AVOIDING IDENTITY THEFT

Quick Guide

V 3.0

260138-1/1

Table of Contents

What is identity theft?

Identity theft is when someone obtains personally identifying information from another individual without permission, then uses that information to assume that person's identity. Perpetrators of identity theft may use the information they steal to take control of bank accounts, open new credit cards, commit crimes, perpetrate fraud, carry out transactions, and make purchases in the victim's name.

Identity theft is a serious threat. It can compromise your name, Social Security number, bank and credit card account numbers, medical record and health insurance information, and other personally identifying data. It is also on the rise.

According to a 2014 report from Javelin Strategy and Research, 13.1 million people in the U.S. became victims of identity fraud in 2013, an increase of 500,000 over 2012. Data breaches were the main source of fraud that year, with one in three people who received notifications of a data breach discovering their identities were being used fraudulently. Someone in America becomes a victim of identity fraud every two seconds.

Identity theft has deep financial repercussions that can affect a person's credit, financial security, taxes, insurance, and overall financial health for years to come. Your best protection is to educate yourself about identity fraud and be on the alert for signs someone has accessed your personal information so you can take prompt action.

Types of identity theft

Tax-related identity theft. In cases of tax-related identity theft, a perpetrator gains access to your Social Security number, then uses it to apply for employment or file taxes and get a tax refund in your name.

Keep in mind that the IRS never initiates communication with a taxpayer via email, text message, or social media and never asks for financial information via these methods. If you do receive a suspicious message from someone claiming to be the IRS, don't answer it. Instead, forward it to phishing@IRS.gov or speak to a local tax expert about it.

Medical identity theft. In cases of medical identity theft, perpetrators gain access to your health insurance information or Medicare identification and use it to gain access to medical care or fill prescriptions. In these cases, discrepancies will show up in medical bills, explanations of benefits, and medical records.

Bank and credit card fraud. Thieves gain access to bank account numbers, passwords, credit card numbers, and pre-approved credit card offers in your name. They use that information to make fraudulent charges or bank withdrawals. Thieves also may apply for loans or lines of credit, or get credit cards in your name.

Cybercrime. Thieves gain access to identifying data via the Internet. This may include user IDs, passwords, and security answers for e-commerce, online banking, payment services, and other types of websites. Thieves may also solicit personal information via email, text message, or social media by pretending to represent a legitimate institution, such as a bank, creditor, government agency, educational institution, or charity.

How thieves get your personal information

Identity thieves and perpetrators of fraud find many ways to access your personal information. They may:

- Go through your trash or recycling bin at home, work, or the public landfill
- Misrepresent themselves as working for a legitimate organization (medical office, pharmacy, government agency, charity) to try to trick you into divulging bank account numbers or other personal information
- Send you emails that look like they are from your bank or another institution you trust asking for personal data

After a perpetrator has gained access to your personal data, such as your social security number, health insurance information, or bank account numbers, they can:

- Drain your bank accounts or investment accounts
- Run up charges using your credit cards
- Apply for loans and credit cards in your name
- Open accounts for utilities, new charge cards, and other items in your name
- Get medical treatment or prescriptions using your health insurance
- Sometimes, give your name to the police in the event of an arrest

Keep important numbers safe

The following numbers, codes, and documents are targets for identity theft. Keep them private and in a safe place:

- **Social Security number.** Keep your Social Security card someplace safe, not in your wallet or vehicle. Don't write your SSN on checks.
- **Bank and credit card numbers.** Only carry essential documents and cards. For example, only carry one credit card in your wallet, and leave the rest at home.
- **Personal identification documents.** Don't carry your birth certificate, passport, or other identifying documents. Keep them locked away in a safe place.
- **PINs.** Avoid writing down PINs for your debit or credit cards and storing them in your wallet or purse. Avoid storing PINs for online banking, Internet payment services, online shopping, and other sites where someone could easily find them. If you must keep a list of PINs, store it in a safe, lockbox, or other secure location.
- **Health insurance membership numbers.** Keep your insurance card or Medicare card at home unless you are going to a medical provider. If you want to carry proof of insurance with you, copy your card and black out all but the last few digits before you store the copy in your wallet or purse.

Safety tips to keep in mind:
Be aware if someone is standing behind you while you use an ATM or punch your password into a keypad at a store counter. Shield the machine with your free hand or your body.

Don't give out account numbers, your Social Security number, or other personal information over the telephone, through the mail, or via the Internet unless you initiated the contact. If you have doubts about someone who has contacted you asking for personal information, call the customer service number listed on your account statement or card to inquire whether a request for information was made.

Keep prying eyes out

Identity thieves often access private information via "dumpster diving" at your place of residence, workplace, or businesses where you have conducted transactions. They also may go through your mail. Keep paperwork out of identity thieves' hands with these measures.

- Don't let mail sit in your mailbox. If you're going to be away for more than a day, put in a hold mail request with the U.S. Postal Service.
- Keep track of your receipts. Ask for receipts in retail stores, restaurants, and medical offices, particularly if you use your credit card. Use them to match transactions with your account statements. Dispose of receipts properly, preferably by shredding them.
- Tear up or shred old receipts, credit card offers, account statements, expired credit cards, health insurance EOBs, and any other paperwork that has your personal information printed on it.
- Don't have new checks mailed to your home, especially if they will sit in the mailbox until you get home from work. Have them sent to a local bank branch so you can pick them up.
- Talk with your landlord, employer, healthcare provider, and others who store and access your personal information to ensure they are keeping it safe.

Stop Pre-Approved Credit Offers

Opt out of pre-approved credit card and insurance offers by calling 1-888-567-8688 or visiting optoutprescreen.com. This service is operated by the three credit reporting agencies. If you choose to opt out, you won't receive credit card offers--but you will also keep them out of the hands of identity thieves.

Keep online transactions safe

These days, many of us bank, communicate with healthcare providers and insurance companies, perform financial transactions, and shop via the Internet. This is convenient, but it also can put your personal information at risk if you're not careful.

- Before you donate or throw away a computer, use a specially designed program to "wipe" the hard drive so personal information is overwritten and can't be accessed.
- Install a firewall and anti-virus protection on your home computer, and keep it up to date.
- Use encryption software to scramble information you send over the Internet so it can't be intercepted by someone en route to its destination. Many banking and shopping websites, as well as other sites that require you to enter financial and other personal information, are equipped with their own encryption software. To ensure your information is being hidden from prying eyes, look for a lock icon in your browser's status bar.
- When you devise passwords for credit card, bank, health insurance, shopping, and other sites, make them as strong as possible. Avoid using whole words, dates, or other information that could be easily guessed. Use a combination of letters, symbols, and numbers.
- If you have trouble keeping track of account numbers, user names, and PIN numbers for varied accounts, consider a secure, online "wallet" or storage solution that stores all your personal data and keeps it locked down in a single, secure location only you can access.
- Be cautious about giving away too much personal information on social media sites. Avoid sharing your address, Social Security number, shopping information, account numbers, vacation plans, etc. Adjust your privacy settings so only the people you are close with can see your posts and view your information.
- Before you recycle, turn in, or sell a mobile device, remove the SIM card that contains records of your personal information.

- Don't send personal information over a public Wi-Fi connection, such as those in coffee shops and airports. When using public Wi-Fi, avoid using automatic log-in that saves your user name and password. Instead, log in by hand and log out when you are done so a thief can't use your laptop or mobile device to access your personal information. Only do business with secure sites over public Wi-Fi.
- Don't open files or click on links emailed by sources unfamiliar to you. These could be "phishing" scams that capture your passwords and other personal information.

FACT: According to a 2012 report from Juniper Research, only 5 percent of mobile devices are protected, and identity theft due to lost or stolen smartphones and tablets is on the rise.

Consider installing security software on your mobile device, especially if you use it to store, access, and transmit personally identifying information. Be cautious, too, about using apps for shopping, banking, investing, and other transactions. Ensure your information is protected with strong passwords, and consider subscribing to a service that will automatically "wipe" your device if it is misplaced or stolen.

Identity theft warning signs

The Federal Trade Commission cautions consumers to keep a close eye on their bank accounts, financial statements, bills, and other records in order to catch the earliest signs of identity theft. If you notice any of these troublesome signs, don't ignore them. The sooner you report identity theft, the more quickly it can be resolved and the less damage will occur.

- Bank account withdrawals you don't recall making
- Missing bills or other mail
- A merchant refusing your check when you are not at fault
- Calls from collection agencies about debts that aren't yours or charges you were unaware of
- Unfamiliar accounts, charges, or inquiries listed on your credit report
- Medical bills or insurance claims for services you didn't receive
- Notices from the IRS that more than one tax return was filed in your name when you try to file taxes and/or get your refund
- Income reported on your tax return from an employer you did not work for
- A notice of a data breach from a company with which you do business or where you have an account
- Being notified of applications for loans, credit lines, or credit cards you did not apply for

Review Your Credit Reports

Federal law mandates you can receive one free credit report per year from each of the three credit reporting agencies: Experian, TransUnion, and Equifax. Get your credit reports annually, and review them thoroughly to ensure all the information is correct and up to date. Keep an eye out for any red flags that could indicate identity theft, such as unfamiliar inquiries or accounts and addresses you don't recognize. Visit www.annualcreditreport.com to order your free credit reports.

Four steps to take if you suspect you have become a victim

1. The first step you should take if you suspect you have become the victim of identity theft is to call your financial institution immediately. Contact your bank as well as your credit card companies, and let them know you have found evidence of theft or fraud. Close your financial accounts.
2. Next, report the suspected theft or fraud to your local police department and fill out a police report. This will formalize your case, and start you on the road to remedying the situation with your creditors. Be sure to get a copy of the police report and note the report number for when you speak with financial institutions and the credit bureaus.

3. Contact the three credit reporting bureaus: Equifax, TransUnion, and Experian. They will flag your account and put a fraud alert on it, letting potential creditors know that new credit can't be given in your name without your approval.
4. Contact the Federal Trade Commission at www.ftc.gov/idtheft or 1-877-ID-THEFT (1-877-438-4338) to report the identity theft to the federal government and fill out an ID theft affidavit that will help you communicate with companies, financial institutions, and creditors about what happened.

Other

What is a fraud alert?

Once you have reported identity theft, you can ask the three major credit reporting agencies to place an extended fraud alert on your credit file. The alert will last for up to seven years, and it lets potential creditors or lenders know that you have been a victim of identity theft so they can help protect you.

Once this fraud alert is in place, you are allowed to receive two free credit reports annually from each of the credit reporting agencies. The credit reporting agencies will also remove your name from the list for receiving prescreened credit offers for five years. You may remove the fraud alert at any time.

What is security freeze?

A security freeze or credit freeze is a step allowed under most state laws that blocks access to your credit report by most third parties or creditors. Certain organizations and individuals may still be allowed access to a frozen credit report depending on the laws in your state, such as potential landlords or employers. Check with your State Attorney General's office for a list of security freeze exceptions in your state.

If you are a victim of identity theft, you have the right under state law to place a security freeze on your credit via all three credit reporting agencies. That way, no one will be able to apply for credit in your name. In order to process a new credit application, you must request that the freeze be temporarily lifted. The freeze will remain in place until you request its removal. There may be a fee associated with placing a security freeze.

Getting your identity back

Identity theft is a serious event, but it does not have to ruin your finances or your good name. Taking the right steps to protect your personal information can

keep it from ever happening to you. If you do become a victim, immediate action can put a stop to financial loss or damage to your credit, and put you on the road to restoring your good name and reputation. The best defense against identity theft is information combined with common sense.

Resources for more information

To find out more information about identity theft, consult the following resources.

Federal Trade Commission

- www.ftc.gov/idtheft or 1-877-ID-THEFT (1-877-438-4338)
- Call the FTC hotline or visit the website to get more information and to report identity theft to the federal government. You can fill out an identity theft affidavit via the FTC that will help you begin to work with companies, financial institutions, and creditors to restore your good name.
- Forward suspicious spam or suspected phishing emails to spam@uce.gov.

Credit Reporting Agencies

- Experian (ww.experian.com or 1-888-397-3742)
- Equifax (www.equifax.com or 1-800-525-6285)
- TransUnion (www.transunion.com or 1-800-680-7289)