ID Theft & Account Fraud: Prevention and cleanup

An identity thief is an imposter who assumes another person's identity to profit illegally or because the thief wants to hide behind a new identity. Identity theft—or ID theft—occurs when the imposter uses your personal information to commit fraud or other crimes.

Account fraud occurs when someone else obtains your credit card number or bank account information and makes unauthorized charges or withdrawals.

Among the pieces of personal information that can be used to commit ID theft and fraud are your name, Social Security number (SSN), birthdate, mother's maiden name, credit report, driver's license and credit card and bank account numbers.

It pays to prevent ID theft because victims spend significant amounts of time and money to clean up their credit records. Victims may lose job and rental opportunities, be rejected for housing, car and education loans and even be arrested for another person's outstanding warrants or suspected crimes.

If you're already a victim, you need to take timely action to clear up the problems created by ID theft and account fraud and to lessen its impact on your life. *(See "ID theft cleanup" section.)*

Prevent ID theft/account fraud

Your credit

- Check your credit reports regularly. You can get free copies every 12 months at AnnualCreditReport.com (*www.annualcreditreport.com*) or by calling 877-322-8228.
- Before you discard documents and mail that contain your SSN, account numbers and other personal information, shred them or tear them into tiny bits.

Personal identification

- Don't carry your Social Security card in your wallet or purse. Memorize your SSN.
- Watch your wallet or purse at all times. At work, keep your purse in a locked drawer or cabinet. Don't hang your purse on your chair in restaurants.
- If your SSN is on your driver's license, ask to have it removed—you have that right under federal law.
- Verify that your employer keeps your SSN and other personal information under lock and key.
- Lower your voice when giving your SSN or other sensitive information in banks or doctors' offices.

Financial information

- Check financial statements and bills as soon as they arrive. Report any unauthorized transactions to the companies immediately.
- Lock your mailbox. Deposit outgoing mail containing checks in a postal box—don't leave it sitting in your unlocked mailbox or apartment lobby.
- At home, hide sensitive information like bank and credit card statements, insurance records, etc. where they can't be seen by visitors or workers.
- At teller machines (ATMs), shield the PIN keypad while entering credit and debit card passwords.

- Try to keep an eye on your credit card when you give it to a merchant or waiter.
- When you order new checks, look out for them. Make sure they are delivered to a locked mailbox.

Phone and internet

- Never respond to requests made by phone or email for your personal information, no matter how urgent the request seems. Find the legitimate contact information for the company online or in the phone directory and contact the company to verify that the request is legitimate.
- Don't provide sensitive personal information when talking on a cell phone.
- Don't give out personal information on the phone, through email or text message, or on the internet unless you've initiated the contact or you are absolutely sure you know the company or person you're dealing with.

Marketing

- Read your bank's privacy notice so that you understand how it uses your information for marketing.
- If you don't want to get preapproved credit offers, call 888-5OPT-OUT (567-8688) to stop them.
- Be careful about giving away information about yourself. Question why a business needs your SSN, mother's maiden name or other information.
- Before entering a contest or answering a survey, consider that any personal information you provide is likely to be used, shared and/or sold to third parties.

Are you already a victim?

ID theft has been called a "shadow crime" because victims can be unaware that their identities have been stolen. These steps may help you identify ID theft and account fraud:

- **Check your credit report.** You can get free annual copies of your credit reports from the three large national credit bureaus at AnnualCreditReport.com (*www.annualcreditreport.com*). Review your reports for accounts you don't recognize or information from companies you don't do business with.
- **Monitor your mail** for missed bills, credit card statements and other mail that you expected. A missing bill might mean that a crook has taken over your account and changed your billing address.
- **Investigate mysterious purchases**, charges, bills or collection calls immediately. If you receive a credit card you didn't apply for, find a strange charge on your credit card or get calls or letters from debt collectors about bills you don't recognize, call the companies immediately to address the problem.
- **Question credit rejections.** If you know you have good credit but your application for a new credit card is denied, it could signal ID theft. When you are denied credit, you can get a free copy of your credit report from the credit bureau used by the lender.

ID theft cleanup

If you discover that you are a victim of ID theft, take these steps to obtain proof of the crime and limit the damage:

Document the crime. File a report with your local police department.

- Get a copy of the police report and make a note of the incident number assigned to your complaint.
- Also contact appropriate state and federal law enforcement agencies (sheriff, state troopers,

state attorney general, the FBI, the U.S. Secret Service, the FTC or the U.S. Postal Inspection Service).

- Download a free ID Theft Affidavit from the FTC (*www.identitytheft.gov/*) and fill it out.
- Get proof of fraudulent accounts. *(See "Monitor accounts" section below.)*

Use fraud alerts. Put a free fraud alert on your credit report to help stop ID thieves from opening accounts.

- Choose an initial alert, which, as of Sept. 21, 2018, stays on your credit report for one year, or an extended alert, effective for seven years. With fraud alerts, your identity must be verified before new credit can be issued, so allow for extra time to open new credit.
- To put an alert on your credit reports, contact any one of the three major credit reporting agencies: Equifax: 800-525-6285 / *www.equifax.com*; Experian: 888-397-3742 / *www.experian.com*; or TransUnion: 800-680-7289 / *www.transunion.com*.
- Always ask for the free credit reports you are entitled to when placing fraud alerts. (Initial alerts give you one additional free credit report from each bureau after filing the alert; extended alerts, two additional free credit reports from each bureau within 12 months of filing the alert.)
- Review your reports closely for listings by companies you don't do business with, accounts you didn't open and debts you don't recognize. Make sure your personal information is correct.
- File a dispute with the credit bureaus if you find any questionable or inaccurate information.

Monitor accounts. Dispute fraudulent accounts and lock out thieves so they don't do more damage.

- Close accounts opened without your knowledge as well as existing accounts on which fraud has occurred. Ask for the security or fraud department of the company. Follow up with a written request.
- Create new personal identification numbers (PINs) and passwords for your accounts. Avoid easy-to-guess PINs such as your birthdate, address or phone number.
- If the identity thief has used any of your existing accounts, ask the credit issuer how to dispute fraudulent charges.
- Ask the credit issuer for a letter stating that the disputed account has been closed and fraudulent transactions erased.

Ongoing prevention

Review your credit reports

- Go to AnnualCreditReport.com (*www.annualcreditreport.com*) or call 877-322-8228 to get your free credit reports.
- Review your reports for listings by companies you don't do business with, accounts you didn't open and debts you don't recognize.
- Make sure your personal information is correct.
- Dispute all questionable or inaccurate information.

Social Security numbers

- Victims of ID theft often ask if they can get a new Social Security number. Usually, this is not possible.
- A new Social Security number might not give you a fresh start because the credit reporting agencies may combine records under your old Social Security number with those under your new number.
- With a new Social Security number, you might find it difficult to get new credit because you have no credit history.
- Visit the Social Security Administration website (*www.ssa.gov*) for more information.

Password all accounts

- Place passwords on your credit card, bank and phone accounts.
- Don't use easy-to-guess names or numbers.
- If companies you do business with want your mother's maiden name, ask to use a different password.

Computer safety

- Never respond to emails or text messages asking for personal information. Legitimate companies don't do this.
- If you are interested in why you were contacted, independently find the legitimate contact information of the company and ask if the communication is legitimate.
- Double-check all web addresses (URLs) when you visit websites so you won't accidentally mistype the URL and land on a "spoof" site designed to trick you and steal your information.
- Make sure the site is secure by verifying the padlock security symbol in your browser's window.

Proof of the crime

- By law, companies must give you free copies of fraudulent applications and other business transaction records relating to your identity theft. You may be asked for proof of identity, a police report and an affidavit before the company complies.
- Copies of the applications and transaction records might help you prove they were forged.

About Consumer Action

www.consumer-action.org

Through multilingual consumer education materials, community outreach and issue-focused advocacy, Consumer Action empowers underrepresented consumers nationwide to assert their rights and financially prosper.

Consumer advice and assistance: Submit consumer complaints to: *https://complaints.consumer-action.org/forms/english-form* or 415-777-9635 (Chinese, English and Spanish spoken).

Be careful and stay informed

- Don't give out personal information unless you are sure you are dealing with a reputable company.
- Don't respond to communications seeking personal information such as account numbers or passwords, or to emails or text messages that ask you to "click" a link to go to the site.
- When you call businesses, use the phone number on your account statement or provided by a trustworthy source.
- Stay informed—check the websites of consumer organizations and businesses for "scam alerts."

'Freezing' your credit

- You have the option to freeze your credit report to prevent new credit from being issued in your name.
- As of Sept. 21, 2018, freezing and unfreezing your reports is free in all states, and you can also get a free credit freeze for children under age 16 in all states.
- To freeze your credit report, contact the three credit reporting agencies. *(See "ID theft cleanup" section, page 2.)*

More information

FTC's ID theft clearinghouse. The FTC provides educational materials and complaint forms at its ID Theft website (*www.identitytheft.gov*) or by phone, through its Identity Theft Hotline, at 877-438-4338.

Free credit reports. Get a free copy of your credit reports every 12 months at AnnualCreditReport.com (*www.annualcreditreport.com*) or by calling 877-322-8228.

About this guide

Consumer Action's Managing Money Project (*www.managing-money.org*) funded updates and revisions to this guide.

Rev. 7/18