Navigating Cryptocurrency Regulation: Common Sense in an Uncommon Industry

Gayle E. Littleton, David Bitkower, and Justin C. Steffen January 15th

The recent, exponential growth of bitcoin, Ether, and other cryptocurrencies has brought cryptocurrencies firmly into the public eye. Some have created crypto-products or tokens to raise funds in a veritable cash grab with little foresight, planning, or disclosure. Others – by the tens and hundreds of thousands – are signing up to purchase crypto-assets. Often these purchasers have no understanding of the underlying technology or the risks involved, proving that, as Mark Twain opined, "common sense is very uncommon."

While the growth of cryptocurrencies can give the appearance of a Wild West for the digital age, individuals and companies active in the area should not be fooled. US Government regulators have been keeping an eye on virtual currencies for several years, and have already moved to fill any lawless void. The Securities and Exchange Commission (SEC), Commodity Futures Trading Commission (CFTC), and Internal Revenue Service (IRS), among other US Government agencies, have issued guidance on the application of laws and regulations to virtual currencies. Numerous agencies have taken enforcement actions to protect consumers. And Congress has been closely watching any connections between virtual currencies and crime or terrorism for several years. As regulators' interest intensifies, newcomers as well as established industry participants will inevitably be subject to increased scrutiny. Businesses, however, can stay on the right side of regulators and help themselves by adhering to some simple, straightforward practices.

Here Come the Regulators

Beginning in the late 1980s, advocates of encryption and privacy in cyberspace joined to create the CypherPunk movement. Almost two decades later in 2008, building on the principles of the CypherPunks, a person or persons using the pseudonym Satoshi Nakamoto penned a white paper describing the digital currency bitcoin and the distributed ledger designed to record transactions in bitcoin, blockchain.

Cryptocurrencies and related technologies gradually gained attention, culminating in the boom of 2017. The price of bitcoin increased approximately 1500% that year alone. Ether, another popular cryptocurrency, saw its price rise in 2017 from $8 to almost $800 a coin. Mirroring this growth, companies are opening new exchanges and launching bitcoin- and crypto-related products.

Similarly, a number of entrepreneurs have bypassed venture capital and other traditional fundraising measures by creating their own "coins" and conducting initial coin offerings (ICOs). Some new projects underlying crypto tokens have garnered tens of millions of dollars in days or even hours. There were over 200 ICOs just in 2017, the largest of which raised in excess of $200 million.

Like the public, regulators have taken note of the crypto boom. For example, the SEC's July 25, 2017 "DAO Report" – which declared that coins or tokens can constitute securities, the unregistered sale or re-sale of which can result in both civil and criminal liability – served as a shot across the bow for some in the cryptocurrency industry. The SEC followed up that warning with action. It created an ICO task force, charged the promoter of two ICOs (DRC and ReCoin) with fraud, halted another ICO (Plexcorps), and warned celebrities about endorsing ICOs. SEC Chairman Jay Clayton cautioned that he had not yet seen an ICO that "doesn't have a sufficient number of hallmarks of a security."

Not to be outdone, the IRS filed suit against Coinbase, a leading digital currency exchange, winning access to 14,000 of Coinbase's user accounts. The Financial Crimes Enforcement Network (FinCEN) fined bitcoin exchange BTC-e over $100 million for failing to comply with money transmitter regulations. The CFTC is investigating a recent Ether crash on the Coinbase Exchange. And the Justice Department has brought criminal charges against a host of individuals for crimes such as fraud and money laundering committed in connection with cryptocurrencies. These recent developments likely represent the beginning of increased regulatory activity, not the end.

What can I do?

In this fast-moving environment, there are several things that companies already involved or considering entry into the cryptocurrency space should consider to prepare for increased regulatory scrutiny and avoid finding themselves in the crosshairs of civil or criminal government inquiries.

1. Understand New Cryptocurrency Regulations and Interpretive Guidance When They Are Announced.

It is important to identify and understand new industry regulations and interpretive guidance as soon as they are released. Given that the crypto-currency industry has developed so quickly, not all in the industry are conditioned to track regulatory changes. But ignoring them now is fraught with peril.

Once regulations are implemented, or interpretive guidance has been issued, the government expects companies to comply. And in many contexts, as a well-known legal principle holds, "ignorance of the law is no defense." If a regulatory violation is committed, the company (and possibly individual employees) may be liable, regardless whether they knew their actions violated the law.

To avoid this risk, it is important to stay abreast of changes to industry regulations in real time. Although doing so may seem difficult, it has in fact never been easier. Like the DAO Report, regulators publically announce industry developments, and these agencies allow the public to receive email updates of those public announcements when they occur. See, e.g., SEC, CFTC, DOJ and IRS . Moreover, numerous industry publications, legal blogs, and podcasts provide regulatory updates, and the speakers and materials provided at industry conferences often cover this topic. CoinDesk, Cointelegraph, and Bitcoin Magazine, for example, all provide extensive coverage of the crypto space.

2. Implement and Update Policies to Comply with New Regulations.

If the company does not already have an existing compliance program, it should consider implementing one immediately. Likewise, although company sizes and structures vary significantly, companies invariably benefit from having someone in the leadership team with responsibility for legal and compliance issues. A strong compliance program will include a policy that makes clear the company expects its employees to comply with the law, sets out the processes and controls in place to ensure compliance, and provides a means through which employees can report possible violations. But a policy will only be successful if employees understand it and embrace the values that prompted its issuance in the first place. As a result, leadership communication and employee training are just as important as the program itself. Whenever a new regulation is implemented, interpretive guidance is issued, or an enforcement action against someone else in the industry is announced, a company should take the time to reconsider its current policies and practices to determine whether the new rules or actions expose any potential weaknesses. If a company identifies any weaknesses, it should act quickly to prevent or mitigate any violation, and employees should be informed of those changes where appropriate.

3. If the Company Receives an Inquiry from the Government, Take Steps to Ensure an Appropriate Response.

If the government comes knocking, the corporate response will be critically important. If handled well, the response can defuse government concerns and lead to quick resolution. But if the response is bungled or not handled with sufficient seriousness, the government's investigation may only grow in scope, time, and cost. Below are just a few steps that companies in other sectors already take when they receive a government inquiry; the same considerations apply – in some cases even more strongly – to companies that deal with virtual currencies:

- Make sure relevant data is preserved. The government is quick to view document destruction as suspicious, even in the ordinary course of business, and destroying records after learning of a government investigation could result in criminal indictment. Upon learning of an investigation, consider implementing an immediate litigation hold, which ensures that all relevant materials are preserved.

- Retain and communicate with the government through the company's outside counsel. Statements made by employees directly to the government will be deemed admissions that may be used against the company and/or the employee making the statement. By contrast, experienced counsel can take the government's temperature – inquiring into the scope of the inquiry and the posture in which the company is viewed – with far less risk.

- Understand the value of cooperation with the government. Although it may not seem natural for a start-up that has successfully embraced a disruptive technology to show its cards to government enforcers, emerging industries quickly learn what their well-established counterparts already know: the government wields immense power in an investigation of alleged corporate wrongdoing. Even where the potential misconduct occurred at a comparatively low-level, or where it was inadvertent, the government typically expects legitimate companies to conduct their own thorough internal investigation, share the results with the government, and then negotiate for a resolution that grants the company credit for cooperating with the inquiry. Experience has shown that companies that take this approach from the beginning tend to come out of any scrutiny more quickly and cheaply than companies that take a more adversarial approach or stall in response to inquiries. Moreover, the company's interactions with the government today will have an impact on how the company is perceived by the government later. Cooperation shows the government that the company wants to ensure compliance, and if another issue arises down the road, the government will more likely approach the company from the premise that there was no wrongdoing, or that any wrongdoing is not systemic – both of which are helpful.

Cryptocurrencies continue to show promising applications, but their rapid rise and abuse by some wrongdoers guarantees that government regulators will keep a close eye on whether companies are following the law, and that Congress will continue to consider whether new laws ought to be passed. When the dust settles, the most successful companies will be those that not only have the best product or service, but also started planning for success from the beginning by establishing a sound compliance program and responding to the government just as intelligently as they respond to the market. The suggestions set forth above are one starting point. More broadly, common sense can help businesses survive and thrive in the new age of digital assets. ▫

Ms. Littleton and Mr. Bitkower are former federal prosecutors and partners with Jenner & Block LLP in the firm's Chicago and Washington, D.C. offices. Justin C. Steffen is a Partner in Jenner & Block's Chicago Office where he concentrates on commercial litigation and FinTech. Mr. Steffen is particularly focused on the intersection of cryptocurrency, blockchain and the law.