

Will insurance cover cryptocurrency claims?



Brian Scarbrough, a partner and co-chair of Jenner & Block's insurance recovery and counseling practice, and Justin Steffen, a partner with Jenner & Block's complex commercial litigation practice, are members of the firm's fintech group. Mr. Scarbrough counsels on insurance issues raised by cryptocurrencies, initial coin offerings, blockchain and other distributed ledger technologies. He can be reached at 202-637-6306 and bscarbrough@jenner.com. Mr. Steffen is focused on the intersection of technology and the financial services industry, including issues pertaining to marketplace lending, cryptocurrency and blockchain, and payments. He can be reached at 312-840-7262 and jsteffen@jenner.com

For years, the cryptocurrency boom continued without regulatory reprisal, but the era of a digital Wild West and unregulated initial coin offerings may have come to an abrupt end.

In July 2017, the U.S. Securities and Exchange Commission issued a report indicating that tokens can be securities in certain circumstances. In the months that followed, the SEC and other regulators issued public statements repeatedly warning industry participants that ICOs may violate securities and other laws. Regulatory actions and subpoenas followed — targeting the companies that sold virtual currencies or tokens, the lawyers and advisers that facilitated those sales, and the exchanges.

Those left to deal with the consequences may incur serious legal fees in the months to come, but how will they pay for those fees?

Insurance policies may provide an answer.

Generally, cryptocurrency refers to a decentralized, digital or virtual currency that utilizes cryptography for security. Cryptocurrency's origins can be traced to Satoshi Nakamoto's 2008 whitepaper on bitcoin. Today, a decade later, there are well over 1,000 different coins, tokens or cryptocurrencies with a combined market cap in the hundreds of billions of dollars. Many new coins or tokens are created in connection with an initial coin offering in which a certain percentage of a new coin or token is often sold to early investors to complete or fund a project.

In 2017, there were approximately 210 ICOs taking in billions of dollars. By mid-April 2018, more money had been raised through ICOs in 2018 than in all of 2017.

The DAO report

Although regulators initially took a wait-and-see approach with ICOs, in July 2017 the SEC issued its decentralized autonomous organization, or DAO report. In the report, the SEC examined The DAO, an unincorporated organization with the objective of operating a for-profit entity that would fund projects through tokens. Notably, the SEC concluded that The DAO token sales violated federal securities laws and warned industry participants that tokens can be subject to securities laws.

On Sept. 25, 2017, the SEC announced the creation of a cyber unit that would focus on “targeting cyber-related misconduct,” including misconduct involving ICOs. The formation of that unit was joined by a flurry of enforcement activity, including:

- In September 2017, the SEC filed suit in the Eastern District of New York alleging that two ICOs were frauds.

- In January 2018, the SEC brought a complaint in the Northern District of Texas that halted an allegedly fraudulent ICO by AriseBank, which claimed to be the first “decentralized bank.”

- According to news reports, on Feb. 28, 2018, the SEC issued subpoenas to as many as 80 entities and individuals involved in the virtual currency space — including companies engaged in ICOs and the lawyers and advisers who facilitated ICOs.

- On March 1, 2018, Overstock.com Inc.'s shares fell as much as 10% after the company's subsidiary, tZero, revealed that the SEC had requested information on tZero's ICO back in December.

- In April, the SEC filed a complaint against the co-founders of a financial services startup for an allegedly fraudulent ICO that raised more than \$32 million and obtained a court order freezing more than \$27 million in trading proceeds associated with a Delaware-based financial technology company.

Does insurance respond?

Entities or individuals receiving subpoenas or lawsuits should consider whether insurance may provide coverage for the likely significant defense costs to be incurred. There are two coverages that are most likely to be relevant: directors and officers liability insurance and professional liability insurance.

D&O generally provides coverage for claims for a wrongful act first made against an insured during the policy period. Coverage usually is provided in three instances: to an insured individual when he or she is not indemnified by the company; to the company to reimburse it for the indemnification it provides to an insured individual; and to the company to the extent the company is subject to a securities claim or any type of nonexcluded claim.

When faced with an SEC subpoena or a lawsuit, the definition of “claim” in a D&O insurance policy will be important. A claim should include at least written demands, a civil or criminal proceeding (lawsuit), an administrative or regulatory proceeding, and a governmental investigation commenced by a written notice identifying the individual as a person against whom a proceeding may be brought. The policy also will require that the claim be for a “wrongful act.” That term should be broadly defined to include at least any error, misstatement, misleading statement, act, omission, neglect, or breach of duty actually or allegedly committed by the insured in his, her or its insured capacity or any other matter claimed against the insured individual or company in an insured capacity.

D&O policies also may provide so-called inquiry coverage or pre-claim coverage when, for example, a governmental agency has requested that an individual appear to provide testimony or produce documents in that individual's insured capacity. Importantly, this expanded coverage usually does not require any allegation of a wrongful act

by the insured individual, but coverage will be dependent on the particular request for information and policy language.

In determining if an individual or company has coverage, attention should be made to the policy definition of insured individuals and the types of claim covered for the company. Private company D&O policies may extend coverage to all employees while also extending coverage to many types of claims against the company, but there may be exclusions for certain types of securities claims. This will depend on the specific policy wording and the circumstances of whether an ICO lawsuit or investigation concerns “securities.” Unlike private company D&O policies, public company D&O policies generally limit coverage for a company only to securities claims. And as to individuals, public company D&O policies generally limit coverage to only selected positions, such as members of the company's board of directors, company officers and other key corporate positions, such as general counsel or risk managers.

D&O policies contain policy exclusions and limit the scope of covered losses or damages. These provisions should be examined carefully. For example, electronic data or similar exclusions; exclusions for criminal conduct or gaining illegal profit triggered only by a final, nonappealable adjudication; and the definition of covered loss may preclude coverage for civil or criminal fines or penalties or matters which may be deemed uninsurable.

Errors and omissions and professional liability insurance also could be relevant if a subpoena or lawsuit targets the lawyers or other advisers that facilitated ICOs. These types of policies cover companies and individuals to the extent that a third party makes claims against them for providing or failing to provide professional services.

Whether professional liability policies are relevant will depend on the type of claim at issue and the specific policy language. But much of the same discussion likely will be relevant with professional liability policies as with D&O policies. Lawyers and other advisers to ICOs should strongly keep such policies in mind.

Provide notice

Whether or not there is a claim or coverage is triggered, companies and individuals would be well served to consider notifying their insurers if they are faced with a claim or even the possibility of a claim. At the very least, a notice of circumstances could be made, meaning that a company or individual is aware of circumstances that may lead to a claim or liability and is reporting it now to the insurer. A notice of circumstances can serve as a placeholder for coverage in the event that a claim subsequently develops.