interpretation would not be afforded

Auchterlonie and Garnett also offer no reason why the SEC interpretation would not be afforded the high level of deference historically and routinely extended to the regulatory agency that has been charged with oversight and enforcement responsibilities. Along those lines, federal courts have already confirmed the SEC's jurisdiction in the SEC's crypto-related emergency asset freeze hearings where the issue was almost certainly considered and affirmed.

2. Auchterlonie and Garnett fail to appreciate the SEC's stridency regarding initial coin offerings, cryptocurrency exchanges and the like, clearly indicating that the SEC's crypto-enforcement crackdown will be lengthy, robust and relentless.

Clayton formally launched his cryptocurrency regulatory efforts with a July 25, 2017, investor bulletin warning investors about ICOs and, issued that same day, a report of investigation pursuant to Section 21(a) of the Securities Exchange Act of 1934, explaining how ICOs are unlawful. During the ensuing months, Clayton went on a crypto tour asserting over and over again that cryptocurrency tokens in many cases looked like securities and were susceptible to fraud and chicanery by insiders, management and better-informed traders and market participants, including on Nov. 9, 2017, speaking at an SEC conference; on Dec. 11, 2017, issuing an official SEC "statement on cryptocurrencies and initial coin offerings"; and on Feb. 6, 2018, testifying before the Senate Banking, Housing and Urban Affairs Committee. The SEC even went so far as to turn the spotlight on celebrities running social media ICO promotions and endorsements, admonishing them that they may run afoul of securities laws when advertising cryptocurrencies and other investments, including ICOs.

Any SEC historian would attest that rarely in its 84-year history has the SEC been so explicit and so recurring in the public expression of its warnings and rebukes. Clearly, issuing an ICO or operating a cryptocurrency exchange is a lightning rod for regulatory (especially SEC) scrutiny and law enforcement interest, and unless a crypto financier is prepared for an exhaustive, protracted, lengthy and expensive investigatory rectal exam, counsel would be wise to sound the alarm.

3. Auchterlonie and Garnett state that the "fear of FinCEN is misplaced" — but the Financial Crimes Enforcement Network's anti-money laundering requirements, combined with state law money services business licensing and bonding requirements not only create a hefty, burdensome and onerous federal and state regulatory burden and concern — they also enhance the risk significantly for any financial firm.

While Auchterlonie and Garnett do admit that the multistate licensing regime can be onerous, they underestimate the added risk that MSB and AML requirements pose to a company's operations, compliance and personnel.

Given the typically suspicious and often international nature of cryptocurrency transactions, meeting AML requirements will be challenging, will require a massive compliance infrastructure, and will create many anticipated and unanticipated consequences. Meanwhile, MSB regulation is state-based — with each state promulgating its own priorities and requirements ranging from record-keeping and bonding to audits and reporting.

For instance, a cryptocurrency firm could be subject to on-site audit and scrutiny of individual transaction activity for AML compliance, which in turn could lead to institutional and management civil liability, penalties, fines, license revocation — even potential criminal exposure for individuals caught intentionally circumventing AML obligations.

Indeed, only a few months ago, in January 2018, New York State Financial Services Superintendent Maria T. Vullo announced that Western Union agreed to pay a $60 million fine as part of a consent order with the New York State Department of Financial Services for violations of New York Bank Secrecy Act and AML regulations. An investigation by DFS found that Western Union failed to implement and maintain an anti-money laundering compliance program to deter, detect and report on criminals' use of its electronic network to facilitate fraud, money laundering and the illegal structuring of transactions below amounts that would trigger regulatory reporting requirements.

Vullo stated at the time:

> Western Union executives put profits ahead of the company's responsibilities to detect and

> prevent money laundering and fraud, by choosing to maintain relationships with and failing to discipline obviously suspect, but highly profitable, agents. DFS will not tolerate unlawful activity that undermines anti-money laundering laws and endangers the integrity of our financial system.

Clearly, the noxious mix of AML and MSB federal and state regulatory requirements not only creates a foggy, deadly compliance labyrinth for any financial firm — but is also replete with risk.

In addition, even more alarming, AML failures provide an ideal, straightforward and wide-ranging criminal prosecutorial hook for federal law enforcement authorities. For instance, in 2015, in addition to being charged for violating computer crime Title 18 U.S.C., Section 1030(a)(7), 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 that 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, or SARs, regarding customers who use cryptocurrencies for nefarious purposes.

4. Auchterlonie and Garnett claim that the U.S. Commodity Futures Trading Commission's jurisdiction is limited — but, although the authors are correct with respect to the CFTC's jurisdictional boundaries, they miss a key takeaway from the SEC/CFTC collaboration.

The frequent crypto coupling of the chairmen of the CFTC and SEC, from their co-authored Wall Street Journal op-ed piece to their joint congressional testimony to their joint statements, evidences an unprecedented level of collaboration and coordination. Historically, the SEC/CFTC relationship has occasionally been a rocky one, laden with regulatory quibbling and even dislike. But with respect to crypto financing, it is a virtual love fest.

The two agencies are working closely together, sharing information, developing mutually beneficial strategies, and "carving up" jurisdiction with graciousness and mutual respect. This collaboration

between the CFTC and SEC foretells a prolonged and coordinated federal response to ICOs, cryptocurrency exchanges and the like — and is clearly a cause for alarm.

5. Auchterlonie and Garnett make no mention of the dark side of cryptocurrency, which will continue to attract increased attention to, and scrutiny of, ICO promoters and cryptocurrency exchange operators.

The underlying product of ICOs and crypto exchanges is not a harmless product like Pokémon cards, Jordan sneakers or some other appreciating and collectable chattel. Rather, ICO tokens represent a pseudo-anonymous currency that has unfortunately evolved into the payment mechanism of choice for unlawful transactions — from buying a fake I.D. or a bottle of opiates, to receiving a cache of credit card numbers or stolen identities, to collecting a ransomware payment demand or even for funding terrorist-related activities. Slowing the growth of this unlawful behavior is a notion that appeals not just to market participants, but also to the myriad victims of

behavior is a notion that appeals not just to market participants, but also to the myriad victims of crypto-funded ransomware, terrorism, drug dealing and the like. The government, in particular FinCEN, is acutely aware of the dark side of cryptocurrency use — and newly appointed FinCEN director Kenneth Blanco, a former U.S. Department of Justice AML expert, has testified before Congress about the threat of virtual currencies and has dedicated increasing resources along those lines.

6. Auchterlonie and Garnett fail to recognize the gravity of the SEC's allocation of significant, specialized and dedicated resources to ICOs, cryptocurrency exchanges and the like.

In late September 2017, just a few months after the DAO 21(a) report and the SEC ICO investor bulletin, the SEC announced the formation of a new cyber unit to target violations involving distributed ledger technology and ICOs as part of a new effort to fight cybercrime. The new cyber unit is also chartered specifically to pursue "misconduct perpetrated using the dark web," where bitcoin and other cryptocurrencies are used to pay for illicit goods.

Separate from the cyber unit, the SEC also created a retail strategy task force that will "develop proactive, targeted initiatives to identify misconduct impacting retail investors." While this task force's mission was not described as specifically aimed at the crypto space, ICOs and cryptocurrency exchanges are clearly one of its targets, especially given the explosive interest in crypto investments by traditional retail investors. This new team will "apply the lessons learned from [past securities fraud] cases and leverage data analytics and technology to identify large-scale misconduct affecting retail investors."

This is not the first time the SEC has established a specialized unit to manage cybercrimes. From 1998 to 2009, before being merged with the SEC's Office of Market Intelligence, the SEC created the Office of Internet Enforcement, the first specialized cyber group. OIE led a broad range of SEC enforcement actions, initiatives and investigations, many filed parallel to criminal prosecutions. The original cyber group faced a similar threat in the form of unlawful offerings conducted via the internet and came out swinging against those frauds, leading five internet fraud sweeps in its first two years.

Auchterlonie and Garnett also fail to mention that the new cyber group also swallowed up the SEC's Distributed Ledger Technology Working Group, naming its leader as one of its assistant directors. Moreover, two assistant directors within the new cyber group were actually members of the original OIE, which adds an extraordinary and immediate level of experience and expertise to the new cyber group's ranks.

Clearly, ICOs and other cryptocurrency issues will be the primary focus of this new cyber group, and if history is at all telling, conducting crypto-related sweeps will be among the reactivated cyber group's early prosecutorial maneuvers. Given the SEC's formation of its own specialized squadron, whose sole purpose every day is to investigate and prosecute crypto-related financiers, ICO purveyors and cryptocurrency exchanges should clearly be sounding the alarm.

7. Auchterlonie and Garnett assert that given SEC budgetary woes, the SEC lacks resources to convert the 100-plus crypto-related subpoenas the SEC has reportedly recently issued into actual SEC cases, but cryptocurrency-related enforcement actions are not a drain on resources.

By citing SEC budgetary woes, Auchterlonie and Garnett not only discount an eager, dedicated and experienced SEC staff (accustomed to working with limited budgets), but the authors also miss a glaring point about crypto-related investigations. Former SEC enforcement lawyers we have talked to attest that crypto-related cases are not difficult, cumbersome or costly to investigate — and do not require much in terms of resources. Here's why:

Cryptocurrency-related investigations are not like accounting frauds, market manipulations or complex insider trading cases, requiring extensive review of financial statements, audit trails and/or market data. Nor do crypto-related investigations typically require the conducting of intense financial or digital forensics, lengthy document reviews, and/or multiple testimonial proceedings. Instead, crypto-related investigations actually require scant evidence gathering.

In fact, the internet provides SEC staff a glimpse into cryptocurrency exchange operations and ICO promotions as they unfold without ever using a subpoena. This has proven to be the most

profound change wrought by the internet in the field of securities regulation. Far from tying regulators hands, the internet has become the virtual rope that many cyber thieves use to hang themselves. Moreover, unlike hackers trying to tamper with the energy grid or clandestinely trying to intrude into the computer networks of public companies, cryptocurrency financiers want to be found. They require a wide audience to review their information, invest in their offering or participate in their exchange. Rather than hide amid the unseen underbelly of the internet, ICO promoters and cryptocurrency exchange operators peddle their services in plain view 24-7 — and can be actively observed from virtually anywhere on the planet.

Relatedly, outside of fraud claims, most SEC crypto-related violations are strict liability, requiring little in the way of scienter, conspiracy or even motive. Simply stated, as a matter of law, every securities offering is either registered, exempt or unlawful — regardless of what anyone in the process honestly believes or testifies.

Final Thoughts

While Auchterlonie and Garnett have every right to believe their crypto clients should not be alarmed by recent regulatory and law enforcement crypto-related efforts, we would strongly urge them to reconsider.

Clayton recently gave an extraordinary speech at the 2018 Securities Regulation Institute in Washington, D.C., adding a new twist to his crypto combat plan — hit the lawyers involved, and hit them hard, moving law firms and attorneys, the so-called "gatekeepers" connected to ICOs and cryptocurrency exchanges, to front and center on the SEC's radar.

By providing the kind of legal advice that can land a client into the SEC's investigative, regulatory and prosecutorial crosshairs, or even worse, into the crosshairs of criminal investigators and prosecutors, lawyers now risk more than just their reputations and livelihoods. Per Clayton, lawyers risk being investigated or prosecuted right beside their crypto clients, no matter what the lawyer's defense and no matter how much the lawyer's good faith.

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.