Identity Theft
Thieves steal your personal financial information and use your identity to commit fraud and other crimes. They use your Social Security Number, birth date, credit card and other account numbers, PINs and passwords.

Warning Signs of Identity Theft
Watch for unexpected transactions or communications that could indicate your identity has been stolen. Warning signs include:

- Seeing withdrawals from your bank account that you didn’t make.
- Missing bills and statements.
- Stores refusing your checks.
- Credit card transactions that don’t go through.
- Letters about accounts you didn’t open.
- Emails about purchases you didn’t make.
- Statements for credit cards you don’t have.
- Debt collectors calling about debts that aren’t yours.
- Passwords or usernames that suddenly don’t work.
- Unfamiliar accounts on your credit reports.
- Medical bills for services you didn’t receive.
- Health records for conditions you don’t have.
- The Internal Revenue Service (IRS) tells you that more than one tax return was filed in your name. If you have income from somewhere you never worked.
- Notification about a data breach.
Steps to Minimize Identity Theft

- **Guard your personal information closely.** If someone asks for your Social Security number or other personal information, ask why they need it. Ask how it will be used, how they will protect it, and what happens if you don’t share it.
- **Don’t respond to unsolicited requests.** They may be text messages, emails, or phone calls asking you for sensitive information.
- **Protect your mail.** Your mail is often an easy target for an identity thief because you receive and send personal information that way.
- **Sign up for direct deposit.** This gives thieves less access to your information if paychecks and checks for public benefits do not go through the mail.
- **Clean up your financial trash.** Destroy all pieces of paper with your personal information before recycling them.
- **Review your financial accounts regularly and carefully.** Contact your bank if there is a difference in your records.
- **Beware of identity theft on the Internet.** Be cautious about giving bank account or other personal information online.
- **Protect your devices, such as computers, phones, and tablets.** Find more information on staying safe online at [www.OnGuardOnline.gov](http://www.onguardonline.gov).
- **Review your credit reports at least once every 12 months.** Carefully check your credit reports for activity you don’t recognize. You can request a copy at [www.annualcreditreport.com](http://www.annualcreditreport.com). It does not affect your credit scores.
- **Keep your important documents secure.** This applies to both paper and electronic documents.
- **Beware of disaster-related scams.** Con artists take advantage of people after disasters. They claim to be from legitimate charitable organizations.

**Reporting Identity Theft and Getting Help**

Create an Identity Theft Report with the FTC if your identity has been stolen. It proves to businesses that someone stole your identity. The report makes it easier to correct problems caused. You contact credit reporting agencies to place a fraud alert on your reports.

- **Experian:** [www.experian.com/fraudalert](http://www.experian.com/fraudalert), 1-888-397-3742
- **TransUnion:** [www.transunion.com/fraud](http://www.transunion.com/fraud), 1-800-680-7289
- **Equifax:** [www.equifax.com/creditreportassistance](http://www.equifax.com/creditreportassistance), 1-888-766-0008

You can also place a freeze on your credit report. A freeze makes it less likely an identity theft can open a new account in your name. To learn more visit FTC website at [https://www.ftc.gov](https://www.ftc.gov) and search for "fraud alerts" and "credit freeze."

This information is an excerpt from the FDIC Money Smart for Adults Credit Reports and Scores Module. Visit the [FDIC website](https://www.fdic.gov/consumers/consumer/moneysmart/adult.html) for more information, or contact us at 1-800-257-1705 for printed materials.