New York Law Journal
SERVING THE BENCH AND BAR SINCE 1888
WWW.NYLJ.COM
An ALM Publication
VOLUME 259—NO. 34
WEDNESDAY, FEBRUARY 21, 2018

Outside Counsel

Bitcoin Things Have Small Beginnings

BY BRIAN R. MICHAEL, KYLE SHEAHEN AND KATIE BARRY


Bitcoin

In 2010, the value of one bitcoin was never more than a single U.S. dollar. A lot has changed. Now, one is reminded of what Dryden told General Murray in *Lawrence of Arabia*: "Big things have small beginnings, sir." And the bigger things get, the more people take notice.

Bitcoin and other cryptocurrencies—ethereum, monero, litecoin, to name a few—have surged in popularity. They have gained tremendous visibility due to increases, and dramatic fluctuations, in value. Blockchains are now being used in global commerce for countless transactions.

We have come a long way since the Dread Pirate Roberts and the days when cryptocurrencies were infamous for purchasing illicit goods on the dark web. Crypto is going mainstream.

> It is critical for any entity involved in cryptocurrencies to stay abreast of the rapidly evolving regulatory landscape and implement basic risk reduction protocols.

This has brought increased financial market sophistication, such as cryptocurrency futures and exchange-traded funds. And of course government authorities are paying much closer attention to look for potential fraud and abuse as crypto comes of age. It is therefore critical for any entity involved in cryptocurrencies to stay abreast of the rapidly evolving regulatory

BRIAN R. MICHAEL, *a partner at King & Spalding, is a former federal prosecutor in New York and Los Angeles.* KYLE SHEAHEN *is a senior associate and* KATIE BARRY *is an associate at the firm. The authors are members of the firm's special matters and investigations practice.*

landscape and implement basic risk reduction protocols.

Enforcement Developments

U.S. regulators have trained their sights on the market for bitcoin and other cryptocurrencies. In July 2017, the SEC made it clear that digital tokens could be securities and Initial Coin Offerings (ICOs) could therefore be regulated under the securities laws, which Chairman Jay Clayton has repeatedly reaffirmed. The SEC further warned about ICOs in August 2017 when it issued an investor alert stating that while some ICOs may be legitimate, a company also might use an ICO or token-related event to manipulate its perceived value. The SEC then ramped up its enforcement capacity in September 2017 by creating a "Cyber Unit" to focus on misconduct with distributed ledger technology and ICOs.

Chairman Clayton has made a number of public remarks on the status and risks of cryptocurrencies. He expressed concerns last year about a "distinct lack of information" in online platforms listing cryptocurrencies, noting that trading on these platforms is susceptible to price manipulation and other forms of fraud. In a January 2018 interview, he further highlighted a focus on exchanges where cryptocurrencies are bought and sold as these lightly regulated exchanges may be easily manipulated, which investors do not always understand. Appearing before the Senate Banking Committee on Feb. 6, 2018, Chairman Clayton stated in written testimony that the SEC would look closely at public companies shifting their business models to "capitalize on the perceived promise of distributed ledger technology." The Chairman emphasized this point even further in his testimony, noting these platforms may deceive investors because they appear similar to registered and regulated securities markets and exchanges, but in reality lack investor protections found on registered exchanges.

> It is imperative for companies and investors alike to familiarize themselves with the evolving regulatory environment, take steps to reduce attendant legal risk, and vigilantly watch and account for new developments.

While this SEC spotlight on cryptocurrencies is not new, and there have always been concerns about fraud, recent enforcement activity indicates that it is shifting into a new, higher gear. On Jan. 30, 2018, the SEC halted an ICO of Dallas-based AriseBank. In December 2017, the SEC suspended trading in shares of The Crypto Company amid concerns about the accuracy of available public information, suspended the ICO of Munchee because of registration concerns and an undercurrent of potential fraud, and obtained an emergency order freezing assets in the ICO of PlexCorps. These actions followed the SEC's suspension of trading of several issuers including First Bitcoin Capital, CIAO Group, Strategic Global, and Sunshine Capital due to issues with their ICOs and other trading incidents. Chairman Clayton has shown that regulatory focus going forward will not be limited to issuers of unregistered securities, as he recently warned "gatekeepers"—including bankers, lawyers, and accountants that help introduce these securities into the market—to be wary of necessary investor protections and disclosures following recent enforcement actions. Chairman Clayton's written Senate testimony emphasized this point further, pressuring market participants to ensure their crypto activity does not undermine AML/KYC obligations.

Other financial regulators in the United States are also increasingly getting into the crypto game. The CFTC and FinCEN have weighed

in, with the CFTC having classified cryptocurrencies as regulated commodities and FinCEN issuing guidance on registration requirements. CFTC Chairman Christopher Giancarlo recently joined Chairman Clayton in publishing a Wall Street Journal Op-Ed warning market participants of stronger forthcoming regulation, and that regulators will "work together to bring transparency and integrity to [cryptocurrency] markets," regardless of whether an offering is labeled as a "coin," "utility token" or anything else. Appearing alongside Chairman Clayton earlier this month before the Senate Banking Committee, Chairman Giancarlo noted in his written testimony that the CFTC has also created a virtual currency enforcement task force to work cooperatively with its SEC counterpart as the two agencies look to navigate their respective jurisdictional lines and enforcement authority. FINRA is also in the mix, having warned investors about the dangers in cryptocurrency trading. State authorities—such as those in New York and California—are paying close attention, too. On Feb. 7, 2018, New York's Department of Financial Services released new guidance reminding all state-licensed virtual currency entities that they must implement measures to effectively detect, prevent and respond to fraud, attempted fraud, and similar wrongdoing, and to be particularly vigilant in preventing market manipulation efforts.

Like the SEC, the CFTC has also flexed its enforcement muscles, having charged My Big Coin Pay, Inc. and two individuals with commodity fraud and misappropriation, after they allegedly misappropriated over $6 million from customers in connection with a virtual currency known as My Big Coin and charging Coin Drop Markets with fraud and misappropriation connected to purchasing and trading bitcoin and litecoin. These cases followed a September announcement that the CFTC filed an enforcement action against hedge fund Gelfman Blueprint Inc. and its CEO, charging them with fraud, misappropriation and issuing false statements in connection with an alleged bitcoin Ponzi scheme.

Not to be outdone, the Justice Department remains active on the criminal side. A New York woman was recently indicted and charged with bank fraud and money laundering offenses after allegedly converting over $85,000 into bitcoin and other cryptocurrencies before laundering it and sending it abroad to support ISIS. DOJ also investigated a Russian individual and organization operating as a bitcoin exchange for allegedly operating an international money laundering scheme in late July 2017.

Practical Considerations

What does this dizzying array of headlines and activity mean for cryptocurrency investors, exchanges, and others operating in this realm? At the bottom, it means that law enforcement is finding its footing with respect to cryptocurrency cases now that securities law and other considerations have joined anti-money laundering offenses as a central area of concern.

One approach might be to avoid crypto altogether. But because we are now in a world where cryptocurrencies and the blockchain are becoming more a part of mainstream commerce, it is wise for anyone in the space to take a few practical steps to reduce legal risks and operate with greater confidence.

First, companies must evaluate their internal controls surrounding cryptocurrencies. Don't have policies addressing the risks inherent in cryptocurrencies? It's time to consider implementing some, or updating existing

policies that are business-specific and take into account the jurisdictions where the company operates, while staying up-to-date on the latest regulatory developments. Procedures should include effective training and education for employees, internal monitoring and auditing, and well-publicized disciplinary guidelines.

While the issue of whether cryptocurrencies are securities is still being debated and even litigated, best practice for now is to assume that in most instances they are and regulators will treat them as such. Recent enforcement activity shows that market manipulation, insider trading, and anti-money laundering concerns should be high on the agenda. On market manipulation, entities should monitor disclosures for indicators of potentially problematic statements. For example, outlandish claims about high returns or statements pressuring investors to make snap purchases may be a red flag for fraud. Companies also should train their employees on insider trading issues and the potential for serious consequences to their employees. It is critical to be vigilant about identifying which employees have access to material nonpublic information and the context in which they have acquired it.

While anti-money laundering concerns surfaced long ago in the cryptocurrency space, remembering a few AML/KYC basics will also go a long way. Companies should establish customer verification and identification programs, as well as controls for identification of suspicious transactions. This can be a difficult balance when crypto customers prize privacy, but steps should be taken to know who is on the other side of a transaction and who really owns the wallet(s) (i.e., account) at issue.

Investors in cryptocurrencies should understand the potential for fraud and abuse and conduct proper due diligence on exchanges and sellers of cryptocurrencies. Information about newer cryptocurrencies can be scarce and investors should be cautious of offerors and exchanges with an unproven track record. Hacking and theft are also ever-present concerns and steps should be taken to monitor wallets for evidence of unauthorized intrusions. And if things go upside down, the government may not be able to come to the rescue. Chairman Clayton did not mince words in his remarks: "If you lose money, there is a substantial risk that our efforts will not result in a recovery of your investment."

What's Next?

Regulators of all stripes are focused on cryptocurrencies and 2018 will certainly bring more enforcement activity. As cryptocurrencies continue to find their way into the portfolios of main street investors, authorities will take action to protect them with all the tools at their disposal. It is imperative for companies and investors alike to familiarize themselves with the evolving regulatory environment, take steps to reduce attendant legal risk, and vigilantly watch and account for new developments.

In *Lawrence of Arabia*, Dryden also said "we all have troubles. Life is a vale of troubles." But cryptocurrencies need not add to those troubles when appropriate precautions are in place.