

Initial Coin Offerings: A New Frontier for the SEC and Whistleblowers

By [Michael A. Filoromo, III](#)
January 16, 2018

In July 2017, the U.S. Securities and Exchange Commission (“SEC”) [issued](#) an investigative report concluding that virtual tokens and coins may be securities subject to federal securities laws. The SEC’s conclusion may have wide-ranging implications for a burgeoning area of investment in innovative financial markets and the tech industry.

Virtual organizations, including many tech startups, increasingly raise significant capital through so-called initial coin offerings (“ICOs”), selling electronic tokens or coins that entitle the buyer to participate in the project, such as by accessing or using the technology a company is developing. The tokens or coins are not equity, but often come with the promise that the investor will share in the financial returns of the project. Investors may also trade these tokens or coins on secondary markets, such as virtual currency exchanges.

What Are Virtual Currencies and Blockchain Technology?

Some background in the technology is helpful to understanding the SEC’s ruling. Many people find virtual currencies, like Bitcoin, mysterious. Their decentralized nature – they do not issue from any country’s government or central bank – and the fact that they exist only in electronic form make these so-called cryptocurrencies different from the money with which most of us are familiar. Yet cryptocurrencies, including the coins or tokens sold in ICOs, have real value.

Virtual currencies and ICOs are secured and supported by blockchain technology, also known as distributed ledgers. Blockchains are an electronic way of recording transactions between individuals. Each block in a chain contains data, including timestamps, about a batch of transactions between individuals. Each block also points to a previous block in the chain of transactions. The promise of blockchain technology is that the linked, iterative nature of a chain divided into blocks makes it more secure. It is impossible to change a given block in the growing list of records without changing all previous blocks. The blocks, in turn, are stored – or distributed – across multiple computers so that altering blocks requires coordinating those computers. This is a taller task for a cyberattacker than merely taking control of a single machine.

The Rapid Rise - and Risks - of ICOs Attract the SEC’s Attention

In 2017, ICOs raised an estimated \$5 billion. Unlike traditional initial public offerings (“IPOs”) that companies use to raise capital, ICO crowdfunding projects have often escaped regulatory scrutiny. An organization making an ICO need not disclose its finances or the viability of its product. Effectively, it need not even demonstrate its existence. As a result, some unscrupulous individuals and organizations have used ICOs as a vehicle to swindle investors.

As ICOs and virtual currencies have become increasingly mainstream, regulators have begun to take note. In July 2017, on the same day it issued the investigative report concluding that ICOs may be sales of securities, the SEC also issued an [investor bulletin](#) to advise consumers of the risks

associated with ICOs. The SEC summarized the impetus for the bulletin: “[ICOs] may provide fair and lawful investment opportunities. However, new technologies and financial products, such as those associated with ICOs, can be used improperly to entice investors with the promise of high returns in a new investment space.” Two months later, in September 2017, the SEC [announced](#) the creation of a Cyber Unit. In addition to focusing on cyber threats and hacking into financial systems, the Cyber Unit’s mandate includes targeting violations involving blockchain technology and ICOs.

The SEC demonstrated its commitment to regulating ICOs very shortly thereafter. On October 1, 2017, the SEC filed fraud charges against Maksim Zaslavskiy, the creator of two ICOs, REcoin and DRC, and obtained an emergency freeze of his assets. REcoin was billed as a virtual currency backed by real estate, while DRC was supposedly based on investments in diamonds. The SEC alleged that REcoin and DRC not only misrepresented the total level of investments they had received and made, but worse, that the tokens were not being transacted on blockchains at all. Thus, the scam was not even a true ICO.

Two months later, on December 1, 2017, the SEC’s Cyber Unit filed its first criminal complaint in federal court and obtained an emergency asset freeze to [stop a \\$15 million ICO scam](#). The SEC charged that Dominic Lacroix, his company PlexCorps, and his partner, Sabrina Paradis-Royer, marketed PlexCoin as an investment that would yield 1,354 percent profit in 29 days. Between August and December 2017, thousands of investors bought millions of dollars’ worth of PlexCoin based on these representations, which the SEC alleges were baseless.

Whistleblowers May Play a Role in Policing ICOs

The ethereal nature of ICOs means that the SEC and other regulators may have to rely on individuals with firsthand knowledge of potentially fraudulent schemes to provide the information necessary to stop them. The [SEC’s whistleblower program](#) incentivizes individuals with knowledge of securities violations to come forward by offering an award equal to 10 to 30 percent of the monetary sanctions the SEC collects if the total exceeds \$1 million. Through December 2017, the SEC had paid more than \$179 million to 50 whistleblowers. This program should be available to individuals who provide information about ICOs as well.

Often, SEC tips that lead to successful enforcement actions come from insiders – employees or officers of a company with insight into its inner workings. But insider knowledge is not a requirement to receive an award. In its [2017 annual report](#) to Congress on the whistleblower program, the SEC noted that nearly 40 percent of whistleblower award recipients were company outsiders, including industry professionals and others who provided relevant information or independent analyses. Notably, 19 percent of whistleblower award recipients were harmed or prospective investors.

In the case of ICOs, investors and those in the rapidly evolving industry may be best poised to identify fraud that would otherwise go undetected. These individuals can provide invaluable information to the SEC that will allow the agency to act quickly to preserve assets and protect investors. In return, these whistleblowers stand to gain significant awards.