# Steps For Fraud / Scam Victims

## Purpose

The purpose of this document is to assist individuals who have been involved with or victimized by a scam or an incident(s) of fraud. This document is intended to be used by victims to help them protect their identities, protect their assets, report their fraudulent encounters and further educate themselves and others against common frauds and scams.

## Resources

*The information in this document is based on information published by the Commodity Futures Trading Commission, the Federal Trade Commission, the Federal Bureau of Investigation, and the Consumer Financial Protection Bureau, including, but not limited to, the following documents and webpages: "6 Steps To Take after Discovering Fraud," available at https://www.cftc.gov/LearnAndProtect/AdvisoriesAndArticles/6Steps.html, and "What To Do if You Were Scammed" available at https://consumer.ftc.gov/articles/what-do-if-you-were-scammed, and "Common Frauds and Scams," available at https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams, and "When Information is Lost or Exposed" available at https://www.identitytheft.gov/Info-Lost-or-Stolen, and "The Latest in Consumer Advise" available at,* https://consumer.ftc.gov/, *and "Protect Your Personal information and Data" available at https://consumer.ftc.gov/articles/protect-your-personal-information-and-data, and "How to Avoid a Scam" available at https://consumer.ftc.gov/articles/how-avoid-scam#signs, and "What to Know About Credit Freezes and Fraud Alerts" available at https://consumer.ftc.gov/articles/what-know-about-credit-freezes-and-fraud-alerts#alerts, and "What does it mean to put a security freeze on my credit report" available at https://www.consumerfinance.gov/ask-cfpb/what-does-it-mean-to-put-a-security-freeze-on-my-credit-report-en-1341/.*

## What is Fraud

Fraud typically involves stealing information, such as bank account or credit card numbers, without the victim's knowledge. Fraudsters rely on illegal access.

## What is a Scam

Scams are typically designed to manipulate a victim into willingly providing their information. Scammers rely on psychological manipulation.

# Steps For Fraud / Scam Victims

## Step 1
## Don't Pay Any More Money

- Be on the lookout for **recovery frauds**. These frauds target recent victims and claim to be able to get the stolen money back if the victims first pay an upfront fee, "donation," retainer, or back taxes.

- Click here (recovery frauds) or visit the Commodity Futures Trading Commission's website at https://www.cftc.gov/LearnAndProtect to learn more about recovery frauds.

# Steps For Fraud / Scam Victims

## Step 2
## Collect All the Pertinent Information and Documents Related to The Incident

- Develop a timeline and collect documents and information related to the fraud/scam. Write down conversations you had with the scammers. Document all dates, times and locations.

- Collect and keep the below listed documents and information.
  - ☐ Names, titles, identities, identifying characteristics, accents, physical descriptions or positions used by the fraudsters.
  - ☐ Details about the fraud/scam (what was discovered and or promised).
  - ☐ Dates and times of interactions.
  - ☐ Copies of all communications (emails, texts, voicemails, social media).
  - ☐ Social media/online profiles, accounts, usernames, group posts, chats, or other online interactions.
  - ☐ Website addresses and screenshots.
  - ☐ Emails and email addresses (including full header information).
  - ☐ Phone numbers used or provided by the fraudsters.
  - ☐ Account information, statements, trade confirmations, disclosures, and sales materials.
  - ☐ Credit card receipts, statements and numbers.
  - ☐ Debit card or bank account receipts, statements and numbers
  - ☐ Exchanges of digital crypto currencies, such as Bitcoin.
    - Transaction (hash) IDs (Example: 8b8729a4e1e54ade3b9657922ea20af427d8dd6c41c96f503e1ad6d80cdc598a)
    - Cryptocurrency Addresses (Example:18cBEMRxXHqzWWCxZNtU91F5sbUNKhL5PX)
    - QR codes (with or without cryptocurrency icons), papers with "wallet" listed
    - Receipts from cryptocurrency ATM transactions (Example: BitcoinDepot)
    - Cryptocurrency websites, bookmarks, applications (Example: coinbase.com)
  - ☐ Records of other forms of payment including cancelled checks or receipts for wire transfers, money orders, or prepaid cards.
  - ☐ Any correspondence received, including envelopes.
  - ☐ Description of vehicle used by fraudsters.
  - ☐ Picture/video surveillance of fraudsters.

# Steps For Fraud / Scam Victims

## Step 3
## Protect Your Identity and Accounts

If you provided personal information or payment information to the fraudsters, take the following steps necessary to block access to your accounts, protect your reputation, and protect against identity theft.

- **Credit Card**
  - If you used credit card information in a fraudulent transaction, or gave someone your credit card information, contact your card issuers immediately to file a fraud report. As part of the process, you may be required to get a new account number.
  - Consider contacting one of the three national credit reporting companies (**Equifax, Experian, Transunion**) and ask that it place a Fraud Alert on your credit file.
    - Click here to learn more about a fraud alert
  - Consider contacting all three of the national credit reporting companies (**Equifax, Experian, Transunion**) to request a security freeze, also referred to as a credit freeze.
    - Click here to learn more about a free security freeze.
- **Debit Card or Bank Account**
  - If you gave the fraudster your debit card number, bank account number or routing number, contact your bank or credit union immediately. You may need to close the account and open a new one.
- **Gift Cards**
  - Payments made with gift cards are typically not reversible. If you paid the fraudster using a gift card, contact the company that issued the gift card. Tell them it was used in a scam and ask them to refund your money. Keep the gift card itself, and the gift card receipt.
  - Look for the company's contact information on the card itself or research online to find out how to reach the card issuer.

# Steps For Fraud / Scam Victims

- **Wire Transfer (E.g. Western Union or MoneyGram)**

    - If you paid the fraudster via a wire transfer, contact the wire transfer company **right away**. Tell them it was a fraudulent transfer. Ask them to reverse the wire transfer and give you your money back. Payments made via wire transfer are typically not reversible.

- **Cryptocurrency**

    - If toy paid the fraudster using cryptocurrency, contact the company you used to send the money and tell them it was a fraudulent transaction. Ask them to reverse the transaction, if possible. Cryptocurrency payments are typically not reversible. Oftentimes you can only get your money back if the person you paid sends it back to you.

- **Cash**

    - If you sent the fraudster cash by U.S. mail, contact the U.S. Postal Inspection Service at 877-876-2455 and ask them to intercept the package.
    - Visit the United States Postal Service's website at https://www.usps.com/ to learn more about this process.
    - If you used another delivery service, contact them as soon as possible.

- **Sextortion/Financial Sextortion**

    - If you sent the fraudster sexually explicit material of yourself or the fraudster claims to already have explicit material (nude picture or video) and threatens to share said material if you do not send more pictures or money, contact the Federal Bureau of Investigation (FBI) at 1-800-CALLFBI (1-800-225-5324) or file a report online with the FBI at tips.fbi.gov.

        - If you are not ready to file a report with the FBI, go to a trusted friend/family member. Tell them you are being victimized and need help.

    - Visit https://takeitdown.ncmec.org/ if you are under the age of 18 years old.
        - Take It Down is a free service that can help you remove or stop the online sharing of nude, partially nude, or sexually explicit images or videos taken of you when you were under 18 years old.

    - Visit https://stopncii.org/ if you are over the age of 18 years old.
        - StopNCII.org is a free tool designed to support victims of Non-Consensual Intimate Image (NCII) abuse.

# Steps For Fraud / Scam Victims

- **Usernames, Logins and Passwords.**
  - If you gave the scammer your username and password or registered for access to a fraudster's website using usernames or passwords that you use elsewhere, be sure to update accounts with new logins as soon as possible.

- **Computer or Phone Number**
  - If you gave the scammer remote access to your computer:
    - Update your computer's security software, run a scan, and delete anything it identifies as a problem. Then take other steps to protect your personal information.
    - Chick here (protect your personal information) or visit the Federal Trade Commission's Consumer Advise website at https://consumer.ftc.gov/ for information on how to protect your personal information.
  - If the scammer took control of your cellphone number or account:
    - Contact your service provider to take back control of your phone number. Once you do, change your account password.

- **Social Security Number**
  - If you gave the scammer your social security number or someone used your Social Security number to make purchases or open accounts:
  - Consider contacting one of the three national credit reporting companies (Equifax, Experian, Transunion) and ask that it place a Fraud Alert on your credit file.
    - Click here to learn more about a fraud alert
  - Consider contacting all three of the national credit reporting companies (Equifax, Experian, Transunion) to request a security freeze, also referred to as a credit freeze.
    - Click here to learn more about a free security freeze.
  - Report your information stolen at the Federal Trade Commission's (FTC's) website.
    - Click here (https://www.identitytheft.gov/) to access the Federal Trade Commission's Identity Theft website.

# Steps For Fraud / Scam Victims

## Step 4
## Report The Fraud/Scam to The Authorities

Notifying local, state and federal authorities will help agencies track incidents of fraud and scams, pursue the involved parties, and warn others.

- File a report with your local police department

- File a report with the Federal Trade Commission (FTC) at https://reportfraud.ftc.gov/

  - ReportFraud.ftc.gov is the federal government's website where you can report fraud, scams, and bad business practices.

  - The FTC uses the reports that are submitted to them to investigate and bring cases against fraudsters, scammers, and bad business practices.

- File a report with the Federal Bureau of Investigation's (FBI's) Internet Crime Complaint Center (IC3) at https://www.ic3.gov

  - The Internet Crime Complaint Center (IC3) is the central hub for reporting cyber-enabled crime. It is run by the FBI, the lead federal agency for investigating crime.

If Identity Theft related:

- File an identity theft report with the Federal Trade Commission (FTC) at https://www.identitytheft.gov/

  - IdentityTheft.gov is the federal government's one-stop resource for identity theft victims. The site provides streamlined checklists and sample letters to guide you through the recovery process.

Victims aged 60 or older

- This National Elder Fraud Hotline is a free resource created by the U.S. Department of Justice (DOJ), Office for Victims of Crime for people to report fraud against anyone age 60 or older.

  - The number for the National Elder Fraud Hotline is 833–372–8311

# Steps For Fraud / Scam Victims

## Step 5
## Check Your Insurance Coverage and Other Financial Recovery Steps

- **Fraud theft insurance.** Check your homeowner's policy to see if it includes coverage for fraud losses or reimbursements for identity theft related expenses.

- **Consider consulting a tax professional.** If you can itemize deductions on your personal income tax return, fraud losses may be deductible in the year the fraud was discovered.

- **Consult a financial counselor or advisor.** Losses to retirement savings that caused significant debt may require the help of a professional financial advisor.

- Beware of credit repair companies that promise to significantly erase your debt.

    - Click here (credit repair companies) or visit the Consumer Financial Protection Bureau's website at https://www.consumerfinance.gov/ to learn more about credit repair scams and credit repair companies.

# Steps For Fraud / Scam Victims

## Step 6
## Consider Changing Behaviors and Building Your Resistance to Fraud

Don't blame yourself for being victimized. Fraudsters and scammers are very good at what they do, and they often target educated and successful people. However, you may want to consider the events or actions that led up to the fraud. Many times, routine activities can lead people into becoming targets, and returning to those activities could start the process over again.

Visit the Federal Trade Commission's Consumer Advise website at https://consumer.ftc.gov/ for more information about unwanted calls, emails and text messages, identify theft, online security, commons signs of scams, how to avoid scams and what to do if you were scammed.

Click here (https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams) or visit the Federal Bureau of Investigation's website at https://www.fbi.gov/ (select the "How We Can Help You" tab) to learn more about some of the most common frauds and scams that the Federal Bureau of Investigation encounters.