Additional Resources

The following websites may provide additional information relating to fraud and fraud reporting.

www.ic3.gov

- Fraud types and schemes
- Report a crime

www.secretservice.gov

- Cryptocurrency Awareness Hub
    - PSA videos
    - Common definitions
    - Cyrpto in the news

www.fbi.gov

- Cybersecurity Awareness Videos
- Submit a tip/report a crime

https://consumer.ftc.gov

- What to know about cryptocurrency

https://sec.gov

- Crypto Assets and Cyber Unit

https://crypto3c.org/

- Reporting on common scams

Commodity Futures Trading Commission

- CFTC.gov/complaint

Tips to Protect Yourself from Fraud

Transactions involving digital assets can be overwhelming. Below are a few items to know to keep you and your digital assets safe from fraud.

Online Use and Wallets

- NEVER invest money you cannot afford to lose.
- Use 2-Factor Authentication (such as a password and a phrase, a fingerprint, or a confirmation text).
- Safeguard your passwords and do not repeat them or share them.
- Maintain your own private key for your digital wallet.
- Store your digital funds in a secure wallet.
- If you did not request to reset your password, do not click the link. Go directly to the website.
- If you receive a request to update information, go directly to your profile to update, do not click links you are not certain of.
- DO NOT store your recovery seed digitally. Keep it secure and in a non-electronic format.
- Read the fine print and know how to exit any investment you pursue.
- Always log out of your wallet and any sites you may have your wallet connected to.

Fraud Awareness

- If you are called and told a friend/family member needs money, HANG UP, and call the friend/family member directly to confirm.
- Do not send or receive funds from someone you do not know or on behalf of someone else.
- Beware of investment opportunities promising guaranteed returns or those sounding too good to be true.

You've been the victim of a scam, now what??

2023

Public-Private
Analytical Exchange Program

Combatting Illicit Activity Utilizing Financial Technologies and Cryptocurrencies

This program enables U.S. government analysts and private sector partners to gain a greater understanding of how their disparate, yet complimentary roles can work in tandem to ensure mission success. Participants work to create joint analytic products of interest to both the private sector and the U.S. Government.

This product was produced by AEP participants.

Where to report the fraud

In the event you, or someone you know, has become or thinks they have become the victim of a fraud, it is important to know where to go and how to report the fraud.

It is important to report fraud to the federal government; but you should also consider reporting any fraud to your local authorities such as state, county, and city police.

Prosecutors can use blockchain data analytics and traditional law enforcement techniques to identify and prosecute complex cryptocurrency investment schemes; price and market manipulation involving cryptocurrencies; unregistered cryptocurrency exchanges involved in fraud schemes; and insider trading schemes affecting cryptocurrency markets.

The Federal Bureau of Investigation (FBI) along with Internet Crime Complaint Center (IC3) lead in federal cyber frauds and crimes related investigations. IC3 review and research complaints, and send the information to federal, state, local, or international law enforcement agencies for possible criminal or civil action.

Below is a list of federal agencies where you can report a suspected fraud. Please see the reverse of this pamphlet for their website addresses.

- Federal Agencies
    - ♦ United States Secret Service
    - ♦ Federal Bureau of Investigation
    - ♦ Federal Trade Commission
    - ♦ United States Securities and Exchange Commission
    - ♦ Commodity Futures Trading Commission

How and why to report a fraud

In the event of a fraud, the two most important elements are 1) reporting the fraud and 2) preserving the data. The flowing tips will help you learn how to accurately preserve the data of the fraud.

<u>Why Should You Report</u>

Join the fight against internet crime! By reporting internet crimes, you are making difference by:

- Bringing criminals to justice
- Making our communities safer, both locally and nationally
- Helping law enforcement track trends and threats
- In some cases, even freeze stolen funds.
- With your help, we can and will respond faster, defend cyber networks better, and more effectively protect our nation .

<u>How to Store Evidence</u>

It is important that you keep any evidence you may have related to your complaint in a safe location in the event you are requested to provide them for investigative or prosecutive evidence.

Be sure to think outside of the box. Evidence can come in many forms and may be physical and digital. Below are some questions that may help you identify sources of evidence.

- Who have you interacted with? What was their name, title, or position?
- How did you interact with them? Was it on a website, social media, group chat, email, text message, phone call, or elsewhere?
- How did you exchange funds? Do you have receipts, cancelled checks, envelopes, prepaid cards?

Save any correspondence such as brochures and pamphlets, web page archives, emails, and other artifacts.

Web pages that are relevant to the scam can be archived in several ways. Services like Archive.org's Wayback Machine can be used to preserve website content.

There are specific attributes to cryptocurrency transactions that are important to record: transaction IDs, where you sent your crypto from (the address of your private wallet, account at a crypto exchange, etc.), and where you believe you were sending your funds (address and purported use).

<u>Important: Cryptocurrency identifiers may be Case Sensitive, for example (bc1qWNx is not the same as bc1wnx...).</u>

What happens next

When a crime is reported, it is natural to wonder what happens next. The below are possible next steps after reporting a fraud.

- FBI/IC3
    - Can rapidly deploy investigative teams located nationally and can provide technical assistance.
- United States Secret Service (USSS)
    - The nearest field office will assesses and activate law enforcement officers as needed.
- Department of Homeland Security (DHS)
    - The department's National Cybersecurity and Communications Center (NCCIC) assists owners in helping find weak spots, other who may be at risk, and share information with other public or private sectors.
- National Cyber Investigative Joint Task Force (NCIJTF)
    - Works together and shares information with other Law Enforcement agencies across the U.S. Government to protect people and put cyber criminals behind bars.
- Fusion Centers
    - Fusion centers share information and pass information between the federal, state, local, and private sectors. They can quickly share and provide information related to threats. A fusion Center can also help ensure common cyber policies, programs, and response plans to address known and possible threats, help exchange subject-matter expertise and help law enforcement and prosecution efforts.