ICOs and Cryptocurrencies: How Regulation and Enforcement Activity Are Reshaping These Markets

Recent global regulatory developments have brought into sharp focus the impact of regulators and the potential for enforcement activity on the nascent world of initial coin offerings (ICOs) and cryptocurrencies. While some welcome these developments as providing much-needed guidance as to what is legally permissible in this space, others feel that any regulatory or enforcement activity will hamper the evolution and adoption of this technology. Nonetheless, regulations, and the enforcement actions that may follow, are very much a reality of the cryptocurrency and ICO worlds.

As discussed below, recent bans or limits on ICOs in China and Singapore have created some uncertainty as to the future of ICOs in certain markets, while pronouncements in other jurisdictions, such as Singapore, Hong Kong and the U.K., have suggested that ICOs can be structured in a legally compliant manner. The U.S. has provided some mixed signals in this area. As also discussed below, regulation of cryptocurrencies and ICOs needs to be distinguished from how regulators generally view blockchain, also known as "distributed ledger technology," which is the revolutionary technology that underlies cryptocurrencies and most ICOs. Here regulators have been more receptive, going so far as to encourage its use.

Regulations, and the enforcement actions that may follow, are very much a reality of the cryptocurrency and ICO worlds.

The Regulatory and Enforcement Landscape

Blockchain technology provides a means for network participants to exchange items of value through a distributed network structure that does not require a central trusted authority. These structures, which are very much in a nascent stage, offer improved security, transparency, efficiency and cost-reduction benefits. Bitcoin, the first widely adopted cryptocurrency, has been followed by a number of other cryptocurrencies. More recently, entrepreneurs have sought to raise money, typically for blockchain projects, by selling "tokens" — a type of blockchain coin. Some entrepreneurs are selling these coins as a form of investment security, while others are positioning their tokens as "utility tokens" that provide access to a blockchain platform that is being built. Given the amount of money being funneled into cryptocurrencies and ICOs, which have raised over $3 billion this year, it is not surprising that these initiatives have drawn close regulatory attention in a number of jurisdictions.

US Securities and Exchange Commission

Recently, the U.S. Securities and Exchange Commission (SEC), which has been studying the effects of distributed ledger and other innovative technologies, released a Section 21(a) Report of Investigation finding that ICOs that issue digital tokens in exchange for fiat or

digital currencies and that offer a return on this investment may be subject to U.S. securities laws. While the SEC Report focused on The DAO, a virtual organization that raised $150 million through an ICO in 2016, it contained sweeping language on the use of ICOs more generally.

The SEC found that The DAO improperly offered and sold securities. In making its determination, the SEC did not create a new regulatory framework; rather, it applied the same test to determine whether an offering was a security that has existed since the landmark U.S. Supreme Court decision in *SEC v. Howey*, 328 U.S. 293 in 1946.[1] ICOs that meet this test must be registered with the SEC or be performed pursuant to an exemption from registration. ICOs may also need to comply with the requirements of Regulation Crowdfunding and other securities laws more generally. Thus, entities that are involved in initial coin or token offering activities must consider the accounting, disclosure and reporting guidance based on the nature of their involvement. In addition, exchanges that allow for the trading of ICO tokens, as well as the firms and professionals who offer, transact in or advise on investments related to such tokens, may also need to be registered or licensed, or avail themselves of a valid exemption. Stephanie Avakian, co-director of the SEC's Enforcement Division, emphasized: "The innovative technology behind these virtual transactions does not exempt securities offerings and trading platforms from the regulatory framework designed to protect investors and the integrity of the markets."[2]

In conjunction with this report, the SEC issued an Investor Bulletin to make investors aware of the potential risks of participating in ICOs. The Bulletin provided a background on ICOs, blockchain technology and virtual currencies while also guiding investors through issues they should consider when determining whether to participate in an ICO. Those issues include whether the offering has been registered with the SEC, whether offerings described as crowdfunding are offered and sold in compliance with the requirements of Regulation Crowdfunding or with the federal securities laws generally, whether the blockchain is open and public, and whether there has been an independent cybersecurity audit of it.

The SEC Divisions of Corporate Finance and Enforcement also issued a statement following the Report of Investigation on The DAO noting that they "welcome and encourage the appropriate use of technology to facilitate capital formation and provide investors with new investment opportunities" while also being mindful of their "obligation to protect investors and recognize that new technologies can offer opportunities for misconduct and abuse."[3] The statement encouraged market participants to consult with securities counsel or contact SEC staff for assistance in analyzing the application of the federal securities laws. It also warned investors to be mindful of traditional red flags when making investment decisions.

SEC Chairman Jay Clayton emphasized in a follow-up statement that the U.S. government supports innovation in this space, but that its top priority would continue to be the protection of investors and markets. In line with this statement, in a November 2017 speech, Chairman Clayton said that ICOs in many cases looked like securities, suggesting that firms using ICOs would need to follow the SEC's rules and regulations. He also warned that many online platforms that list and trade virtual coins or tokens may be susceptible to manipulation or other fraudulent practices.

On November 1, 2017, the SEC also stated that endorsements by celebrities and others who use social media networks to encourage the public to promote ICOs, purchase stocks and other investments may be unlawful under the anti-touting provisions of the federal securities laws if they do not disclose the nature, source and amount of any compensation received in exchange for the endorsement.[4] Persons making these endorsements may also be liable for potential violations of the anti-fraud provisions of the federal securities laws, for participating in an unregistered offer and sale of securities, and for acting as unregistered brokers. The SEC further encouraged investors to be wary of investment opportunities that "sound too good to be true."

Consequences of the SEC Announcements

Although the SEC's announcement was seen by many as a welcome clarification, it has significant ramifications for ICOs that are open to U.S. investors and to digital asset trading platforms, which may be required to register as national securities exchanges and be subject to new regulations.

The SEC has already started to follow through on its enforcement strategy related to ICOs. On September 29, 2017, it announced that it charged an individual and two companies related to him with violations of the anti-fraud and registration provisions of the federal securities laws. The complaint states that the individual defrauded investors in a pair of "ICOs"

[1] In *SEC v. Howley*, the Supreme Court ruled that a security includes an "investment contract," which constitutes an (1) investment of money (2) in a common enterprise (3) with a reasonable expectation of profits (4) to be derived solely from the entrepreneurial or managerial effort of others.

[2] *See* SEC press release, "SEC Issues Investigative Report Concluding DAO Tokens, a Digital Asset, Were Securities" (July 25, 2017).

[3] *See* SEC public statement, "Statement by the Divisions of Corporation Finance and Enforcement on the Report of Investigation on The DAO" (July 25, 2017).

[4] *See* SEC public statement, "Statement on Potentially Unlawful Promotion of Initial Coin Offerings and Other Investments by Celebrities and Others" (Nov. 1, 2017).

purportedly backed by investments in real estate and diamonds by selling tokens, as unregistered securities, that did not really exist for companies that had no real operations. The individual charged had sold the tokens as "the First Ever Cryptocurrency Backed by Real Estate" and made a number of misstatements, including that the company had a "team of lawyers, professionals, brokers, and accountants" that would invest the ICO proceeds into real estate, when in fact it had none. The SEC obtained an emergency court order to freeze the assets of the individual and his companies. In its complaint, the SEC has also sought an officer-and-director bar and a bar from participating in any offering of digital securities.

Investors may also start to rely on the SEC's announcement with respect to The DAO in investor lawsuits. For example, two class action lawsuits have now been filed against the organizers of Tezos, a blockchain network that conducted an ICO in July 2017, in California state court and in a Florida federal district court. The lawsuits allege that Tezos' founders broke federal securities laws and made misrepresentations with respect to the project during the ICO.

US Financial Crimes Enforcement Network

The U.S. Financial Crimes Enforcement Network (FinCEN) is also becoming an important enforcer in this area. In 2015, FinCEN, in coordination with the U.S. Attorney's Office for the Northern District of California, assessed a $700,000 monetary civil penalty against Ripple Labs and its wholly owned subsidiary, XRP II LLC, for willful violations of the Bank Secrecy Act. FinCEN found that Ripple had acted as a money services business and sold its virtual currency, XRP, without registering with FinCEN. In addition, FinCEN found that Ripple had failed to implement and maintain an adequate anti-money laundering program to protect its products from use in money laundering or terrorist financing. Jennifer Shasky Calvery, FinCEN's then-director, stated that "virtual currency exchangers must bring products to market that comply with our anti-money laundering laws. Innovation is laudable but only as long as it does not unreasonably expose our financial system to tech-smart criminals eager to abuse the latest and most complex products."

In July 2017, FinCEN determined that grounds existed to assess a $110 million civil penalty against BTC-e, a bitcoin processor, and a penalty of $12 million against BTC-e's owner/operator, Alexander Vinnik, a Russian national who was arrested in Greece in cooperation with U.S. authorities. In FinCEN's view, BTC-e, a non-U.S. entity, is subject to U.S. jurisdiction because it conducted over 20,000 bitcoin transactions worth more than $296 million in the U.S., with thousands of transactions in other convertible currencies, and, on some occasions, with funds sent customer-to-customer within the United States. FinCEN found that BTC-e and Vinnik willfully violated money service business requirements related to registration and renewal, as well as requirements to implement an effective anti-money-laundering program, detect suspicious transactions and file suspicious activity reports, and obtain and retain records relating to transmittals of $3,000 or more. Jamal El-Hindi, FinCEN's then-acting director, emphasized the agency's focus on cryptocurrency enforcement: "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] laws."[5]

US Department of Justice

The U.S. Department of Justice (DOJ) is also investigating and prosecuting matters related to the use of cryptocurrencies. For example, the DOJ also charged BTC-e and Vinnik, discussed above, in a multiple-count indictment for operating an unlicensed money service business, conspiracy to commit money laundering, money laundering and engaging in unlawful monetary transactions. The DOJ said that it "would continue to devote the necessary resources to ensure that money launderers and cyber-criminals are detected, apprehended, and brought to justice wherever and however they use the internet to commit their crimes."[6] The DOJ has sought to extradite Vinnik, a request that has been granted by a Greek court. However, both Russia and Vinnik have challenged the extradition to the United States. Russia wants Vinnik to face charges there, where he is accused of a $11,500 fraud. Russia has argued that its request for extradition takes precedence because of Vinnik's Russian nationality. Vinnik denied all charges in Greek court during the extradition hearings.

US Internal Revenue Service

Cryptocurrencies are also likely to attract the attention of the U.S. Internal Revenue Service (IRS) in relation to tax evasion offenses, as well as similar regulators in other jurisdictions. The IRS treats cryptocurrencies as property for U.S. federal tax purposes and not as "real" currency — *i.e.*, coin and paper money. As such, cryptocurrencies do not have legal tender status in the U.S., but they are still subject to taxes such as, for example, in situations where cryptocurrency is used to pay wages or reimburse independent contractors, or where the cryptocurrency

[5] *See* DOJ press release, "Russian National and Bitcoin Exchange Charged in 21-Count Indictment for Operating Alleged International Money Laundering Scheme and Allegedly Laundering Funds From Hack of Mt. Gox" (July 26, 2017).

[6] *Id.*

is a capital asset that experiences gains or losses. Likewise, payments made using cryptocurrencies are subject to information reporting to the same extent as any other payment made in property in the United States.

As a result, the IRS has already attempted to identify taxpayers who have participated in transactions it suspects as being used for tax avoidance through Coinbase. Litigation over the IRS' efforts to enforce a summons for Coinbase customer names is pending in California, but it may signal a broader desire by the IRS to pursue tax evasion offenses related to cryptocurrencies.

International Regulators

Regulatory and criminal enforcement of cryptocurrencies is starting to develop outside the United States. In early September 2017, Chinese regulators announced that token sales are "an unauthorized and illegal public financing activity, which involves financial crimes such as the illegal distribution of financial tokens, the illegal issuance of securities and illegal fundraising, financial fraud and pyramid scheme." They warned that token sales present numerous risks and cautioned the public to be vigilant.

China also directed any entity or individual who had already completed a token sale to make appropriate arrangements to protect its investors' rights, including refunding crypto assets. Chinese regulators defined token sales very broadly as "a process where fundraisers distribute digital tokens to investors who make financial contributions in the form of cryptocurrencies such as bitcoin or ether." At least in the short term, this announcement has effectively shut down the ICO market in China, the largest in the world. The announcement also extended to token exchanges operating in China, stating that no exchange can: (1) offer exchange services between fiat currency and tokens or between cryptocurrencies and tokens; or (2) act as a central party facilitating the trading of tokens for cryptocurrencies. Violators will have their websites and mobile applications shut down and delisted from application stores. The exchanges also risk having their business licenses voided. Financial institutions and nonbanking payment institutions are now also prohibited from operating any businesses that deal with token sales, including by providing account opening, registration, trading, clearing and settlement services, or insurance for tokens or cryptocurrencies. It remains to be seen whether China will provide a regulatory framework under which certain ICOs could proceed.

On September 29, 2017, South Korea became the latest country after China to announce a potential ban of ICOs. South Korea's Financial Services Commission stated that cryptocurrency trading needed to be tightly controlled and that ICOs needed to be banned, with stiff penalties imposed for violators.

Most recently, Taiwan's Financial Supervisory Commission chairman stated that Taiwan would not seek to follow China and South Korea in banning ICOs but that it should aim to model Japan by enacting regulations to control cryptocurrency outflows without hampering technological development opportunities.

Japan, an early adopter of bitcoin, has not yet spoken on ICO regulation but has enacted legislation to protect cryptocurrency users from the collapse of trading platforms that are used to invest in ICOs, such as by putting in place capital requirements. Japan has also required cryptocurrency exchanges to comply with the country's anti-money laundering regulations.

Taking an approach more similar to the SEC, Hong Kong regulators stated that "depending on the facts and circumstances of an ICO, digital tokens that are offered or sold may be 'securities' as defined in the Securities and Futures Ordinance, and accordingly subject to the securities laws of Hong Kong." Similarly, Canada has issued a notice stating that it had found, in many instances, that coins/tokens had constituted securities for the purposes of securities laws, including because they involved investment contracts. More generally, the European Union has also focused on strengthening its anti-money laundering regulations, which increase due diligence requirements on cryptocurrency exchanges. The European Securities and Markets Authority has also publicly stated that it is observing ICOs and expects action to be taken on a case-by-case basis. Switzerland's Financial Market Supervisory Authority (FINMA), specifically, announced in late September 2017 that it was reviewing a number of ICOs for potential breaches of provisions related to anti-money laundering and terrorist financing. FINMA stated that because ICOs and token-generating events had a close resemblance to "conventional financial-market transactions," they may be covered under existing financial regulations.

In an effort to protect investors, the U.K.'s Financial Conduct Authority (FCA) recently issued a warning on the risks of investing in ICOs and is working on additional guidance on the issue. Likewise, the Australian Securities and Investments Commission issued new guidance for ICO issuers, warning consumers that they must understand potential risks and be wary of scams.

International Cooperation in Enforcement

We believe international cooperation among law enforcement authorities is likely to become commonplace in this area given the global nature of ICOs and cryptocurrencies. However, enforcement authorities may encounter challenges in obtaining and using information related to users and their investments in ICOs and cryptocurrencies across international borders. In its Investor Bulletin on ICOs, discussed above, the SEC warned investors that

investing in ICOs may limit their recovery in the event of fraud or theft because of limits to the SEC's ability to obtain information internationally. The Bulletin explains that third-party wallet services, payment processors and virtual currency exchanges may be located overseas, and there is no central authority that collects virtual currency user information. This means that the SEC must rely on other sources for this type of information and may be unable to obtain such information from persons or entities located overseas. The Bulletin states, "Although the SEC regularly obtains information from abroad (such as through cross-border agreements), there may be restrictions on how the SEC can use the information and it may take more time to get the information. In some cases, the SEC may be unable to obtain information from persons or entities located overseas."[7]

Regulations Seeking to Promote Distributed Ledger Technologies

In the U.S., state regulators have started to focus on ways to encourage and facilitate the use of distributed ledger technologies such as blockchain. For example, New York has designed and implemented "BitLicenses," which grant businesses the ability to operate in the state, provide a framework for cryptocurrency exchanges and encourage the long-term growth of new technologies and industries. Most recently, New York granted a BitLicense to the large cryptocurrency exchange Coinbase after a comprehensive review of Coinbase's anti-money laundering, capitalization, and consumer protection and cybersecurity policies. However, the licensing process appears to be somewhat burdensome — a number of applications have been denied, and the price of obtaining a license has been criticized by some as disadvantaging small businesses. As a result, some companies have decided to abandon the New York market instead of seeking a license to operate there.

The U.S. Commodity Futures Trading Commission (CFTC) has also taken steps to support access to cryptocurrencies. In July 2017, it approved the creation of the first swap execution facility (SEFs), which gives institutional investors access to the bitcoin market for swap trading. The CFTC issued a registration order to LedgerX LLC, an institutional trading and clearing platform, which grants it status with the CFTC as a SEF and effectively approves bitcoin options trading for institutional traders such as hedge funds.

International regulators are also showing a willingness to allow new technologies and related businesses to innovate and come to market in their jurisdictions. In the U.K., for example, the FCA has created a "regulatory sandbox," a space open to both authorized and unauthorized firms that allows new businesses to test their technologies and services while receiving guidance and clarity about the regulatory landscape that may impact their services. Businesses selected for this project include a cross-border money transfer service powered by digital currencies and blockchain technology; an e-money platform based on distributed ledger that facilitates the secure transfer and holding of funds using a phone-based app; and a smart-card-enabled retail payment system based on a distributed ledger.

* * *

As the use of cryptocurrencies and services based on distributed ledger technologies becomes more mainstream, we are likely to see new risks in the regulatory and enforcement environment, including divergent regulations and policies among international regulators and increased enforcement. Companies and individuals operating in the cryptocurrency and ICO spaces would do well to pay careful attention to regulatory and enforcement developments worldwide.

Portions of this article were published in International Comparative Legal Guide to Business Crime 2018.

Click here to read the November 2017 issue of *Cross-Border Investigations Update*

[7] *See* SEC Investor Bulletin: Initial Coin Offerings (July 25, 2017).