SAUL EWING ARNSTEIN & LEHR LLP

Alert

CYBERSECURITY AND PRIVACY PRACTICE

JANUARY 2018

AUTHOR

JONATHAN A. HAVENS

In The Midst of Cryptocurrency Craze, Cybersecurity Threat Emerges

SUMMARY

Ernst & Young (E&Y) indicated in a report (https://go.ey.com/2DyD47T) released on Monday, January 22, 2018, that more than 10 percent of initial coin offering (ICO) funds are lost or stolen in hacker attacks (almost $400 million), and that cryptocurrency exchanges have an average of $2 billion in hacking losses. By way of background, an ICO is a fundraising mechanism in which a new venture sells its own cryptocurrency "tokens" to investors in exchange for legal tender or other digital currencies like Bitcoin and Ethereum.

Per E&Y, "[p]hishing is the most common form of funds theft during ICOs," noting that "hackers steal ... up to US$1.5 million in ICO proceeds per month." In announcing (https://go.ey.com/2mZ7lkY) its report, E&Y observed that:

> Hackers benefit from the hype, irreversibility of blockchain-based transactions and basic coding errors that, had the ICO been carefully reviewed by experienced developers and cybersecurity analysts, could have been avoided. Funds are misappropriated via substituting project wallet addresses (phishing, site hacking), accessing private keys and stealing funds from wallets, or hacking stock exchanges and wallets; all on top of indirect losses caused by high reputational risks for project founders.

E&Y's report came soon after U.S.-based cybersecurity firm AlienVault released its analysis (http://bit.ly/2rzVzD9) of malware that is being used to mine the Monero cryptocurrency and send it to Kim Il Sung University in Pyongyang, North Korea. As noted in a recent article in The Hill (http://bit.ly/2BpUEom) about the AlienVault report, cryptocurrencies like Monero have gained popularity over the past couple of years, "particularly among cyber criminals looking to hide their tracks"; Monero claims to be "untraceable." Monero and other digital currencies have also emerged as alternatives to Bitcoin, which, in light of its massive popularity and price spike, has attracted regulatory scrutiny.

On the topic of regulatory scrutiny, in remarks (http://bit.ly/2n3iGBq) at the Securities Regulation Institute in Washington, D.C. earlier this week, U.S. Securities and Exchange Commission (SEC or the Commission) Chairman Jim Clayton delivered a stern warning on ICOs:

> Market professionals, especially gatekeepers, need to act responsibly and hold themselves to high standards. To be blunt, from what I have seen recently, particularly in the initial coin offering

> ("ICO") space, they can do better…I have instructed the SEC staff to be on high alert for approaches to ICOs that may be contrary to the spirit of our securities laws and the professional obligations of the U.S. securities bar.

Chairman Clayton went on to indicate that the Commission is also looking closely at distributed ledger or "blockchain" technology, and in particular, "public companies that shift their business models to capitalize on the perceived promise of distributed ledger technology and whether the disclosures comply with the securities laws, particularly in the case of an offering."

This is not the first time Chairman Clayton has raised the alarm on cryptocurrencies and ICOs (see, e.g., December 11, 2017 statement [http://bit.ly/2C7emqG]). In recent days, the Commission issued a letter (http://bit.ly/2DpXsaj) to two trade groups, Investment Company Institute and Securities Industry and Financial Markets Association, in which the SEC said that cryptocurrency funds raise "investor protection issues that need to be examined before sponsors begin offering these funds to retail investors." Also within the last week, the U.S. Commodity Futures Trading Commission (CFTC) and the SEC issued a joint statement (http://bit.ly/2FXkRhB) regarding virtual currency enforcement actions. The statement followed on the heels of the CFTC filing two lawsuits (http://bit.ly/2DzQso5) against "allegedly fraudulent cryptocurrency investment schemes."

To be sure, regulatory scrutiny and enforcement action in the cryptocurrency space have focused on securities law and investor protection rather than cybersecurity vulnerabilities. However, regulators could broaden the scope of their actions in light of recent events and increased focus on such vulnerabilities, which appear to be widespread.

We will continue to monitor these and other cryptocurrency and cybersecurity developments and provide further updates as more information becomes available. If you have any questions regarding an issue raised in this alert, please contact the author or the attorney at the firm with whom you are regularly in contact.

This Alert was written by Jonathan A. Havens, a member of the firm's Cybersecurity and Privacy Practice. Jonathan can be reached at 410.332.8757 or jonathan.havens@saul.com. This publication has been prepared by the Cybersecurity and Privacy Practice for information purposes only.