Blaney McMurtry LLP

PUBLICATION

Kleptocurrency: Crime insurers face new challenges with cryptocurrency

Date: May 01, 2019
Co-Author: Maria Christodoulou

This article was originally published by Claims Canada Magazine.Click here to view the PDF file.

Every day seems to bring a new headline announcing another massive cryptocurrency loss. In February, QuadrigaCX, Canada's largest cryptocurrency exchange, allegedly lost access to some $190 million worth of clients' cryptocurrency. According to QuadrigaCX, its CEO was the only person able to access the cryptocurrency. The CEO was reported to have died suddenly in India at the age of 30 – a report that was greeted with skepticism in some quarters.

Insurance for financial loss resulting from the use of technology to commit fraud has existed in various forms for decades. However, cryptocurrency represents a new asset class, and thus a new challenge for fidelity/crime insurers. An understanding of cryptocurrency and blockchain technology is essential.

What is Cryptocurrency?

A cryptocurrency is a digital asset that serves as a medium of exchange and relies on cryptography to control the creation of units and to secure and verify financial transactions. Over 1,000 cryptocurrencies have been in use. Cryptocurrencies differ from traditional currency in that they: (1) are decentralized; (2) are generated in a limited supply; (3) have no physical form; (4) accommodate pseudonymous – and often anonymous – transactions; and (5) are not legal tender. Cryptocurrency transactions are generally non-reversible.

Decentralization is a critical feature of cryptocurrency. In a "traditional" online transaction between two people, a third party intermediary (such as PayPal) is necessary to complete the transaction. In a decentralized model, transactions are not processed through a third party; they

move directly from person to person. One issue that a cryptocurrency system must address is how to confirm – without a third party intermediary – that A owns the cryptocurrency A proposes to transfer to B, and has not already spent it in a prior transaction. This is known as the "double-spend" problem.

A cryptocurrency system solves the double-spend problem by use of a blockchain, which is a decentralized public ledger distributed through a peer-to-peer network among all the users of that cryptocurrency. Each user maintains a "wallet" (software which stores the user's private keys). A private key is a string of alphanumeric characters, the possession of which enables the user to transact cryptocurrency. If a private key is lost (as is alleged with QuadrigaCX), the cryptocurrency cannot be accessed and is effectively gone forever.

The wallet applications carry out the transaction by "announcing" the proposed transaction (which includes the private key) to the network of participating servers. These servers ("cryptominers") collect proposed transactions and verify that the cryptocurrency exists. Cryptominers then collect transactions and aggregate them in blocks. When a transaction appears in a valid block, it is considered confirmed.

Crime Insurers Respond

Several American insurers have made forays into the cryptocurrency sphere. A fundamental threshold issue in extending crime coverage to cryptocurrency is that crime policies only cover "money" (coins and currency), "securities" and certain other classes of tangible property. Cryptocurrency is an intangible asset, so specific endorsement language is necessary to extend coverage to it.

In the United States, Insurance Services Office, Inc. introduced an "Include Virtual Currency as Money" endorsement, while Great American Insurance Group introduced an endorsement that adds cryptocurrency to the definition of "Securities". To date, no Canadian crime insurer has offered a general coverage extension in respect of cryptocurrency, although several are exploring the idea.

Considerations for Crime Insurers

While cryptocurrencies offer protections against double spending, such protocols cannot prevent wrongful single spending. The blockchain is indifferent as to whether the user of a private key is the "legitimate" owner, or a fraudster.

Assuming that cryptocurrency is recognized as covered property by endorsement, some of the "traditional" crime insuring agreements could apply. Examples include employee dishonesty, social engineering fraud (SEF) and (with important qualifications) computer fraud. Other insuring agreements, such as loss inside the premises and loss outside the premises, do not "fit" conceptually with cryptocurrency loss scenarios.

Employee Theft: Cryptocurrency can be lost through employee dishonesty. In April 2018, an Indian cryptocurrency trading platform alleged that a rogue employee sent 438 bitcoins to an

unauthorized recipient. As with any loss alleged to have been caused by an employee, there will be evidentiary issues surrounding the proof that it was an employee that caused the loss, rather than a third party.

One challenge in the investigation of cryptocurrency losses is that the transfer mechanism is nearly anonymous. In order to prove employee involvement, it would be necessary to demonstrate that the employee had access to the private key, and to negate the possibility that the private key fell into the hands of a third-party fraudster. As infinite copies of a private key can exist, this could pose a practical challenge to demonstrating employee involvement.

SEF: SEF occurs when an insured voluntarily transfers property based on a fraudulently induced mistaken belief as to the ownership of that property. An insured may be duped into transferring cryptocurrency to a public key that is mistakenly believed to represent a legitimate recipient, but is in fact controlled by a fraudster. As with existing SEF coverage endorsements, underwriters will need to consider appropriate limits and whether verification/callback requirements might be appropriate conditions to coverage.

Computer Fraud: The intent of computer fraud coverage is to indemnify the insured with respect to hacking incidents, i.e., where a hacker directly causes the insured's computer to make an unauthorized transfer of money without any involvement on the part of the insured or its employees. Some U.S. insurers have made it clear their policies do not provide indemnity for cryptocurrency hacking losses, but a form of specialized computer fraud coverage could be developed for hacking incidents involving cryptocurrency.

Loss Inside/Outside the Premises: These coverages do not readily apply in the case of cryptocurrency, because they are tied to the existence of physical property and physical premises. But what happens if the private key is given physical manifestation, such as a wallet stored on a USB drive, or a piece of paper with the private key written on it? At first blush, it would seem that coverage could arise, as there is now something that can be physically transported. However, the issue is not that clear. A piece of paper containing a written private key is simply a piece of paper containing data; it is not the cryptocurrency itself. It can be copied ad infinitum, and has no more intrinsic value than a monthly bank statement with an account balance written on it.

Underwriters will also need to analyze new types of losses as the cryptocurrency ecosystem continues to evolve. For example, if an employee uses workplace computing resources for cryptomining (a costly, energy-intensive process), is that an employee theft loss? Policy conditions, such as those relating to valuation, will also need to be considered. Cryptocurrencies are notorious for significant price volatility, so valuation provisions will need to be drafted with this in mind.

Despite the scary headlines, cryptocurrency is beginning to form part of the legitimate commercial ecosystem – a part that displays significant growth potential. The question for crime

insurers is not whether there should be coverage for cryptocurrency, but what form(s) such coverage will take.