Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

How To Use Insurance To Shield Against Cryptocurrency Risks

By **Jeff Sistrunk**

Law360 (July 25, 2018, 9:34 PM EDT) -- As cryptocurrencies continue their meteoric rise, companies in the space are facing an expanding range of risks, including the threat of large-scale theft and class actions filed by disgruntled investors in funding ventures known as initial coin offerings.

Here, Law360 looks at some of the perils faced by cryptocurrency businesses, and how insurance may help shield against those risks.

Cryptocurrency Theft

Digital currency companies, exchanges and purchasers have become increasingly popular targets for cybercriminals in recent years, with thieves stealing more than $1 billion worth of cryptocurrency in the first half of 2018, according to a June report issued by cybersecurity firm Carbon Black Inc. In one headline-grabbing incident in January, hackers plundered about $500 million of a cryptocurrency called NEM from Japanese exchange Coincheck, which had the digital coins stored in an internet-linked "wallet."

According to attorneys, with cryptocurrencies now numbering in the thousands, theft will continue to be a major concern for industry participants and consumers — one that demands robust insurance coverage.

While several major global insurers — including Chubb Ltd. and XL Group Ltd. — have begun offering insurance policies specifically tailored to cryptocurrency theft, attorneys say businesses and consumers may also be able to turn to traditional crime insurance for coverage.

Many conventional crime policies cover losses of funds due to computer fraud. Insurance companies have long contended that such language only applies to incidents involving hackers directly infiltrating a policyholder's computer systems, but two federal appeals courts recently undercut that argument by finding coverage under crime policies for losses attributable to multiple-step "social engineering" schemes in which criminals manipulated companies' employees into wiring funds to sham bank accounts by posing as executives of those businesses in emails.

Anderson Kill PC partner Daniel J. Healy, who represents policyholders, said those decisions, rendered in cases called Medidata and American Tooling Center, indicate that some courts are now taking a broader view of what can constitute computer fraud under crime policy language. As such, courts may be

receptive to arguments that crime coverage also applies to cryptocurrency losses tied to attacks on digital wallets or blockchain networks, which enable the currencies, attorneys say.

"Recent decisions on coverage under crime policies have been useful, applying fairly old policy language to fairly high-tech schemes," Healy said. "We would like to think that courts looking at cryptocurrencies and blockchain in general will understand that, despite the new technologies, the same types of business transactions are involved. Because of that, many existing policies may provide coverage for these losses."

Barnes & Thornburg LLP partner Scott Godes, who also represents policyholders, said cryptocurrency businesses and consumers should challenge coverage denials by their crime insurers.

"It really should not be the policyholder's obligation to be an insurance expert at the time of purchase to figure out where there are trapdoors in coverage as they are buying them," Godes said. "It should be the obligation of the underwriter and the policy drafting team to present a product that is ready and able to provide coverage for companies in this space."

Initial Coin Offering Litigation

Digital currency fundraising endeavors known as initial coin offerings, or ICOs, have attracted the attention of plaintiffs attorneys, presenting a host of potential legal exposures for businesses that launch such offerings.

In ICOs, startups create and sell their own digital currency in order to fund projects, using the same blockchain technology that powers bitcoin, ether and other cryptocurrencies. Through these offerings, companies can sell digital tokens that promise purchasers access to a product or service, while other tokens are structured more like investments.

However, the regulatory landscape surrounding ICOs remains unclear, and a slew of companies have been hit with class action complaints alleging their offerings did not comply with the law. For instance, in one recently filed suit, investor Ryan Coffey alleged that blockchain developer Ripple Labs Inc., CEO Brad Garlinghouse and subsidiary XRP II LLC skirted state and federal securities law by marketing and selling their tokens as strong investments without first registering them with the U.S. Securities and Exchange Commission.

Companies and their executives have long relied upon directors and officers policies to cover claims stemming from issues with traditional initial public offerings. But at this point, it is unclear whether D&O policies will also apply to actions tied to ICOs, attorneys say.

"D&O coverage in the cryptocurrency arena is an emerging area," said Ivan J. Dolowich, co-managing partner of Kaufman Dolowich & Voluck LLP, who represents insurers. "Right now, in the cryptocurrency environment, ICOs may give rise to claims by disgruntled purchasers. However, while federal and state regulators have started to scrutinize these ICOs, the regulatory landscape is still unsettled, so it is uncertain whether these sorts of claims will trigger coverage under a D&O policy."

One of the key unsettled questions bearing on the availability of D&O coverage for ICO-related actions is whether digital tokens are securities. D&O policies often include coverage for "securities claims" alleging wrongful acts.

A Florida magistrate judge on June 25 issued a first-of-its-kind finding, subject to a district judge's final approval, that tokens issued by technology startup Centra Tech Inc. qualify as securities. And Bill Hinman, the director of the SEC's Division of Corporation Finance, said at a cryptocurrency conference on June 14 that many digital tokens sold in ICOs should be considered securities, although his remarks weren't an official statement of the agency's policy.

Regulatory Investigations

As regulators get their heads around ICOs, businesses conducting such offerings should be wary of potential probes or enforcement actions by the SEC and Federal Trade Commission, which may also implicate D&O coverage, according to attorneys.

The SEC fired a warning shot in July 2017, when it concluded that an ICO conducted by a group known as the DAO amounted to an unregistered securities offering. The agency began regulating ICOs more aggressively following the DAO report, carrying out enforcement actions that alleged fraud in several cases and reportedly issuing dozens of subpoenas to parties engaged in ICOs as part of its broader crackdown on illegal offerings.

Although ICOs are new territory in the D&O insurance realm, policyholders should still be able to rely on existing case law, according to some attorneys, such as the Second Circuit's 2011 decision in MBIA Inc. v. Federal Insurance Co., which found broad coverage under a D&O policy for various costs relating to a government investigation.

"When looking at an SEC or FTC investigation into a token offering, we would expect case law like the MBIA decision to apply," said Anderson Kill partner Stephen D. Palley. "Even though we are dealing with a new kind of technology, that doesn't mean old case law can't apply."

Marc S. Voses, co-chair of Kaufman Dolowich & Voluck LLP's data privacy and technology services practice, said insurers are likely to deal with developing cryptocurrency risks in the short term by "adding manuscripted endorsements to policies indicating the risks the insurer is willing to cover, and those it is unwilling to take on."

"With D&O policies as well as cyber and crime policies potentially implicated, it will be interesting to see whether a new product will emerge to address the risks faced by cryptocurrency industry participants," Voses said.

"These products were not initially intended to cover these specific types of risks," he added. "It will take a while for the marketplace to feel things out and decide how to respond to the needs of policyholders."

--Editing by Katherine Rautenberg and Kelly Duncan.
