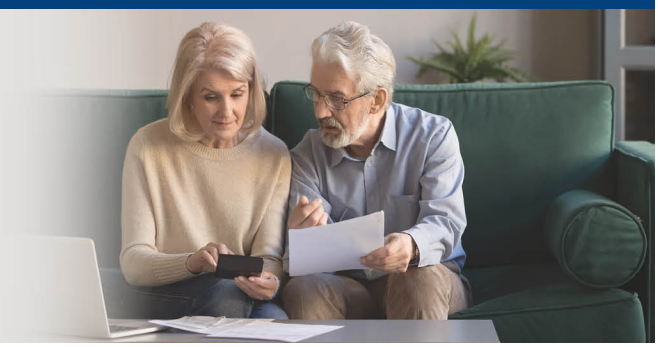
YOU'VE BEEN SCAMMED — Now What?



The sooner you act, the better you can protect yourself. The following steps can help you guard against further theft, report the fraud, and start the recovery process. *These are for informational and educational purposes only and should not be considered legal or investment advice or a comprehensive list of solutions.*

Take Action NOW! All of Your Accounts Are at Risk — Not Just Your Financial Ones.

REVIEW AND SECURE YOUR EMAIL ACCOUNT(S)

Fraudsters often compromise individuals by first gaining access to their email by sending them phishing emails with malicious links or attachments. If you click on the link or open the attachment, the malicious code gives the fraudsters access to your email and all its content. It can also allow them to send and receive emails from your email account.

- ☐ Change your email password to something new and unique.
- ☐ Be sure to enable any multifactor authentication capabilities associated with your email account.
- ☐ Check your sent and deleted emails to ensure there are no emails that you didn't send or delete.
- ☐ Check to ensure no email folders have been created.
- ☐ Check to ensure there are no auto forward rules set that are sending incoming emails to another (fraudster's) email address.
- ☐ Check to ensure no autoreplies have been established.

ENSURE YOUR PERSONAL COMPUTER'S ANTIVIRUS, OPERATING SYSTEM, AND BROWSER VERSIONS ARE CURRENT

- ☐ Run antivirus software to check for spyware, keyloggers, and other types of malware.

REVIEW AND SECURE ALL YOUR ONLINE ACCOUNTS (NOT JUST THE COMPROMISED ACCOUNTS)

- ☐ Review all your accounts and ensure no unauthorized changes or transactions have been made.
- ☐ Ensure your contact information including your address, phone number, email address, and bank account information are correct.
- ☐ Ensure your bank balances are accurate and any past transaction activity was authorized.
- ☐ Change passwords, PINS, and usernames (if possible) ensuring the same passwords or usernames are not used more than once and none have been reused.
- ☐ Take advantage of all security features available, especially multi-factor authentication.

CONTACT YOUR FINANCIAL INSTITUTIONS

- ☐ Inform all the financial institutions you do business with that your identity has been compromised including insurance companies, 401(k) providers, banks, and credit card companies.
- ☐ Inquire about any additional actions that can be taken to protect your accounts including "freezes" or "holds" that can limit access or withdrawal.
- ☐ Ask for new account numbers and/or cards if available.

LIMRA LOMA
Navigate With Confidence

1013-2024

FILE A REPORT

- [ ] File a complaint with the Federal Trade Commission (FTC) at IdentityTheft.gov if you've been the victim of identity theft. They can help you report and recover from identity theft.
  - ○ Complete the FTC's online form or call (877) 438-4338. Based on the information you enter, IdentityTheft.gov will create your identity theft report and recovery plan. Note: if you create an account, IdentityTheft.gov will walk you through each recovery step, update your plan as needed, track your progress, and pre-fill forms and letters for you.
- [ ] Report the incident to your local law enforcement. Items you'll need include:
  - ○ Copy of your FTC identity theft report
  - ○ Proof of your address (mortgage statement, rental agreement, utility bill)
  - ○ Government-issued ID with photo
  - ○ Any other proof of the theft (bills, IRS notices, statements, etc.)

  Alert the police that someone stole your identity and you need to file a report.

  Ask for a copy of the police report.
- [ ] Report the incident to the FBI's Internet Crime Complaint Center (IC3) for cybercrimes.

Next Steps

Keep a log of the businesses you've contacted, their phone numbers, the people you've spoken with, and the dates of your conversations.

CLOSE NEW ACCOUNTS OPENED IN YOUR NAME: CALL THE FRAUD DEPARTMENT OF EACH BUSINESS WHERE AN ACCOUNT WAS OPENED.

- [ ] Explain that your identity was stolen.
- [ ] Request the business close the account and confirm in writing that the fraudulent account isn't yours, that you're not liable for it, and that it be removed from your credit report.
- [ ] Maintain the letter on file in case the account winds up on your credit report.

REMOVE CHARGES FROM YOUR ACCOUNT THAT WEREN'T YOURS.

- [ ] Explain that someone stole your identity, that the charges are fraudulent, and you're requesting they be removed.
- [ ] Ask for a letter confirming they've removed the charges and keep the letter on file in case the account winds up on your credit report later.
- [ ] Correct your credit report: If someone steals your identity, you have the right to remove fraudulent information from your credit report. This is called blocking. Once the information is blocked, it won't show up on your credit report, and companies can't try to collect the debt from you. If you have an FTC identity theft report, credit bureaus must honor your request to block this information.
- [ ] Write to each of the three credit bureaus. Include a copy of your FTC identity theft report and proof of your identity and ask them to block fraudulent information from the report.

  Equifax.com P.O. Box 105069, Atlanta, GA 30348-5069 | **(800) 525-6285**
  Experian.com P.O. Box 9554, Allen, TX 75013 | **(888) 397-3742**
  TransUnion.com Fraud Victim Assistance Dpt. P.O. Box 2000, Chester, PA 19016 | **(800) 680-7289**

  - ○ Consider adding an extended fraud alert (this can last for 7 years) or a credit freeze (lasts until you remove it) to prevent new accounts from being opened in your name.
  - ○ Review your credit reports often by accessing AnnualCreditReport.com.