LAW | REAL ESTATE | FINANCE
DailyBusinessReview.com
ALM.
JUNE 23, 2022
DAILY BUSINESS REVIEW

Crypto Scams Are Flourishing and Brokerages Claim They Are Not Responsible

These types of socially engineered hacks are happening at an alarming rate, and the crypto brokers are well aware of the problem because they are on the front lines of the complaints generated by their customers.

By Aaron Cohn

You receive a text from your crypto wallet custodian, such as Coinbase or Gemini, claiming a fraudulent transaction has occurred on your account. Some detail related to the transaction is provided. You do not recognize the transaction and respond indicating fraud and that you would like to speak to a representative, who promptly calls you. The representative has your personal information, asks you to confirm certain details, then instructs you to report the code just sent to your phone to confirm your identity. You do it—and you've been hacked.

The code was generated by the scammer's online attempt to reset the password for your account to gain access through the two-step authentication process. Once you provide the code, the fraudster can access the account and execute transactions. When you are finally able to sort out what happened, the account has been cleaned out and—because of the nature of the blockchain—there is no way to recover the stolen crypto or track down the fraudsters, many of whom operate outside of the United States in jurisdictions with no accountability. Even worse, your crypto wallet custodian or broker denies any responsibility because, under the user agreements, you are purportedly responsible for the security of your account.

These types of socially engineered hacks are happening at an alarming rate, and the crypto brokers are well aware of the problem because they are on the front lines of the complaints generated by their customers. Last year, Coinbase publicly agreed to refund 6,000 account holders due to hacking, and that is just the tip of the iceberg across the industry. The FTC just reported that more than 46,000 consumers

Courtesy photo

Aaron M. Cohn, partner with Weinberg Wheeler Hudgins Gunn & Dial.

lost over $1 billion in crypto scams last year. Hundreds or thousands of victims are likely reporting this type of fraud to crypto institutions every day.

Socially engineered hacks like this are so rampant that the IC3, the FBI's Internet Crime Division, recently published an article warning consumers about this particular type of scam. And, it is not just the customers of crypto-

brokers like Coinbase that are subject to these socially engineered hacking schemes. According to a letter authored by two U.S. senators, 18 million Zelle customers—who use the peer-to-peer payment system to send and receive money among bank accounts—have experienced some type of similar fraud. Indeed, Zelle is currently named a defendant in a class action lawsuit pending in federal court related to this problem. Zelle transactions, however, are easier to track and recover because they involve real bank accounts that are subject to strict compliance regulations designed to deter and minimize fraud, among other things. In contrast, crypto is decentralized with no authority available to reverse or correct fraudulent transactions or track account holders.

Other hacking scams can be even more sophisticated, including the emerging "SIM-swap" scams that use fraudulently obtained SIM cards from a mobile service provider like T-Mobile to hack accounts. A "SIM card" is a digital identifier. Scammers that obtain or create a copy can gain access to the customer's phone, text or email communications. That information can be used to receive and use the two-step authentication codes required to gain access to crypto wallets and other accounts without the victim knowing. When this happens, the victim's crypto accounts can be hacked and wiped out without the victim even being contacted.

Given the situation, retail investors considering crypto "investments" need to understand the elevated risks and should employ heightened "safeguards" to help ensure they do not become the next victim. Institutions need to do more, too.

As to the risks, investors should understand that the benefits of crypto—including, primarily, the decentralized blockchain ledger—means there is no centralized party for the transactions executed on the blockchain. Transactions are recorded based on inputs that cannot be reversed. Thus, there is a higher risk to holding crypto.

Second, as to the heightened safeguards, retail investors should keep in mind the following:

- No matter who contacts you from your crypto brokerage (or any financial institution, for that matter), the better practice is to not respond. Instead, look up the official number for the institution and initiate independent contact. That way you know you are talking to a legitimate representative instead of a scammer.
- Diversify your riskier holdings so less is at risk with any particular brokerage or crypto wallet.
- Avoid maintaining a permanent link between riskier crypto brokerage accounts and traditional bank accounts.
- If you receive notice of unusual activity on an account, do not wait to place a hold on any future transactions based on fraud.
- If anything unusual seems to be happening with your account, do not authorize any transactions—period. Many times, fraudsters say that money must be transferred in and out, or to a third party, to resolve the problem with potential fraud. Almost always, those transfers enable the fraud.
- Perfect your rights with your crypto brokerage or financial institution. Usually, for a claim to be subject to proper investigation by your brokerage, a formal complaint is required. The investor needs to figure out whether that is required and how to do it, and quickly.

Anecdotally, as a lawyer that represents victims of financial fraud, my practice has seen a strong increase in victims seeking assistance related to their hacked crypto accounts recently. This may be just the beginning.

Aaron Cohn *is a partner with Weinberg Wheeler Hudgins Gunn & Dial. His practice focuses on business, investment, and commercial disputes. Cohn may be contacted at acohn@wwhgd.com or 305-455-9133.*