

Federal enforcement trends in the cryptocurrency sphere

Technology, Privacy, and eCommerce



Although virtual currencies proliferate across the market, there remains much confusion about what exactly constitutes a cryptocurrency, how its value is determined, and how cryptocurrencies can be used. Facebook's recent announcement that it intends to launch its own cryptocurrency, Libra, has put the topic of cryptocurrencies front and center and has drawn heightened attention to the need for regulation in this space. Increasing enforcement actions demonstrate that policing cryptocurrencies is becoming a priority for a number of federal agencies, from the Department of Justice (DOJ) to the Securities and Exchange Commission (SEC).



These enforcement actions have provided some much-needed guidance as institutions and individuals seek to determine appropriate compliance with the various regulatory regimes in place. Keeping a finger on the pulse of enforcement trends is vital for those who would like to use cryptocurrencies or to do business with others who use cryptocurrencies – particularly because enforcement is on the upswing.

Overview of cryptocurrencies

Although cryptocurrencies is the common term by which virtual currencies are known, cryptocurrencies are but one type of virtual currency. Virtual currency generally refers to currency available in electronic form that is stored through designated software and is transferred through the internet or over secure dedicated networks. Unlike traditional currencies, virtual currencies are not issued by banking regulatory authorities.

While cryptocurrencies are a type of virtual currency, they differ from other virtual currencies because they are characterized by the use of cryptography technology that keeps transactions secure in the absence of financial intermediaries, such as a bank. Given the lack of a centralized regulatory authority, cryptocurrencies can (and often do) wildly fluctuate in valuation. Bitcoin, one of the largest and most widely used cryptocurrencies, is often used in peer- to-peer electronic payments and has

been the focus of a number of enforcement actions.

United States' regulatory guidance and enforcement overview

The cryptocurrency sphere has been evolving quickly and a comprehensive federal regulatory framework governing cryptocurrencies has not yet been developed. Regulators in the United States, however, have been working to implement guidance regarding cryptocurrencies and have pursued enforcement actions to hold culpable actors liable for cryptocurrency-related misconduct. In late July 2019, Treasury Secretary Steven Mnuchin indicated that federal regulators were committed to creating a unified approach and predicted that more regulations would be forthcoming.

To date, the DOJ, the Commodity Futures Trading Commission (CFTC), the Internal Revenue Service (IRS), the Financial Crimes Enforcement Network (FinCEN), the Office of Foreign Assets Control (OFAC), and the SEC have all issued guidance and/or brought enforcement actions in the cryptocurrency sphere. Federal enforcement efforts have generally fallen within the following categories: (i) fraud-related allegations; (ii) registration requirement allegations; (iii) Bank Secrecy Act/Anti-Money Laundering allegations; and (iv) trading allegations. While beyond the scope of this article, it is worth noting that civil litigation is also on the rise, with actions that commonly involve allegations of fraud or misappropriation, violations of securities laws and regulations, negligence, and breach of contract. Additionally, state regulators, such as the New York State Department of Financial Services, are also active in the cryptocurrency sphere and have, among other things, implemented robust requirements that cryptocurrency exchanges must satisfy in order to conduct business in the state.

> "While beyond the scope of this article, it is worth noting that civil litigation is also on the rise, with actions that commonly involve allegations of fraud or misappropriation, violations of securities laws and regulations, negligence, and breach of contract."

FinCEN's regulatory guidance and enforcement actions

While the enforcement efforts of various agencies have ramped up since 2017, FinCEN issued interpretative guidance and asserted its jurisdiction over virtual currency as early as 2013. According to FinCEN, users who obtain cryptocurrency in order to purchase goods and/or services are not generally considered money transmitters subject to FinCEN's authority. Issuers/redeemers of cryptocurrency and exchangers of cryptocurrency, on the other hand, do fall within the ambit of FinCEN's regulatory authority. They are considered money transmitters and thus subject to, among other things, FinCEN's Bank Secrecy Act (BSA) requirements.

In April of 2019, FinCEN announced its first enforcement action against a peer-to-peer virtual currency exchanger, which was the first instance in which it had penalized an exchanger of virtual currency for failure to file Currency Transaction Reports (CTRs). In that case, the exchanger, Eric Powers, had conducted approximately 160 purchases of Bitcoin for an aggregate $5 million through in-person cash transactions, yet never filed a CTR. He also processed numerous suspicious transactions, including doing business related to the Silk Road dark web marketplace, without ever filing a Suspicious Activity Report. FinCEN's action against Powers highlights the risk to individuals and institutions transmitting virtual currency without attention to FinCEN's BSA requirements.

The SEC's enforcement actions

The SEC has focused its efforts on pursuing entities for issues with their initial coin offerings (ICOs) as well as pursuing individuals and entities for fraudulent behavior in connection with soliciting investors for digital currency schemes. ICOs involve the sale of digital tokens as a way to raise capital. There are different kinds of tokens – some represent a right to a not-yet-released product or application (utility tokens),while others represent equity and are often intended to be converted into a cryptocurrency at a later stage (equity tokens). In 2018, ICOs raised upwards of $7 billion, and in the first half of 2019, upwards of $1.5 billion was raised through a relatively new phenomenon known as cryptocurrency initial exchange offerings (IEOs).

The SEC has concluded that digital tokens can, depending on the facts, be considered securities subject to SEC regulation. Recently, in June of 2019, the SEC filed suit against KIK Interactive Inc. (KIK) for conducting an illegal $100 million securities offering of digital tokens without registering its offer and sale as required by the US securities laws. The SEC also alleged that the company marketed the tokens as an investment opportunity even though it was aware that its representations were not accurate. This was not the first action of its kind, as the SEC has brought and settled other, similar actions against companies. But KIK has publicly vowed to fight the SEC in its case and to challenge the SEC's application of the securities laws in this setting.

> "The Centra case marks another example of federal regulators seeking to stem the rise of unscrupulous actors in the cryptocurrency market and highlighting the danger of believing unverified representations made by those peddling digital currencies."

In another enforcement action, filed in November of 2018, the SEC ordered Zachary Coburn, the founder of the EtherDelta cryptocurrency exchange, to cease and desist from operating the trading platform. This case marked the first time that the SEC has pursued a cryptocurrency exchange for operating as an unregistered national securities exchange. The SEC concluded that the tokens traded on EtherDelta included securities, and found that because EtherDelta was not registered as an exchange, EtherDelta had violated US securities laws. Coburn settled the case and agreed to pay $300,000 in disgorgement, plus $13,000 in prejudgment interest and a $75,000 penalty. As the Coburn case makes clear, trading platforms must engage in adequate legal due diligence to assess the risk that individual tokens may be deemed securities by the SEC.

The DOJ's enforcement actions

The DOJ's enforcement efforts have been varied and have focused on a wide range of issues connected to the use of digital currencies. The DOJ has pursued entities and individuals for acting as exchangers of virtual currencies without operating with the requisite licensing for a money services business, engaging in money laundering (oftentimes on the dark net), and engaging in fraudulent conduct, such as by duping investors.

In August of 2018, the DOJ brought charges against Jacob Burrell, a 21-year-old Bitcoin dealer. The DOJ alleged that Burrell, who conducted 971 separate transactions with over 900 individual customers, accepted cash with no questions asked, and thus solicited and introduced into the US banking system close to $1 million in unregulated cash. Shortly after being charged, Burrell pleaded guilty to operating a Bitcoin exchange without registering with FinCEN and without implementing the required anti-money laundering safeguards. He admitted that he had no anti-money laundering or know-your-customer program, and performed no due diligence on the source of his customers' money. In April of 2019, Burrell was sentenced to two years' imprisonment and required to forfeit

$823,357. The DOJ's case against Burrell, like the recent FinCEN action against Eric Powers, is a reminder that federal anti-money laundering laws apply equally to cryptocurrency transactions.

In February of 2019, the DOJ brought charges against Randall Crater, the founder and principal operator of My Big Coin Pay Inc. (My Big Coin Pay), for his alleged participation in a scheme to defraud investors by marketing and selling fraudulent cryptocurrency. The DOJ, along with the CFTC, which brought its own action against Crater, contends that from 2014 to 2017, Crater and his affiliates lied to investors that a virtual currency called My Big Coin was backed by gold and could be traded on exchanges. This scheme allegedly resulted in Crater receiving approximately $6 million of investor money, which regulators contend he misappropriated for his own use. Notably, in the CFTC action, Crater and the other defendants attempted to argue that the CFTC lacked the ability to regulate My Big Coin Pay because it, unlike Bitcoin, did not involve futures contracts. The court determined, however, that cryptocurrencies meet the definition of a commodity and are within the purview of the CFTC's authority.

In another recent action, the DOJ pursued the co-founders of a startup company called Centra Tech, Inc. (Centra). The DOJ alleged that, in connection with soliciting investors to purchase unregistered securities in the form of digital tokens issued through an ICO, the co-founders of Centra made a series of false representations, including fabricating partnerships with legitimate companies and falsely claiming that the company had money transmitter licenses in a number of states. The SEC brought a parallel action against the co-founders, alleging that they violated the anti-fraud and registration provisions of the US securities laws. In July of 2019, the former chief operating officer of Centra pleaded guilty to a series of securities and wire fraud charges in connection with the same scheme. The Centra case marks another example of federal regulators seeking to stem the rise of unscrupulous actors in the cryptocurrency market and highlighting the danger of believing unverified representations made by those peddling digital currencies.

Guidance from other federal regulators

The CFTC: The CFTC has taken the position that cryptocurrencies are commodities, i.e., closer to gold than to traditional currencies or securities. Federal courts, as in the My Big Coin Pay case, have agreed with the CFTC's position on this issue. The CFTC, accordingly, has asserted its authority to regulate cryptocurrency-related fraud activity, and has also successfully pursued regulatory action against cryptocurrency trading platforms.

OFAC: In 2018, OFAC released guidance, issued in the form of Frequently Asked Questions (FAQs), explaining that transactions involving cryptocurrencies would be treated the same as other transactions for sanctions purposes. In the FAQs, OFAC made clear that compliance obligations would be the same, and that companies would be expected to develop tailored risk-based compliance programs that address the risks posed by digital currencies. There is thus an expectation that OFAC will bring enforcement actions against those who transact in cryptocurrencies in violation of US sanctions.

The IRS: In 2014, the IRS issued a notice stating that cryptocurrency is treated as property for federal tax purposes. As a result, disposing of cryptocurrency can give rise to a taxable gain. In 2017, the IRS successfully obtained a court order requiring Coinbase, a cryptocurrency exchange, to turn over customer data relating to customers who may not have paid federal taxes on their virtual currency profits. As a likely result of this court order, the IRS announced in late July 2019 that it has identified more than 10,000 individuals who may have failed to report income and pay the resulting tax from virtual currency transactions. The IRS has started to send out warning letters to these

individuals that indicate that the IRS is beginning to form views on whether individuals' noncompliance is potentially culpable behavior. The IRS is also reported to be building criminal tax evasion cases involving cryptocurrency, including through an international tax enforcement collaboration known as the Joint Chiefs of Global Tax Enforcement, or J5.

Conclusion

As digital currencies increase in popularity and use by businesses and individuals alike, it is likely that the upward trend in federal enforcement actions will continue. The recent proclamation by Treasury Secretary Mnuchin that regulators are seeking to increase regulation further underscores the importance of actively monitoring cryptocurrency regulatory developments. It is equally important for companies to monitor the enforcement landscape periodically because it is in a constant state of evolution, with new guidance being created nearly every day.

Sarah Paul



Partner

Eversheds Sutherland

Sarah Paul, partner in the New York office, advises clients across all areas of white-collar defense, with a particular focus on government, internal, and cross-border investigations, tax controversy, and cybersecurity and privacy law. As a former Assistant United States Attorney for the Southern District of New York in the Criminal Division, a position she held for nearly a decade, she has extensive

experience litigating complex criminal and civil cases, including wire fraud, bank fraud, cybercrime, international money laundering, securities fraud, Foreign Corrupt Practices Act violations, healthcare fraud, and Bank Secrecy Act violations.

Sarah Chaudhry



Associate

Eversheds Sutherland

Sarah Chaudhry, associate in the New York office, counsels on a variety of commercial litigation matters with an emphasis on financial services, internal and governmental investigations, and securities litigation. Her practice contains cross-border components and includes class actions.