PRACTICE FOCUS / BUSINESS

Victim of Crypto Fraud? A Forensic Accountant May be Able to Help

Commentary by Stanley Foodman

Investors in the crypto space ought to be aware that crypto fraud exists in the crypto space the same way it exists and takes place in the traditional fiat space. Crypto investors have lost crypto currency as a result of criminal activities that include theft, scams, misappropriation and insider fraud. If you are a victim of crypto fraud, you may need a forensic accountant to assist you in the recovery of cryptocurrency assets.


Foodman

Crypto investment scams can occur in different ways and present deceptive promises and guarantees. Investors need to understand that although a crypto investment website may look legitimate and may include an endorsement of a "celebrity," once the investment is made and the money is out the door, the investor may not be able to recoup his money.

Examples of crypto fraud activities that a forensic accountant is trained to recognize:

• Investment Schemes: a fraudster will solicit funds by promising a high return on a cryptocurrency such as Bitcoin

• Embezzlement: the perpetrator will create a "fake account" on an exchange and falsely "credit the account" with fiat amounts that are non-existent. In turn, the perpetrator will purchase "real crypto currency" from customers on an exchange that are then not able to access their accounts because they lack the password.

• Phishing: the attacker will attract its victim into sending cryptocurrency payments. These payments settle immediately and are not reversible. The attacker will use the information to blackmail or phish to extort cryptocurrency payments.

• SIM Swapping: the criminal will impersonate a mobile carrier customer to switch the victim's phone number to a fraudulent SIM card gaining the access to the victim's cryptocurrency accounts.

• Crypto mining Malware: the cybercriminal will install malicious code on the devices of individuals or organizations. The malicious codes include processing power to generate cryptocurrencies through mining. The cybercriminals then transfer the newly mined cryptocurrencies to wallets that they control.

• Ransomware: the hackers install malicious software that takes control of the victim's digital device(s) and holds it hostage until the victims pays the hacker in Bitcoin to get the access back.

• Exchange Hacks: the criminals hide the unlawfully acquired cryptocurrency in other exchanges and subsequently convert it into fiat currency.

Forensic accountants can utilize traditional "follow the money" investigative tools, but with additional challenges when cryptocurrency is involved.

The forensic accountant is tasked with tracing the illicit crypto transaction in order to facilitate a recovery of potential criminal proceeds. They have to search for the evidence to explain what happened to the cryptocurrency, identify its proceeds, and the parties that have either handled or received the cryptocurrency or its proceeds.

BOARD OF CONTRIBUTORS

Here is what the forensic accountant brings to the table when "following crypto":

• A specialized understanding and expertise of what the "cryptocurrency value" is when it is exchanged in a transaction.

• A realization that Financial Institutions like banks and brokerage houses lack internal controls and strategies for cryptocurrencies.

• Cryptocurrency fraud can turn into a complex international issue given that the cryptocurrency can be transacted in "international high-risk locations" where financial controls are nonexistent.

• The flow of cryptocurrency funds in the banking system can move quickly in and out, making the "source of funds" challenging to identify

• Very often, there is difficulty in determining who the crypto wallet provider is, who the payer is, the identity of the transaction and who the beneficial owner is. Consequently, a forensic accountant must apply "advanced investigative tools" in order to capture information on senders/recipients.

• Full recovery of cryptocurrency fraud is difficult to achieve. The recovery champion is the IRS Criminal Investigation's Cyber Crime Unit which seized $3.5B in cryptocurrency according to the IRS-CI 2021 annual report.

• Cyber criminals like to darken, obscure and baffle cryptocurrency transaction details in order to "launder the cryptocurrency assets". Meaning, initiating transactions between different cryptocurrencies, or mixing cryptocurrency wallets and re-creating transactions of the same value which are basically impossible to trace.

KNOW THIS:

• A cryptocurrency transaction can not be disrupted or prevented once it is initiated.

• When the cryptocurrency resides in a "wallet," it can only be accessed with a unique private key. Know your passwords!

• Not all crypto transactions are private. There are crypto transactions that are publicly available.

• There is no regulatory agency that oversees crypto. You are on your own.

• Cryptocurrency can be anywhere (probate and divorce proceedings, bribery and corruption, asset misappropriation, money laundering, and tax evasion), so there is a need for looking beyond the numbers.

• Beware of charity organizations or individuals requesting donations for "charity."

• If cryptocurrency assets can be traced, then there is a probability that they may be recovered.

DO THIS:

• Do your research before investing in crypto.

• Be aware that "if it sounds too good to be true, it probably is!"

• Tweets, texts, emails, or any other message from social media from that tells you to pay with cryptocurrency is a scam.

• If you are donating funds by using cryptocurrency, make sure that the wallet address is legitimate.

• If you are a victim of crypto fraud, consider the assistance of a crypto experienced forensic accountant.

Stanley Foodman is president and CEO of Foodman CPAs & Advisors in Miami.