



IDENTITY THEFT PROTECTION CHECKLIST

IdentityTheft.gov. Visit the Federal Trade Commission site for guidance on how to report and recover from identity theft.

Order a copy of your credit report from each of the three major credit bureaus. Your credit report contains information on where you work and live, the credit accounts that have been opened in your name, how you pay your bills and whether you've been sued, arrested or filed for bankruptcy. Make sure it's accurate and includes only those activities you've authorized. The major credit bureau agencies charge a minimal fee for your report (usually not more than \$10 per report). Be wary of companies charging in excess of this amount. Visit www.annualcreditreport.com or use the phone numbers below.

Equifax 1-877-322-8228

Trans Union 1-800-888-4213

Experian 1-866-200-6020

Pre-Screened Credit Offers

If you receive pre-screened credit card offers in the mail (namely, those based upon your credit data), but don't shred them after you decide you don't want to accept the offer, identity thieves could retrieve these offers for their own use without your knowledge. To opt out of receiving prescreened credit card offers, call: 1-800-5-OPTOUT. (1-888-567-8688) or www.optoutprescreen.com.

Telemarketing

The federal government created the National Do Not Call Registry – it's a free, easy way to reduce the telemarketing calls you get at home. To register or for more information, visit www.donotcall.gov or call 1-888-382-1222 from the phone you want to register.

Mail

The Direct Marketing Association's (DMA) Mail Preference Service lets you "opt out" of receiving direct mail marketing from many national companies for five years. When you register for this service, your name will be put on a "delete" file and made available to direct-mail marketers. However, your registration will not stop mailings from organizations that are not registered with the DMA's Mail Preference Service. Register online at www.dmachoice.org.

Email

Use DMA's Email Preference Service to help you reduce unsolicited commercial emails. To "opt-out" of receiving unsolicited commercial email, use the online form at www.dmachoice.org. Your online request will be effective for one year.

Accounts

Close all dormant/unused bank and credit accounts. These accounts may show as available credit, which may not always be good when applying for new credit and could bring your credit score down.

Inventory

Make an account inventory that includes account numbers and contact phone numbers. In the unfortunate event you have lost a credit card, checkbook, or if your identity has been stolen, you will be able to quickly notify the appropriate companies. Make sure you keep this in a secure place, such as your safe deposit box or a locked cabinet/drawer in your home.

IDENTITY THEFT PROCEDURES

What to do if you are a victim

**KEEP A RECORD OF ALL CONVERSATIONS AND CORRESPONDENCE WITH FEDERAL AND LOCAL LAW ENFORCEMENT AGENCIES.
(Include contact names and dates of contact)**

1. Call Identity Theft Hotline to report incident: 1-877-ID THEFT (1-877-438-4338)
2. Complete ID Theft Affidavit: go to www.consumer.gov/idtheft
3. Close any accounts that have been tampered with or opened fraudulently.
4. File a report with local police in the community where theft took place.
5. Call one of the following Credit Reporting Agencies:

Equifax:	1-877-322-8228
Trans Union:	1-800-888-4213
Experian:	1-866-200-6020

Request a copy of your credit report; review it for any inaccuracies, and place a fraud alert on your report. Also send the credit agency copies of your affidavits describing any fraudulent activity.

6. If identity theft involves mail, contact the U.S. Postal Inspection Service at www.usps.gov/websites/depart/inspect
7. If identity theft involves Social Security number misuse, contact the Social Security Administration at **1-800-269-0271**

TIPS TO AVOID BECOMING A VICTIM OF IDENTITY THEFT

MANAGE YOUR MAILBOX

- Do not leave bill payment envelopes clipped to your mailbox or inside with the flag up; criminals may steal your mail and change your address.
- Know your billing cycles, and watch for any missing mail. Follow up with creditors if bills or new cards do not arrive on time. An identify thief may have filed a change of address request in your name with the creditor or post office.
- Carefully review your monthly accounts, credit card statements and utility bills (including cell phone bills) for unauthorized charges as soon as you receive them. If you suspect unauthorized use, contact the provider's customer service and fraud departments immediately.
- When you order new checks, ask when you can expect delivery. If your mailbox is not secure, ask to pick up checks instead of having them delivered to your home.
- Although many customers appreciate the convenience and customer service of general direct mail, some prefer not to receive offers of pre-approved financing or credit. To "opt out" of receiving such offers, call (888) 5 OPT OUT sponsored by the three credit bureaus.
- The Direct Marketing Association offers services to help reduce the number of mail and telephone solicitations. To join their mail preference service, mail your name, home address and signature to: Mail Preference Service, Direct Marketing Association, P.O. Box 9008, Farmingdale, NY 11735-9008

CHECK YOUR PURSE OR WALLET

- Never leave your purse or wallet unattended, even for a minute.
- Protect your pin numbers (don't carry them in your wallet!) and passwords; use a 10-digit combination of letters and numbers for your passwords, and change them periodically.
- Carry only personal identification and credit cards you actually need in your purse or wallet. If your ID or credit cards are lost or stolen, notify the creditors immediately, and ask the credit bureaus to place a "fraud alert" on your file.
- Keep a list of all your credit cards and bank accounts along with their account numbers, expiration dates and credit limits, as well as the telephone numbers of customer service and fraud departments. Store this list in a safe place.
- If your state uses your Social Security number as your driver's license number, ask to substitute another number.

KEEP YOUR PERSONAL NUMBERS SAFE AND SECURE

- When creating passwords and PIN numbers, do not use any part of your Social Security number, birth date, middle name, wife/husband's name, mother's maiden name, address, consecutive numbers, or anything that a thief could easily deduce or discover.
- Ask businesses to substitute a secret alpha-numeric code as a password instead of your mother's maiden name.
- Shield the keypad when using ATMs
- Memorize your passwords and PINs; never keep them in your wallet, purse, Rolodex or electronic organizer.
- Get your Social Security number out of circulation and release it only when necessary – for example on tax forms and employment records, or for banking, stock and property transactions.
- Do not have your Social Security Number printed on checks, and do not allow merchants to write your Social Security Number on your checks. If a business requests your Social Security Number, ask to use an alternate number.
- Never give your Social Security number, account numbers or personal credit information to anyone who calls you.

BANK, SHOP, AND SPEND WISELY

- Store personal information in a safe place, and shred or tear up documents you don't need. Destroy charge receipts, copies of credit applications, insurance forms, bank checks and statements, expired charge cards and credit offers you get in the mail before you put them out in the trash.
- Cancel unused credit cards so that their account numbers will not appear on your credit report.
- When you fill out a loan or credit application, ensure that the business either shreds these applications or stores them in locked files.
- Tear up receipts, bank statements and unused pre-approved credit card offers and convenience checks before throwing them away.
- When possible, watch your credit card as the merchant completes the transaction.
- Use credit cards that have your photo and signature on the front.
- Sign your credit cards immediately upon receipt.
- Keep track of credit card, debit card and ATM receipts. Never throw them in a public trash container. Tear them up or shred them at home when you no longer need them.

- Ask businesses what their privacy policies are and how they will use your information: Can you choose to keep it confidential? Do they restrict access to data?
- Choose to do business with companies that are reputable, particularly online.
- When conducting business online, use a secure browser that encrypts or scrambles purchase information and make sure your browser's padlock or key icon is active.
- Don't open email from unknown sources. Use virus protection software.

REVIEW YOUR INFORMATION

- Order a copy of your credit report from the three credit reporting agencies every year and make sure all the information is correct, especially your name, address, and Social Security number. Look for indications of fraud, such as unauthorized applications, unfamiliar credit accounts, credit inquiries and defaults and delinquencies that you did not cause.
- Check your Social Security Earnings and Benefits statement once each year to make sure that no one else is using your Social Security number for employment.

11/06/2017

Your partner in banking