I am lawyer who represents whistleblowers. I also am fascinated by the worlds of cryptocurrency and blockchain technology. Increasingly, these two worlds intersect, if not collide. As anyone steeped in the fintech arena knows, blockchain has the potential to revolutionize banking and financial transactions. Unfortunately, cryptomania has resulted in numerous Ponzi-like scams, and other dubious activities such a market manipulation, money laundering, and tax evasion.
Even legitimate cryptocurrencies, like Bitcoin (BTC) and Ethereum (ETH), are frequently used for unlawful ends. Governments around the world, including India and China, have already started to heavily regulate, or even outlaw, the use of cryptocurrency. In the United States, various government agencies have investigated and brought legal actions against many crypto and blockchain projects and their teams.

As has happened in other industries, whistleblowers are the ones most likely to lead the way in cleaning up crypto. The crucial whistleblowers are people inside the business, who understand the technologies that drive it, and who, proverbially speaking, know where the bodies are buried. They are the ones best positioned to explain what is happening in this highly technical sector, and to expose the wrongdoings possibly being undertaken by people who are practicing nefarious activities within the cryptosphere.

Now for the good news. Not only can blowing the whistle be the ethically right thing to do, but also you can earn very substantial monetary rewards. Over the last 35 years, the laws of the United States have undergone what I call the “whistleblower revolution.” Both Congress (spearheaded primarily by Senator Chuck Grassley, a staunch advocate for whistleblowers) and the Executive Branch have come to recognize the incredibly valuable role that whistleblowers can play in stopping fraud and other illegal activity. And in recognition of that value, they have passed a series of laws that both protect whistleblowers, but also incentivize whistleblowing by offering monetary rewards.

This whistleblower revolution began in 1986, when the False Claims Act—which covers fraud on government programs or by government contractors—was amended to provide a series of new incentives for whistleblowing. But in the years since, these types of whistleblower reward laws have been passed covering a variety of additional areas, including securities fraud, commodities futures fraud, banking fraud, tax fraud and, most recently, money laundering. These are all areas where crypto-related wrongdoing is occurring in the here and now.

These whistleblower reward programs have paid out billions of dollars, and routinely pay multi-million-dollar rewards to individual whistleblowers. This is because, in all of the programs, the amount of the rewards is calculated as a percentage of the money recovered by the government. Whistleblowers who expose big frauds earn big rewards, and the bigger the fraud the bigger the potential reward.

Now let me turn to the details. I will start by explaining what I call the “Big Five” key concepts that apply across all the whistleblower reward programs. These are important concepts to consider in deciding whether you have information that would fall within the whistleblower reward programs, and whether pursuing a reward makes sense.

Then, I will list the four whistleblower reward programs that are most likely implicated by crypto-related wrongdoing, and for each I will give an example of how crypto-related shenanigans that we already know about would have fallen within that particular program if it had been reported by a whistleblower.

**The “Big Five” Key Concepts the Apply to All of The**
Whistleblower Reward Programs

Key Concept #1: Follow the Process

There are many ways to blow the whistle on illegal conduct. You can call the police or the FBI. You can send a letter to a Member of Congress. You can write about it on a blog or give an interview on TV. None of those ways, however, will lead to you earning a reward.

Under all the whistleblower reward programs, the only way to preserve your right to a reward is to follow an extremely specific process for reporting the illegal conduct to the relevant government agency. In all cases, the report must be in writing, and it must follow the rules of that program. Some of those rules are about the substance of the report (what information must be included), and some of the rules are about process (the format of the report, and where and how it is submitted). In some, but not all, cases the report may be anonymous, although anonymous reporting must generally be done through an attorney so that the agency has someone to communicate with about the matter. But the key concept here is that, before you start blowing on that whistle, make sure you fully understand the processes of the particular whistleblower reward program. Failing to follow the correct process, both substantive and procedural, may cause you to forfeit your right to a reward.

Key Concept #2: Provide Original, Non-Public, Information

The reason why government agencies are willing to pay out big rewards to whistleblowers is to get information that the agencies would not otherwise know. So, all the whistleblower reward programs have some version of a requirement that the information provided by the whistleblower be “original” and not already “public.” How these requirements apply in practice is one of the murkiest and most complicated parts of this area of law because it is not always clear when information becomes “public” or when a whistleblower is the “original” source of information. But in simplest terms, you cannot learn about a fraud by reading about it in a newspaper, and then seek a reward for giving that already-public information to the government. Most successful whistleblowers come to the government with insider knowledge about something that is new to the government agency.

Key Concept #3: Do not Wait

Once you decide that you are ready to blow the whistle, do not delay. The reasons for this are many. Government enforcers are more interested in, and more likely to pursue, wrongdoing that is ongoing or very recent. They are instinctively less interested in stuff that happened years in the past. In addition, the rules of certain of the reward programs allow the agency to take the whistleblower’s speed in reporting the wrongdoing into account in deciding how much to reward; the agencies look less favorably on a whistleblower who sat on the information for a long time while more harm was done.

Finally, see Key Concept #2 above: the longer you wait, the more likely it is that someone else will disclose the same fraud to the government or make it public in
some way, after which it may simply be too late to claim a reward.

**Key Concept #4: Consider Your Own Level of Culpability**

This should seem obvious, but you cannot commit a big fraud, turn yourself into the government, and then expect the government to reward you for “blowing the whistle” on yourself. All the whistleblower reward programs have rules that preclude the government from giving a reward to someone who masterminds an illegal scheme.

Where things can get murkier is when a whistleblower did not plan or run the scheme but did play some more minor role in it—the “foot soldier” in the criminal enterprise, or the “cog” in the corporate machine. Sometimes, those more minor players are the best whistleblowers, because they have the most intimate knowledge of the illegal conduct. And so, minor players generally are not prohibited from receiving a reward. But this is a line-drawing exercise that will depend heavily on the particular facts of the case.

If you personally participated in the wrongdoing that you now seek to expose, you should get legal advice about how to proceed, both because you want to do your best to preserve your right to a reward, but also because, depending on your level of personal culpability, you may also have exposure to becoming a target of the very investigation you birth.

**Key Concept #5: Rewards Are Based on Recoveries**

In all the whistleblower reward programs, the amount of the reward is calculated as a percentage of the amount recovered by the government agency. The exact percentage in particular cases is determined by a variety of factors. But in all cases, the government must get some money first, and then the whistleblower gets a part of that money. This has two primary implications for someone considering whether to blow the whistle through one of the reward programs.

First, not all wrongdoing leads to financial recoveries by the government. In some cases, the government will respond not by seeking money from which a reward will be paid, but instead by seeking a court injunction to stop the wrongdoing, or by going after the wrongdoers under criminal law.

Second, even when the government does seek a monetary recovery from which a reward could be paid, the government must be able to collect that money. Some targets—big companies with lots of assets inside the United States—are relatively easy for the government to collect against. Other targets—for example, individuals living in other countries and without assets in the United States—are much harder. This “collection risk,” as us lawyers like to call it, is something to consider when deciding whether to blow the whistle through one of the formal reward programs.

**The Four Whistleblower Reward Programs Most Likely Implicated by Cryptocurrency Wrongdoing**

In the United States, we have numerous different whistleblower reward programs covering different types of unlawful conduct. Here are the four that I think are most
likely to be implicated by crypto-related wrongdoing. For each, I give an example of the type of conduct that might be covered by that program.

The SEC Whistleblower Program

What it covers: Following the financial crisis of 2008, and the disclosure of the massive Bernie Madoff Ponzi scheme, the Dodd-Frank Wall Street Reform and Consumer Protection Act was passed. That law created a program designed to reward whistleblowers who disclose violations of securities laws to the U.S. Securities Exchange Commission (SEC), and to protect those whistleblowers from retaliation by their employers. That program, administered by the SEC Office of the Whistleblower, provides a path for someone with information relating to a violation of the securities laws to report that information to the SEC using what is known as a “tip, complaint and referral” (TCR). If the TCR is presented to the SEC using the correct procedures, and if the government collects at least $1 million as a result, then the SEC will award the whistleblower between 10-30% of the money collected. Since the first award made by the SEC under this program in 2012, the SEC has awarded more than $800 million to whistleblowers.

The types of misconduct potentially within the scope of the SEC whistleblower program include market manipulation (for example, so-called “pump and dump” schemes), misstatements or omissions in required disclosures (for example, in quarterly or annual financial reports), sales of unregistered securities, insider trading, Ponzi schemes, and bribery of foreign officials (which potentially violate the Foreign Corrupt Practices Act, also within the SEC’s jurisdiction).

Cryptocurrencies are not inherently considered “securities” governed by the SEC, but the SEC will consider a cryptocurrency to be a “security” if it is marketed as an investment in a particular company, as most initial coin offerings (ICOs) have been. In addition, as crypto-related companies become publicly traded entities, as Coinbase did recently, they become subject to SEC reporting requirements.

A crypto example: In late 2019, the SEC brought an enforcement action against Telegram Group, Inc., and TON Issuer Inc. to stop the sale of GRAM tokens, which had raised $1.7 billion. The SEC alleged that GRAMS were securities, and that the companies had sold those securities to individuals in the United States without first registering the securities under U.S. law. The court in that case ordered the defendants to disgorge approximately $1.2 billion and imposed a civil penalty of $18.5 million.

The CFTC Whistleblower Program

What it covers: The Dodd-Frank Act also established a program to encourage whistleblowers to report fraud in connection with the sale of commodities futures. Under this program, a whistleblower must disclose the information to the Commodity Futures Trading Commission (CFTC), which has adopted procedures like the SEC Office of the Whistleblower.

As is the case with the SEC’s program, if the information leads to a recovery, then the CFTC will award the whistleblower between 10-30% of the total amount obtained
by the Government. Since its inception, the CFTC whistleblower program has paid out approximately $90 million in known awards, and an unknown additional amount in awards where the amount has not been disclosed. It is probably safe to assume that, over the seven years that the program has been active, the CFTC has paid out over $100 million in awards to whistleblowers.

The CFTC, supported by several courts, has ruled that cryptocurrencies are commodities, and thus within the CFTC’s jurisdiction where that cryptocurrency is part of a derivatives contract, or where there is fraud or manipulation in the trading of the cryptocurrency. Of particular concern to the CFTC would be unregistered cryptocurrency exchanges, or businesses offering to finance cryptocurrency transactions (sometimes called “margin buying”). The CFTC also has regulatory authority to stop Ponzi schemes involving cryptocurrencies. The CFTC has established a Digital Asset Task Force that is specifically focused on cryptocurrency issues within the CFTC’s jurisdiction.

A crypto example: In July of 2020, the CFTC announced charges against Plutus Financial, Inc. and Plutus Technologies Philippines Corp. (which did business under the name Abra), for running a non-registered exchange that permitted customers, using a mobile app, to enter swaps of digital assets and foreign currencies. The CFTC fined the companies $150,000 and entered an order prohibiting the companies from engaging in this line of business. As is often the case, the CFTC and SEC worked jointly on the matter, due to their overlapping jurisdiction.

The IRS Whistleblower Program

What it covers: Since the passage of the Tax Relief and Health Act of 2006, a tax whistleblower who provides information to the United States Internal Revenue Service (IRS) about tax fraud or underpayment of taxes, totaling $2 million or more, qualifies for an award of between 15% and 30% of the total recovered by IRS. The tax whistleblower law is not limited solely to intentional fraud; any underpayment of taxes, even if the result of mere negligence or innocent calculation error, is covered. However, intentional frauds are the bread-and-butter of the IRS Whistleblower Office, which administers the program. Since 2006, the IRS has paid out more than $1 billion to whistleblowers.

The IRS considers cryptocurrencies, or other virtual assets, to be property just like any other. This means that, for persons or companies subject to taxation by the United States, cryptocurrency transactions must be reported on their tax returns, and money made from such transactions, including capital gains, is taxable. Similarly, if a business receives payment for goods or services in cryptocurrencies must treat those payments as income, and wages paid in cryptocurrencies must be reported to the IRS and are subject to withholding and payroll taxes.

A crypto example: Tax privacy rules generally mean that we know less about IRS enforcement than we do about enforcement by other agencies. However, there are some cases in which the Department of Justice will assist the IRS in court proceedings relating to IRS investigations, and this can give us some window into the types of cases the IRS is pursuing. One known instance of this involved the use of a so-called “John Doe summons” served on Coinbase. A federal court in California
authorized the summons, which allowed the IRS to obtain records of Coinbase customers’ cryptocurrency transactions for the period 2013-15. And just last month, in April of 2021, a similar “John Doe” summons was approved by a federal court in Massachusetts, and served on another high-profile crypto player, currency exchanger Circle Internet Financial Inc. That summons sought information about transactions with or through Circle during the period 2016-2020. The scope of these summonses (and the press releases issued by DOJ when they obtained the summonses) make it clear that the IRS is investigating possible tax violations by Coinbase and Circle customers, most likely failure to report capital gains on cryptocurrency trades made through those platforms.

The Anti Money Laundering Whistleblower Program

What it covers: In early 2021, Congress passed the Anti-Money Laundering Act of 2020 (AMLA). This new law creates a whistleblower reward program, to be administered by the U.S. Department of the Treasury, like the ones administered by the SEC, CFTC, and IRS. It covers violations of the Bank Secrecy Act, and a whistleblower under this program may receive a reward of up to 30% of the amount recovered by the government. The Department of the Treasury is required to issue regulations with the details of how it will implement AMLA; this has not yet occurred, but likely will happen soon. However, whistleblowers do not need to await those regulations to begin making reports to the government.

A company that acts as a currency trader, currency exchanger, or money transmitter is considered a “money services business” (MSB) subject to the Bank Secrecy Act. Almost any business that engages in the sale, trade, or transmission of cryptocurrencies will be an MSB. If the business is located outside the United States, it can still be considered an MSB if it has customers in the United States. The Bank Secrecy Act has numerous requirements that apply to MSBs, including that the business register with the U.S. Department of the Treasury’s Financial Crimes Enforcement Network (“FinCEN”), that the business implement an internal Anti-Money Laundering (AML) program that is designed to prevent money laundering and terrorist financing, and that the business comply with various record-keeping and reporting requirements, including the requirement to file suspicious activity reports (SARs) with FinCEN. Accordingly, a whistleblower with information showing that an MSB is failing to take these required steps could have a claim under the new AMLA whistleblower provision.

A crypto example:

In 2015, FinCEN and the Department of Justice assessed a $700,000 civil penalty against Ripple Labs, Inc., and their cryptocurrency XRP. At the time, XRP was second only to Bitcoin in market capitalization. FinCEN concluded that Ripple acted as an MSB and sold XRP without registering with FinCEN, and by failing to implement an adequate AML program. Ripple entered into a settlement agreement with the government in which is agreed to come into compliance with Bank Secrecy Act requirements, including registration and AML.

As the popularity and value of cryptocurrencies continues to grow, the various government agencies mentioned above will focus more and more of their
investigative time and resources on ferreting out illegal uses. Given the roles that cryptocurrencies play in financial transactions around the globe, securities and commodities violations, tax violations, and anti-money laundering violations all are likely to be both prevalent, and of great interest to the government. Whistleblowers from inside crypto-related businesses are likely to lead the way in fighting against unlawful activities, and through the various reward programs offered by the government, those whistleblowers can do good and do well.

© 2021 by Tycko & Zavareei LLP

National Law Review, Volume XI, Number 147