WHAT TO DO IF YOU BELIEVE YOU WERE SCAMMED: RESOURCES FOR SCAM VICTIMS

IMMEDIATE ACTIONS TO PROTECT YOURSELF

Did you make a payment through your financial institution?

Contact your institution and notify them that you may be the victim of a scam. In addition to stopping payments made to the criminal, your institution may be able to help recover stolen funds and provide guidance on reporting the scam to law enforcement.

Did you provide personal information or account login credentials?

Notify your financial institution that you provided your account login credentials to a potential criminal. Your financial institution can help you identify any unauthorized transactions that may have occurred, notify you of any recent suspicious account activity, and advise on other actions to help protect your identity and accounts — e.g., freezing your accounts, changing your passwords, personal identification numbers (PINs) or other login credentials.

Consult IdentityTheft.gov. This federal government-run website provides numerous resources for identity theft victims and those at risk, including guidance on how to create and implement a personal recovery plan.

Did you provide access to your device?

Investigate whether malware was installed on your device. Your data and identity could be at risk if you clicked on a link or provided remote access to your device. You can scan your device to detect the presence of malware or viruses. If detected, notify your financial institution that your account may be at risk and consult **IdentityTheft.gov.**

PROTECTING FUTURE VICTIMS: THE IMPORTANCE OF REPORTING

Sharing the details of what happened with local law enforcement, the Federal Trade Commission (FTC) and Federal Bureau of Investigation (FBI) can make investigation of scam cases more effective. Furthermore, reporting to these organizations and local law enforcement can offer insights into current scam trends and threats, providing a foundation for better education and resources to help protect the public.

- **File a police report with local law enforcement.** Local law enforcement can investigate what happened to you and potentially, assist in recovery of stolen funds.
- **Report the incident to the FTC:** The FTC maintains a centralized repository of reports, which is available to law enforcement agencies and other industry partners to help launch investigations and analyze current fraud trends.
- **File a complaint with the FBI Internet Crime Complaint Center (IC3):** IC3 shares fraud and scams reports with the FBI's network of field offices and other law enforcement agencies.

WHAT TO DO IF YOU BELIEVE YOU WERE SCAMMED: RESOURCES FOR SCAM VICTIMS

Some examples of resources that can help guide individuals through reporting:

- **AARP Fraud Watch Network Hotline:** Staffed by trained volunteers, callers are guided through the reporting process and referred to law enforcement.
- **National Elder Fraud Hotline:** Run by the Department of Justice's Office for Victims of Crime, this hotline assigns case managers who assist victims in fraud reporting and provide other resources to victims as needed.

Victims of scams may face both devastating financial losses and emotional distress. Here are just a few resources available for those seeking mental health support and recovery:

- **AARP Fraud Victim Support Group**
- **Romance Scam Recovery Group** — led by **FightCybercrime.org**
- **It's Not Your Fault: Empowerment After Financial Fraud** — FINRA Investor Education Foundation
- **Scam Survival Toolkit** — Better Business Bureau

The scams mitigation toolkit was developed by the Federal Reserve to help educate the industry about scams and outline potential ways to help detect and mitigate this fraud type. Insights for this toolkit were provided through interviews with industry experts, publicly available research, and team member expertise. This toolkit is not intended to result in any regulatory or reporting requirements, imply any liabilities for fraud loss, or confer any legal status, legal definitions, or legal rights or responsibilities. While use of this toolkit throughout the industry is encouraged, utilization of the toolkit is voluntary at the discretion of each individual entity. Absent written consent, this toolkit may not be used in a manner that suggests the Federal Reserve endorses a third-party product or service.