Analysis

Robbing a Locked Bank Vault from Home: Legal Issues Raised by Cryptocurrency Frauds

A cryptocurrency wallet can be dispiritingly similar to an in-real-life wallet, whose currency and credit/debit card contents are only as secure as we keep the wallet itself.

By **Chris Ott, Davis Wright Tremaine** | September 17, 2018 at 10:00 AM

The number of individuals and businesses holding or using cryptocurrencies is expected to reach **200 million by 2024**. The advent of cryptocurrencies has raised a host of legal issues; some of the most immediate ones—such as whether cryptocurrencies are securities—appear to have been **resolved**, but cryptocurrency theft remains a **major concern** for traders and investors given that billions of dollars of cryptocurrency are **stolen** every year. These cutting-edge problems intersect in interesting ways with companies' existing fraud and anti-money laundering concerns, but it all starts with the cryptocurrency "wallet."

A cryptocurrency wallet stores the cryptographic keys (both public and private) that one uses to access and spend cryptocurrencies. Each wallet can contain multiple keys as well as independent cryptographic software or a mnemonic device for memorizing the cryptographic keys. It is important to note that crypto wallets themselves are generally not a part of a given cryptocurrency's technology. Therefore, the wallet can be dispiritingly similar to an in-real-life (IRL) wallet, whose currency and credit/debit card contents are only as secure as we keep the wallet itself.

A Cryptocurrency Theft Primer

Cryptocurrency theft frustrates technology in several ways. Thieves appear to adhere to **Sutton's Law** because most of the documented attacks target "where the money is": the crypto wallet itself.

The most common manner of losing control of your crypto wallet is to lose operational security of your smartphone and the cryptographic keys stored on it. One way this occurs is when users unknowingly download malware from an app store. For example, traders at Poloniex, an American cryptocurrency exchange, **downloaded** Android mobile applications hackers had posted on Google Play. These apps falsely purported to provide a mobile gateway to the crypto exchange Poloniex had established for Bitcoin and Monero markets. The traders inputted their information into the app, including their cryptographic keys, which put thousands of Poloniex traders' infected wallets at risk.

To address this risk, cryptocurrency traders should install as little software as possible, enable 2-factor authentication (or higher) on all applications, and take care to research an app's official connection with the cryptocurrency project. Other similar techniques practiced by hackers involve **malicious browser add-ons for cryptocurrency trading** or compromising public **Wi-Fi routers**.

Another technique for stealing your crypto wallet information is social media engineering. Documented examples include deploying **bots in a Slack-channel**, **site- cloning**, and **phishing**. However, one of the most pernicious current methods combines social engineering techniques with attacks upon the operational security of the victim's mobile phone SIM card, which opens new frontiers of legal liability for mobile phone service providers as well.

SIM Swap Fraud

SIM swap fraud can target **all types** of online banking. The fraud is based upon a simple process that most of us have completed at least once in our life. When one registers a newly-purchased phone, a new SIM card is usually registered to an existing phone number. Once that is done, the old SIM card becomes invalid and the first phone will stop processing signal. However, if someone else effectuates the transfer, they will have successfully hijacked all the target's telephone calls and SMS messages to the scammer's SIM card, at least until the fraud is noticed. In this manner, scammers can defeat most two-factor authentication protections.

The fraud typically begins with a call from a scammer claiming to represent the target's mobile service provider. Any number of lies or promises may follow—better speed, fewer drops, or better reception—but the key goal is for the scammer to get your 20-digit SIM card number. The scammer will then contact the mobile service provider and begin the process of migrating the target's telephone number to a new SIM card that the scammer possesses. If the story provided by the scammer initially is believed, when the target receives a confirmatory text from their actual service provider, he or she will happily approve the transfer. But once the transfer occurs, the target's phone number and related stored information is hijacked to the scammer's phone with the newly activated SIM card. The old phone will no longer function and the new phone, that the scammer possesses, will receive all the target's communications. The actual transfer can take four hours. The fraudsters often try to annoy the victim into turning off their ringer during this time. They may accomplish this by repeated calls to the original/transferee phone.

It is important to note that this scam involves fooling at least two different people: the phone owner and the service provider. However, it is likely the fraud did not start with the scammer's SIM card swap phone call to the phone owner. At the point that the phone call was initiated, the scammer likely already has a great deal of information about the target, including banking information and passwords. These banking details could have been harvested from prior phishing attacks or culled from large databases of this type of information that have been collected from other large-scale hacks and are available on the deep web. The data leakages that make up this "starter" knowledge were likely harvested from security failures the victim, the banks, or, as with loss of the crypto wallet, the cryptocurrency exchanges as well. Each of those failures may have their own litigation or regulatory consequences.

Once the cryptocurrency information is harvested by the scammer, the target's bitcoins can be transferred, and traditional bank accounts emptied. However, this is not necessarily a one-time event. Once a SIM card is in the possession of others, scammers can try again and again to **re-hijack** the phone targeting brick and mortar stores and customer service arms of large mobile service carriers. The approaches would again seek to exploit informational and training gaps in the carriers' systems to cause yet another fraudulent SIM swap. These repeated attacks are problematic because the carrier will usually have actual knowledge of the first fraudulent swap, which may heighten the legal risks to the carrier for the serialized swap attacks that may follow.

Legal Consequences of a Cryptocurrency Theft

A successful SIM swap fraud likely most likely involves duping a mobile phone carrier into initiating a SIM transfer. This will mean that there has most likely been an unauthorized disclosure of Customer Proprietary Network Information (CPNI). Pursuant to the Communication Act, the carrier could be liable for failing to protect that CPNI. While the exact contours of this liability in SIM swap fraud cases are still unclear, recent **lawsuits** have suggested that that the failure to prevent SIM swap fraud creates liability under the Communications Act and other laws protecting privacy of personal information.

This type of case thus poses several thorny problems for carriers. For the major carriers, these cases involve opportunistic frauds that may take advantage of the gap between the corporate decision-makers at one end and the large sales and customer service arms at the other. The possibility of an insider element to this fraud makes a robust internal investigation critical. In addition, the stakes of the bank fraud enabled by these alleged CPNI security failures can elevate an employee training issue into a **nine-figure legal dispute**.

Another potential avenue of liability exists for traditional financial institutions caught up in these transactions, which are covered by the Bank Secrecy Act and the Gramm-Leach-Bliley Act (GLBA). The Bank Secrecy Act has broad anti-money laundering and recordkeeping requirements that may be triggered by several aspects of scammers' fraudulent transactions. The GLBA is a federal law requiring financial institutions to explain how they share and protect their customers' private information. To be GLBA compliant, financial institutions must communicate to their customers how they share the customers' sensitive data, inform customers of their right to opt-out if they prefer that their personal data not be shared with third parties, and apply specific protections to customers' stored private data in accordance with a written information security plan created by the institution. This last requirement, called the **Safeguards Rule**, outlines the data security requirements that the financial institutions face, **including**:

- Private information must be secured against unauthorized access.
- Customers must be notified of private information sharing between financial institutions and third parties and can opt-out of private information sharing.
- User activity must be tracked, including any attempts to access protected records.

In a successful SIM swap fraud, all these protections may have been compromised.

The FTC's **Privacy of Consumer Financial Information Rule (Privacy Rule)** creates still other GLBA requirements. The failure to abide by these protections could trigger a flurry of enforcement activity. The GLBA is enforced by the FTC, the federal banking agencies, and other federal regulatory authorities, as well as state insurance oversight agencies.

Forgetting the traditional financial institutions for a moment, the cryptocurrency exchanges may have the same obligations. For example, whether a sponsor of a token offering or token exchange meets the Bank Secrecy Act's definition of a "financial institution" will determine if the sponsor must assist the U.S. government in the detection and prevention of money laundering. These financial institutions will have obligations to maintain cybersecurity policies and procedures under cybersecurity regulations pursuant to the GLBA and various state laws. As to the **Bank Secrecy Act**, the term "financial institution" is very broad. Therefore, cryptocurrency exchanges should at least explore their data protection responsibilities under the Bank Secrecy Act and the GLBA. This may include possible registration as a money transmitting business under federal and state law.

Even a trading platform that is a registered money transmitter in compliance with the Bank Secrecy Act and state licensing laws may face potential regulatory scrutiny from the Commodities Futures Trading Commission (CFTC). In a **detailed opinion issued in March 2018**, longtime federal judge Jack Weinstein ruled that "virtual currencies" are commodities subject to oversight by the CFTC.

For businesses, cryptocurrency fraud may only mark the beginning of litigation and regulatory headaches. The exploding value of these frauds incentivizes the fraudsters and raises the stakes. Like a stone striking a pond, the legal effects of these frauds ripple farther and farther out, altering the eyeline of everyone on the water.

Chris Ott, CIPP/US, advises industry-leading organizations in sensitive cyber incidents, national security matters, white-collar investigations, government enforcement actions, and high-stakes litigation. Chris has served as an influential law enforcement official for multiple administrations, led some of the largest white-collar investigations in United States Department of Justice (DOJ) history, won more than 30 trials as a first-chair litigator, and spearheaded some of the DOJ and the SEC's first successful cyber investigations. Chris, who is a partner in the Washington, D.C. office of Davis Wright Tremaine, can be reached at ***chrisott@dwt.com****.*