LJN LAW JOURNAL NEWSLETTERS

Business Crimes Bulletin ®

An ALM Publication

Volume 25, Number 3 • November 2017

New-Wave Legal Challenges for Bitcoin and Other Cryptocurrencies

By Robert J. Anello and Christina Lee

As the adoption of cryptocurrencies — or digital currencies that are encrypted for security — spreads throughout the business and financial sectors, so too do the concerns that lack of regulation render the new-age currency susceptible to fraud, manipulation, and to being used as a vehicle for money laundering. Nevertheless, recent efforts by U.S. enforcement agencies to apply and enforce financial regulations indicate that cryptocurrency-based transactions will be under greater scrutiny than ever before.

The Securities and Exchange Commission (SEC) recently issued a report suggesting that it broadly considers Initial Coin Offerings (ICOs) — a popular method of raising investment funds through cryptocurrency, which function like traditional securities offerings — to be subject to federal securities laws, and has since established a Cyber Unit that will target securities violations involving ICOs. Now, those involved in global ICOs and similar transactions will need to consider whether the cryptocurrencies concerned are securities, as well as the extent to which U.S. securities laws apply to such transactions made outside the United States.

In a recent shot across the bow after issuing its report, the SEC filed an emergency TRO to freeze the assets of a Brooklyn-based businessman and two of his companies in an attempt to halt two ongoing ICOs, including one that the SEC claimed was disguised as a club membership. The Department of Justice (DOJ) too has recently weighed in. In July, the DOJ brought criminal charges against BTC-e, a major foreign platform for buying and selling virtual currencies, and its Russian operator for violations of U.S. anti-money laundering laws. Other countries, including the United Kingdom and Japan, similarly have indicated that regulatory reform to address cryptocurrency growth is on the horizon. In light of this enforcement environment, those using cryptocurrency to do business need to pay attention to the rules of financial regulatory compliance and the possibility of defending civil or criminal charges.

What Is Cryptocurrency?

Cryptocurrencies are digital currencies that allow users to securely send or receive payment on the Internet. Unlike fiat currencies — such as dollars, euros, pounds or yen, which are legal tender regulated by the governments — cryptocurrencies have no central regulatory authority and operate through decentralized networks of computers. Because cryptocurrency transfers are encrypted and permanently recorded on a digital ledger, third parties (at least in theory) cannot tamper with payments, thereby providing security and privacy both for the sender and the receiver. Cryptocurrencies also are a hyped low-cost alternative to using banks, money transfer companies or brokers, all of which can charge hefty fees for transferring funds internationally.

Robert J. Anello

Christina Lee

Cryptocurrency Growth and Ongoing Concerns

As cryptocurrencies have become more well known, they increasingly have been embraced as legitimate forms of alternative payment. Several large companies, including Microsoft, Overstock.com, and DISH Network, along with hundreds of thousands of other vendors worldwide, now accept various cryptocurrencies. The broader adoption of this virtual payment method also has popularized the concept of using cryptocurrency to fund businesses and investments and has generated

Robert J. Anello, a member of *Business Crimes Bulletin's* Board of Editors, is a partner in Morvillo Abramowitz Grand Iason & Anello P.C. **Christina Lee** is an associate with the firm.

cryptocurrency exchanges around the world. These exchanges, such as Coinbase and Bitfinex, allow people to buy, sell, and transfer funds across cryptocurrencies and central bank-backed currencies, such as dollars and euros.

This year, cryptocurrency trading reached new heights. In September, cryptocurrency trading posted a record $11 billion in trading volume according to *Cryptocoins News*, an industry tracking website. According to a recent article in *The Financial Times*, software developers have raised more than $1.3 billion in 2017 from the sale of new virtual currencies with names like Tezzies, Atoms, and Basic Attention Tokens.

As new applications of cryptocurrencies develop, concerns about virtual currencies abound. Skeptics of these trend-setting currencies point to the fact that cryptocurrencies attract transactions connected to illicit and criminal activity, including money laundering, identity theft, fraud, drug sales, tax evasion, and ransom, due to their encrypted and unregulated nature. Other critics worry about the price volatility of these currencies stemming from fluctuations in demand for bitcoins and other cryptocurrencies, and the uncertain regulatory landscape for cryptocurrency. The most infamous example of cryptocurrencies' vulnerabilities is Mt. Gox, which at one point was the leading exchange for Bitcoin, one of the first and largest virtual currencies. In 2014, Mt. Gox collapsed after acknowledging that the exchange had lost hundreds of millions of dollars in bitcoin for reasons that were unclear but which may have included theft, fraud or mismanagement of the exchange.

SEC Cracks Down on Initial Coin Offerings

Over the last few months, the SEC has demonstrated that it intends to pursue enforcement of securities law on certain cryptocurrency transactions, especially increasingly popular ICOs, in response to concerns about fraud and manipulation. In an ICO, virtual coins or tokens are distributed by a company to the public in exchange for another cryptocurrency or fiat currency. These coins or tokens come with particular rights, which could range from a right to access software, redeem the token for a currency or service, or receive future earnings from the company. In September, the SEC announced the creation of a new Cyber Unit within the Enforcement Division that will focus on, among other cyber-related issues, targeting securities violations involving ICOs. This announcement came in the wake of guidance from the SEC on the risks of investing in ICOs, as well as an illuminating report on its investigation into potential securities law violations by The DAO, an Internet-based organization that operated as decentralized venture capital fund.

Cryptocurrencies … are a hyped low-cost alternative to using banks, money transfer companies or brokers, all of which can charge hefty fees for transferring funds internationally.

Although the SEC ultimately decided not to pursue an enforcement action, or make findings of any violations, in connection with The DAO, it nevertheless made the investigation report public to provide insight into the SEC's view on how U.S. securities laws apply to offers and sales of coins, tokens and other cryptocurrencies. According to the SEC's report, The DAO raised funds for projects by offering "DAO Tokens" to investors in exchange for Ether, one of the most popular virtual currencies. Investors who owned DAO Tokens could choose to share in the anticipated earnings from projects as a return on their investment, or resell their Tokens on a secondary market. By mid-2016, The DAO had raised the equivalent of $150 million from approximately 11,000 investors but then fell victim to a cyber attack. Although The DAO quickly acted to avoid any loss to DAO Token holders, this cyber attack prompted the SEC to investigate potential securities law violations by The DAO.

In its report, the SEC asserted that the offers and sales of DAO Tokens were subject to securities regulation, because DAO Tokens constituted an "investment contract," which is a "security" under the Securities Act and the Exchange Act. To come to this conclusion, the SEC analyzed the Tokens under the "investment contract" test adopted by the U.S. Supreme Court in *SEC v. W.J. Howey Co.*, 328 U.S. 293 (1946). Under the *Howey* test, an "investment contract" is "a contract, transaction, or scheme in which: (1) a person invests something of value (2) with a reasonable expectation of profit (3) derived from managerial efforts of others."

The SEC concluded that the DAO Tokens met all three requirements. First, the investors paid "contribution of value" for the Tokens, because Ether was comparable to money or a good. Second, the investors who purchased Tokens reasonably expected profits, because various marketing material repeatedly stated that The DAO's objective was to fund projects that would provide a return on investment. Third, Token holders relied on managerial efforts of others, including "curators" of the fund. Importantly, similar to investors who hold a traditional security, the SEC concluded that the Token holders had diminished voting rights and lacked the ability to exercise meaningful control of the company. Therefore, the Token holders had to rely on the managerial efforts of others at The DAO. Once the SEC determined that DAO Tokens were securities, it concluded that The DAO was required to register any offer or sale of DAO Tokens under the

Exchange Act, and that any secondary exchange in which these tokens were traded similarly needed to be registered under the Exchange Act.

Although the SEC declined to bring an enforcement action against The DAO, in a recent action filed with the Eastern District of New York, the SEC charged Maksim Zaslavskiy and his two companies with defrauding investors in connection with two ongoing ICOs. The SEC obtained an emergency TRO freezing Zaslavskiy's assets. The SEC alleged that the defendants offered "coins" or "tokens" as disguised as a club "membership" and raised at least $300,000 from investors, according to the SEC, by misrepresenting expected returns on investments and the companies' operations. Although the defendants characterized one of the two offerings as "membership" in the Diamond Reserve Club, a group that purported to invest in diamonds, the SEC saw the "membership" as a "security," because: 1) investors allegedly were offered "membership" with the expectation of profits; 2) based on efforts of Diamond Reserve Club to invest in diamonds; and 3) investors had limited ability to take action with respect to Diamond Reserve Club's infrastructure and development.

The SEC's report suggests that the agency is taking a broad view concerning the application of securities laws with respect to innovative transactions involving virtual currency. Under the SEC's analysis in the report on The DAO, any type of cryptocurrency "coin" or "token" that is exchanged for either traditional money or another cryptocurrency with the expectation of profit based on the work of others would be subject to federal securities laws. Thus, regardless of the novelty of transaction type, those involved in cryptocurrency transactions who determine that the transactions function similarly to traditional securities offerings or sales need to consider whether their offering must comply with disclosure, registration, and antifraud provisions of securities laws.

Non-U.S. Defendants Face Uncertain Securities Fraud Liability

The treatment of ICOs as securities offerings raises the question about the extent to which U.S. securities laws would apply to securities transactions involving cryptocurrencies that occur outside the United States. In the 2010 case of *Morrison v. National Australia Bank*, 561 U.S. 247, the Supreme Court carefully defined the limits of U.S. securities laws to transactions outside the United States. The Supreme Court held that U.S. statutes do not apply outside the United States unless clear indication exists in the statute that Congress intended such an extraterritorial reach. The Court interpreted the Exchange Act as having no clear indication that the securities fraud provision applied extraterritorially. In doing so, the Supreme Court limited the securities fraud provision to applying only to securities transactions listed on U.S. exchanges and the purchase or sale of any other security in the United States. Under *Morrison*, only claims connected to a security sold or listed on a U.S. exchange or sold or purchased in the United States can be litigated in U.S. courts.

Only a few weeks after *Morrison* was decided, Congress passed the Dodd-Frank Act. Under the Act, U.S. courts have jurisdiction over claims of securities violations brought by the SEC or DOJ that involve: 1) significant steps in furtherance of a violation that occurred in the United States even if the transaction took place outside the United States; or 2) conduct outside the United States that has a "foreseeable substantial effect" within the United States. The majority of U.S. courts have not yet opined on whether or how this Dodd-Frank Act provision alters the limitation set out in *Morrison*.

The uncertainty surrounding the extent to which U.S. securities laws apply to non-U.S. based transactions presents a challenge in evaluating securities liability with respect to ICOs and other cryptocurrency-based transactions outside the United States. Cryptocurrency transactions often involve parties dispersed across various countries, and the entities doing business in virtual currency often do not have a physical location, and operate only through an Internet website. For example, under *Morrison*, The DAO likely would only have to be concerned about facing securities fraud charges for those tokens sold in the United States or tokens sold on U.S. exchanges despite having sold tokens to thousands of foreign customers. Under the Dodd-Frank Act, U.S. courts have jurisdiction over claims involving token sales made outside the United States as long as wrongful conduct had occurred in or had a foreseeable substantial effect within the United States. Because cryptocurrencies transactions and exchanges by nature are not limited by jurisdiction, businesses conducting a large volume of securities transactions in cryptocurrencies should consider whether their conduct will have substantial effects within the United States.

Regulators Take Aim at Money Laundering Enabled By Virtual Currencies

Because cryptocurrency transactions are encrypted and decentralized by nature, virtual currencies continue to provide a convenient method of transferring funds obtained from illegal activities without risk of a central authority discovering the funds' illicit nature. On the other hand, transactions involving traditional financial actors, such as banks, brokers and dealers, and money service businesses, are subject to U.S. anti-money laundering laws and regulations aimed at detecting and reporting suspicious activity, including money laundering and terrorist financing, as well as predicate offenses like securities fraud and market manipulation. Nevertheless, the recent message from U.S. enforcement agencies is that, going forward, they will be enforcing anti-money-laundering regulations

upon virtual currency exchanges, even those operating outside the United States. This past July, the DOJ brought criminal charges against BTC-e, a major foreign Bitcoin exchange for anti-money-laundering violations; and against Alexander Vinnik, a Russian national who operated BTC-e, for operating an unlicensed money service business and for money laundering and engaging in unlawful monetary transactions. The Financial Crimes Enforcement Network (FinCEN) also imposed a $110 million fine against BTC-e for anti-money-laundering violations, and $12 million against Vinnik for his role in these violations.

As a part of this enforcement effort, BTC-e temporarily shut down for several days after U.S. enforcement agents seized BTC-e's domain in anticipation of the criminal charges brought against the exchange.

According to the DOJ and FinCEN, BTC-e fell under the definition of a "money transmitter," because it served as a platform for the offer and sale of virtual currencies. Under anti-money-laundering regulations, money-transmitting businesses are required to register with the U.S. Treasury Department; implement an anti-money-laundering program, policy, and controls; have a program to collect customer identification information and report suspicious activity; and maintain proper records. According to the DOJ and FinCEN, BTC-e willfully failed to meet these requirements. 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.

The BTC-e case 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. Under anti-money-laundering regulations, foreign-based money transmitting businesses doing substantial business in the United States must comply with the regulations. Although BTC-e was not based in the United States, DOJ and FinCEN determined that U.S. anti-money-laundering rules applied because a significant number of transactions — more than 21,000 bitcoin transactions worth over $296 million according to FinCEN — were sent to, and received from, customers in the United States.

Looking at the case of BTC-e, going forward, cryptocurrency exchanges, including those operating outside the United States, will need to understand and comply with U.S. anti-money laundering requirements if they seek to have a significant U.S. customer base. Moreover, DOJ's and FinCEN's willingness to pursue criminal charges and significant civil fines — $110 million for BTC-e and $12 million for Vinnik, respectively — is a sign that cryptocurrency exchanges and individuals involved in these exchanges should be prepared to face significant fines and possibly even criminal charges if exchanges choose not to comply with U.S. anti-money-laundering requirements, even if the companies are operating outside of the United States.

International Response to The Cryptocurrency Boom

U.S. regulatory enforcement agencies are not alone in beginning to respond to the boom in virtual currency. Countries around the world have begun to review cryptocurrency to evaluate and assess potential changes to the laws and regulations related to it.

China has wholly banned ICOs and shut down cryptocurrency exchanges due to money laundering and security concerns. Other countries, including the United Kingdom, Japan and Australia, have taken a less extreme approach, striving to balance the need to address the potential for fraud and money laundering while taking care not to stifle the growing cryptocurrency economy. For example, on Sept. 12, the United Kingdom's Financial Conduct Authority (FCA) posted a statement regarding ICOs, noting that whether "an ICO falls with the FCA's regulatory boundaries or not can only be decided case by case." Japan and Australia have responded by making serious efforts to regulate cryptocurrency more generally. Earlier this year, Japan issued a new law requiring cryptocurrency exchanges to operate under the Japanese Financial Services Agency.

In August, the Australian government made a similar move with a proposed set of reforms to bring digital currency exchange providers under the Australian Transactions and Reporting Analysis Centre (AUSTRAC). Because cryptocurrency more often than not involves cross-border transactions, one or more jurisdictions will likely be implicated as countries develop their own regulations on cryptocurrency. Coordination across different countries will be a key aspect of the regulation and enforcement effort in the future.

Conclusion

Given the innovative nature of cryptocurrency, novel uses of this virtual currency — like initial coin offerings — are only expected to rise. In response to increased activity and new applications of cryptocurrency, U.S. enforcement agencies have become aggressive in the pursuit of securities and financial regulatory violations by cryptocurrency exchanges, investment funds based on cryptocurrencies, and individuals. Cryptocurrency advocates, participants, and innovators must be prepared for the potential regulatory and criminal implications as cryptocurrency transactions evolve.

—❖—