

Steps To Take After A Scam

STOP CONTACT WITH THE SCAMMER. Hang up the phone. Do not reply to emails, messages, or letters that the scammer sends. Do not make any more payments to the scammer. Beware of additional scammers who may contact you claiming they can help you get your lost money back.

SECURE YOUR FINANCES.

- Report potentially compromised bank account, credit or debit card information to your financial institution(s) immediately. They may be able to cancel or reverse fraudulent transactions.
- Notify the three major credit bureaus. They can add a fraud alert to warn potential credit grantors that you may be a victim of identity theft. You may also want to consider placing a free security freeze on your credit report. Doing so prevents lenders and others from accessing your credit report entirely, which will prevent them from extending credit:
 - **Equifax**
 - <https://www.equifax.com/personal/credit-report-services/>
 - (800) 525-6285
 - **Experian**
 - <https://www.experian.com/fraud/center.html#content-01>
 - (888) 397-3742
 - **TransUnion**
 - <https://fraud.transunion.com/fa/fraudAlert/landingPae.jsp>
 - (800) 680 -7289

CHECK YOUR COMPUTER. If your computer was accessed or otherwise affected by a scam, check to make sure that your anti-virus is up-to-date and running and that your system is free of malware and keylogging software. You may also need to seek the help of a computer repair company. Consider utilizing the Better Business Bureau's website to find a reputable company.

CHANGE YOUR ACCOUNT PASSWORDS. Update your bank, credit card, social media, and email account passwords to try to limit further unauthorized access. Make sure to choose strong passwords when changing account passwords.

REPORT THE SCAM. Reporting helps protect others. While agencies can't always track down perpetrators of crimes against scammers, they can utilize the information gathered to record patterns of abuse which may lead to action being taken against a company or industry.

Report your issue to the following agencies based on the nature of the scam:

- **Local Law Enforcement:** Consumers are encouraged to report scams to their local police department or sheriff's office, especially if you lost money or property or had your identity compromised.
- **Federal Trade Commission:** Contact the Federal Trade Commission (FTC) at 1-877-FTC-HELP (1-877-382-4357) or use the Online Complaint Assistant to report various types of fraud, including counterfeit checks, lottery or sweepstakes scams, and more.
- **Identitytheft.gov:** If someone is using your personal information to open new accounts, make purchases, or get a tax refund, report it at www.identitytheft.gov. This federal government site will also help you create your Identity Theft Report and a personal recovery plan based on your situation. Questions can be directed to 877-ID THEFT.
- **The Social Security Administration (SSA):** If your social security number was exposed, you will need to contact the Social Security Administration by calling 1-800-772-1213. Another suggestion is to create a "my Social Security" account if you haven't already.
- **Better Business Bureau (BBB):** Reporting to the BBB Scam Tracker can help others become aware of scams that may be circulating in your local area.