Bitcoin/Crypto Currency

In the October 2014 issue off The Atlantic Magazine, I was asked the question, "What is the greatest scam?" My response was as follows: "Bitcoin will make you the target of hackers who will steal your money. More expensive than other forms of payment, Bitcoin is a way to rob people of their life savings. Most important, if something goes wrong, the money may never be recovered."

PT Barnum is notoriously attributed to having said, "There's a sucker born every minute." He was right. It is human nature to be vulnerable to believing the unbelievable. Mr. Barnum eventually went bankrupt by over-extending his entrepreneurial activities. Unfortunately, today "suckers" are easily found every day in the Crypto world. And, for every one of those "suckers," there is a scam artist ready and willing to help that "sucker" part with his/her money or crypto currency.

The crypto currency world is both a legitimate world and a conman's playground. To most people the Crypto world is a mystery. To others it is a magical financial alternative world full of opportunity to invest and make quick money. After all, "everyone's doing it and becoming millionaires!" To the con man, it is a new world full of creative technological challenges and opportunities to re-invent PT Barnum and part naïve investors from their money. The Crypto world has become a very high-stakes enterprise, with large numbers of victims.

The recent collapse of the FTX enterprise resulted in billions of dollars in investments lost by people of every level. FTX received world-wide publicity because of the scale. But, every day there are "normal people" who become victims of scammers in the Crypto world. According to the FTC, in 2021 there was over $1B in crypto fraud/scams; real people suffered devastating losses. In most cases these losses are not recoverable. In the Crypto world, the saying is, "Once it is gone, it is gone forever."

There is a new industry growing, that attempts to recover those losses and to hold 'intermediaries' accountable. The government(s) is concerned with this new "Wild West" financial world. But until more control is imposed, the scammers will continue to develop more and more sophisticated systems to steal your last dollar.

No one sets out to be "taken" by a fraudster, but people become blinded by the gold, the dream, the excitement, for many different reasons. The scammer knows this too, and intends to use you to reach his/her goals—not yours. Below, I set forth some "Red Flags" that you might consider and heed, red flags that you can recognize if you look objectively.

- Foremost – If you do not personally know the person very well, do not invest with them or act upon their suggestions, or even use a platform they recommend. People meet in various ways; social media, work, friend of a friend, at a bar, etc. The most common way to get scammed is via someone you meet on social media. If you do not really know the person, find out everything about them before you invest. There are many ways to research: Do they have a LinkedIn account? A Facebook account? (Scammers may use fake accounts.) Ask for a physical address, a phone number, and check both out. Ask friends you DO trust; find mutual friends; use sites like "BeenVerified" or "Truthfinder" or "Intelius." If anyone that only wants to communicate with you via Internet (WhatsApp, Text, Telegram, etc.), run away! Never give or send your money to any investment until you check out the people. Do NOT invest from an Email invitation or from a phone call you did not originate. Never invest with anyone you meet on one of the 'romance websites,' chat sites; etc. Ask detailed questions of the person about their background, work history, and investing experience. Check everything thoroughly. Ask them to explain crypto investing and their theory about investing, etc. Get a sense of their legitimacy. But be aware; scammers are very polished and know what to say to gain your trust.
- Check out the Platform being recommended to use. Scammers will recommend, suggest or even cajole you into using their 'special platform.'

Do as much research as you can on Google or other public 'fraud' check websites. For example, one site was recommended – "DooCoin," which was said to be an 'invitation only' private investment firm site. It isn't. Research it – ask their customer service contact about it. Ask where the site is located, its address, phone number, how long it has been in existence, how many members/users, transaction volume, rules for investing/sending money, rules for withdrawing, is it registered with the country's finance agency, etc.

  - Some of the scams while investing with fraudulent sides include: (1) Asking you to invest to certain levels and you will be given special promotions (free money, etc.) (2) You are only able to wire money to the platform. (3) When you want to withdraw money they tell you that you must pay taxes TO THEM on your gains before you can withdraw money. (4) The entity is regulated by agencies or entities that you don't recognize and/or cannot confirm actually exist. (5) They claim that if you do not add more money you will be penalized in some way. (6) You have to pay additional money (to them, for ANY reason) before you can withdraw your money. If it sounds strange, it probably is a scam.
  - If you have any doubts about the platform, check with your bank or accountant or any reputable investment firm to see if they have information. (There also are on-line websites that keep a running list of fraudulent or suspicious platforms and websites.) If the person you are dealing with tries to reassure you or persuade you not to check it out—Run away!—at least until you check it out and confirm it is legitimate. If the platform is located in the Far East or Africa, I recommend extensive due diligence before investing.

- Investing money. Most sites have a method of adding money to your site's wallet. The site's customer service will instruct you how to do that, if it is not clear. Some fraudulent sites provide you directions on where/how to wire money to them. It is usually through an intermediary—a recipient at a well-known Bank. Before you wire any money research the recipient entity that is provided to you. For example, if they say wire your money to XXJ

Trading Company (who the site will claim is one of their intermediaries to transfer money to the platform and to your wallet,) RESEARCH them. In a case I am aware of, the trading platform's intermediary turned out to be a garage door repair company operating out of a run-down apartment. If they are a legitimate company, they can be found via Google and almost certainly will be registered with the state's Secretary of State office. If you cannot find them, do NOT send money. You can also have your bank check them out with the recipient's bank. Scammers use confederates as intermediaries to take your money and will 'fund' your wallet with fictitious funds (which you won't find out until you try to withdraw it) – almost like a "demo account."

- Trading. If you are "trading" or doing any kind of investing with a person you met, and at that person's direction, you always make money and never lose – it is most likely a scam. No one is that lucky. If they are, they would be in Vegas! If you're trading with someone and the person constantly pressures or cajoles you to invest more ("the more you invest the more you can make"), run away! If they keep telling you how much they made (especially in a short period,) be suspicious. If the person attempts to become more 'friendly' than you want or intended in the beginning, be suspicious. If the person's 'advice' or 'tips' for investing are coming from their "uncle" or other such relative, be suspicious – ask detailed questions about that relationship and situation.
- Withdrawing Funds. If the platform requires you to pay additional money or take any unusual action in order to withdraw funds, it is most likely a scam – and you may never see the money in your wallet/account again. If they require you to either invest or withdraw funds in a specific crypto currency, be suspicious.

Scammers are becoming more and more ingenious in developing websites and methods of "looking real" but are not. For example, Metatrader 4/5 is a reputable trading platform used by many people around the world, including on Wall Street. Scammers have developed a way to use that trading platform and manipulate it in conjunction with their own website to make it appear like

you are trading with Metatrader 4/5, but are not. Your account is actually fictitious – and your money is already gone. In one such technique, to ensure that you cannot withdraw money, the person directs you to trade in a specific way (in this particular case using currency arbitrage). That specific trade will crash, wiping out your entire account. In reality, the fraudulent platform is manipulated behind the scenes to cause a 'Pearl Harbor' attack and show that your trade crashed and either wiped out your entire account or caused a 'stop loss' forced liquidation of your account. Since your money was never there anyway, they had to make you think you don't have any money left to withdraw.

If you do invest and get scammed, there is little you can do. Keep all records, bank documents, funds sent, correspondence with the platform, etc. Any efforts to recover funds will require you present these documents. File complaints with the FBI's site – IC3.gov, or the FTC, SEC, your bank, or the intermediary's bank. There are Crypto recovery entities that attempt to get your money back, but they charge 10-15% of your pursued loss 'up-front' and a percentage of any recovery. Crypto fraud is becoming so prevalent that the FBI receives thousands of such complaints every month.

Approaching your bank to see if their fraud department can seek reimbursement is one avenue to consider. Another avenue is to approach the platform's intermediary bank to notify them in writing that they have a customer participating in a scam and/or money laundering activities. Some banks will cooperate, some will not (for a variety of reasons). Banks should place a high priority on ensuring that their customers and non-bank customers are not defrauded. They should have aggressive investigation programs that include bank account freezes, and attempts to reimburse individuals defrauded by their customers.

Remember, if you make it easy for someone to steal from you, it's unfortunate, but chances are someone will; so, don't make it easy.

12/07/2022