ADAMS & ASSOCIATES, PLC

CRIMINAL DEFENSE GROUP

Summer 2024 Newsletter

Cryptocurrency Scams in 2024

Cryptocurrency is a form of digital currency existing only electronically and stored in a digital wallet, usually protected by a password. Cryptocurrency and traditional currency are different because cryptocurrency values are constantly fluctuating, and cryptocurrency is not insured by any government.

The Federal Trade Commission (FTC) has cited three reasons why they believe cryptocurrency appeals to scammers:

1. Cryptocurrency transfers are non-reversible.
2. There is no centralized entity or bank to enforce preventative measures when suspicious or fraudulent activity begins to occur.
3. Cryptocurrency is still unfamiliar to many individuals.

Cryptocurrency scams have been a rising problem prosecutors continue to address. In 2021, the FTC reported losses at the time were sixty times greater than the reported losses in 2018. In March of 2023, the FBI released a public service announcement warning the public of a spike in cryptocurrency investment schemes. The Department of Financial Protection and Innovation's Consumer Services Office also reported a rise in crypto-related complaints in the third quarter of 2023. Breon Peace, United States Attorney for the Eastern District of New York is one of the prosecutors responding to this rise of cryptocurrency scams. He noted that, "Protection from fraud and manipulation extends to all consumers and investors, including those participating in the fast-evolving market for NFTs and other crypto assets. Our Office is committed to bringing to justice any criminal actor abusing any markets for their own gain."

The following are common cryptocurrency scams possibly implicated in charges brought by prosecutors:

Bitcoin Investment Schemes
This type of cryptocurrency scam occurs when scammers pose as "investment managers," claiming they have made extensive profits off cryptocurrency investments. These scammers falsely promise this same success for their victims and request an upfront fee from victims. The scammers steal the paid fee. Scammers may also use fake celebrity endorsements.

Rug Pull Scams
Rug pull scams involve scammers "boosting up" new projects, NFTs (non-fungible tokens), or coins to make money. Consumers invest in the projects only for the scammer to delete or lock the startup. Bitcoin purchases may not be resold due to the investment code, leaving victims with worthless investments.

In 2023, a criminal complaint was brought for such a scheme in which “Mutant Ape Planet” NFT purchasers were defrauded for $2.9 million in cryptocurrency. The purchasers “were falsely promised numerous rewards and benefits designed to increase demand for, and the value of, their newly acquired NFTs.” The “rug pull” occurred when the scammers abandoned the unfinished project and stole the invested money, leaving the investors with nothing.
Read more here.

Romance Scams
Romance scams occur when a scammer starts a long-distance and strictly online relationship with a victim to gain the victim’s trust. After the victim grows to trust the scammer, the scammer begins convincing the victim to buy or give them cryptocurrency.

A lawsuit recently brought by Google alleged the defendant used romance scams as a part of their fraudulent schemes. The complaint discusses the use of Google Voice text messages to potential victims. The scammers then formed faux romantic relationships or friendships with the message recipients to later convince them to download and invest in Google Play apps. These apps then used a Bitcoin investment scheme to steal victims’ money.

The complaint filed on 04/04/24 may be found here.

Phishing Scams
Phishing scams occur when scammers trick users into giving up login information for their accounts. Phishing schemes specific to cryptocurrency include:

- Seed phrase phishing: Phishing of this type uses false account recovery forms requiring users to enter a recovery phrase, ultimately giving scammers access to the victim’s crypto wallets.
- Ice phishing: Phishing of this type occurs when scammers use clickjacking, or clicking on a false item that seems legitimate, to obtain user tokens. it tends to occur during account transfers.

Man-in-the-Middle Attacks
Man-in-the-middle attacks occur when scammers steal sensitive information after a user accesses their cryptocurrency accounts in public. The scammer can steal such information by intercepting information sent over public Wi-Fi networks near the scammer’s network. Scammers use this intercepted information, often including passwords and wallet keys, to steal victims’ cryptocurrency.

Virtual private networks (VPNs) offer the best protection against such scammer attacks by encrypting transmitted data.

Social Media Cryptocurrency Giveaway Scams
Social media is also used as a tool in cryptocurrency scams. Social media cryptocurrency giveaway scams use social media posts or fake celebrity accounts to promote fraudulent giveaways. Users clicking on the giveaway are taken to a website offering Bitcoin if the user first goes through a verification process requiring a user payment (the scammers claim this is used to verify the account’s legitimacy). This payment is either lost by the victim or the link leads to the theft of the user’s personal information, leading to theft of the victim’s cryptocurrency.

Ponzi Scams
Ponzi schemes generally involve paying existing investors their promised returns with funds obtained from new investors. Scammers reel in new investors by promising high returns with little risk. Recent trends show the use of cryptocurrency and Bitcoin in such schemes.

Fake Cryptocurrency Exchanges
Faky cryptocurrency exchange scams falsely promise to exchange cryptocurrency for an investor’s deposit. The investor’s deposit is ultimately lost to the scammers.

Employment Offers and Fraudulent Employees
Scammers in scams such as these send out attractive job offers to victims. These victims are told to pay for work training with cryptocurrency, a payment which is then stolen.

Flash-Loan Attacks
Flash loans are short-term loans, which can last mere seconds, to facilitate token trades. Flash loans involve no credit checks and have no collateral, so scammers use such loans to manipulate pricing on another platform. The scammers here create an appearance of high demand through multiple buy-and-sell orders. Once prices increase, scammers cancel the orders, causing prices to drop. Scammers are then able to turn a profit by making purchases on another platform at this decreased price.

AI Scams
Artificial intelligence (AI) has also been employed to steal cryptocurrency. AI scams include chatbot scams, scams employing manipulated documentation, and deepfake impersonation scams. Chatbot scams use chatbots to interact with users, informing individuals of fake tokens and fraudulent investment schemes that lead to "pump-and-dump schemes," causing artificial token value inflation. AI scams that use manipulated documentation use AI to "overexaggerate[] the cryptocurrency project," especially in terms of followers, and frustrate a user's ability to decide if the token is fraudulent. Finally, deepfake impersonation scams use AI to use trustworthy celebrity faces to endorse cryptocurrency-related projects that will ultimately steal from investors.

Facing Allegations of Cryptocurrency Scams?
Adams & Associates, LLC is well-versed in defending cases involving allegations of cryptocurrency scams like those listed above, on both the State and Federal level. Should you have any questions, or need our assistance, please do not hesitate to contact us at 480 219 1366, or visit our website at www.azwhitecollarcrime.com.

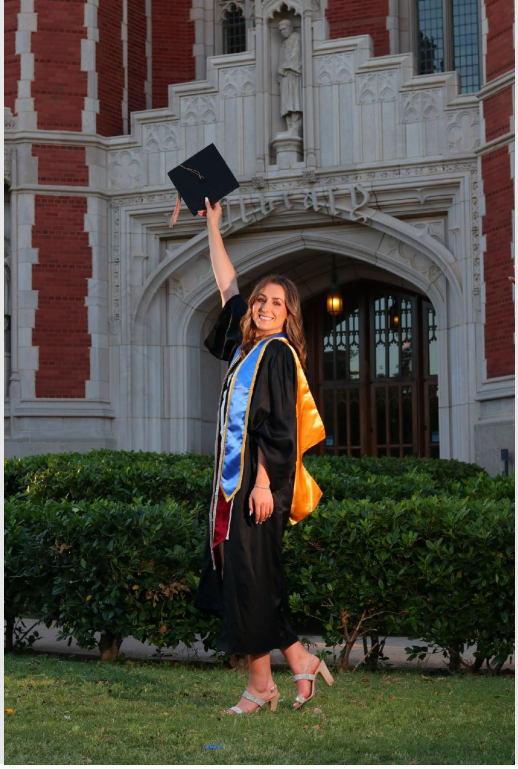
Sources:
https://www.techtarget.com/whatis/feature/Common-cryptocurrency-scams
https://fingfx.thomsonreuters.com/gfx/legaldocs/znvnkoaebpl/GOOGLE%20CRYPTO%20SCAMMER%20LAWSUIT%20complaint.pdf
https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/06/reports-show-scammers-cashing-crypto-craze#crypto7
https://consumer.ftc.gov/articles/what-know-about-cryptocurrency-and-scams
https://sanctionscanner.com/blog/10-common-crypto-scams-and-ways-to-avoid-them-712
https://www.justice.gov/usao-edny/pr/non-fungible-token-nft-developer-charged-multi-million-dollar-international-fraud
https://www.ic3.gov/Media/Y2023/PSA230314
https://www.sec.gov/files/ia_virtualcurrencies.pdf

Congratulations to Adams & Associates!

- **Ashley Adams was named one of the Top 25 Women Attorneys in the Southwest by Super Lawyers® list. See her designation here.**
- **Chase Wortham obtained a dismissal of a disorderly conduct complaint in Cottonwood Municipal Court. Congratulations, Chase!**
- **Adams & Associates, PLC was able to get AHCCCS to lift the CAF suspensions of two health care providers who had been wrongly accused of fraud.**

Congratulations to

Madelaine Feldman, Ashley's daughter, who graduated with high honors from the University of Oklahoma in May, 2024. Boomer Sooner!



PartnersforPaiute

PLEASE DONATE TO OUR SUMMER WATER DRIVE FOR THE PAUTE NEIGHBORHOOD CENTER AT THE LINK BELOW

https://www.gofundme.com/f/help-paiute-center-provide-water-to-families?utm_source=copy_link&utm_medium=customer&utm_campaign=man_sharesheet_ft&attribution_id=sl:75ed68a8-08be-4b35-becb-1a6c0bf08cf5

OUR COMMUNITY NEEDS US!

Adams & Associates, PLC

7502 E. Monterey Way
Scottsdale, AZ 85251

Phone: (480) 219-1366
Fax: (480) 219-1451

Visit Our Website