

Brown County Sheriff's Office

Safety Tip: Identity Theft

Identity theft is one of the fastest-growing financial crimes in America, accounting for losses in the billions of dollars every year. The Federal Trade Commission reports that 10 million Americans discovered that their personal information had been misused by someone else in some manner last year. The Brown County Sheriff's Department offers these tips for protecting yourself, and advice of what to do if it happens to you.



Identity theft is when someone illegally obtains a person's identifying information, such as name, address, date of birth, social security number or mother's maiden name. Armed with this information, an imposter can open new credit card accounts, drain your bank accounts, purchase automobiles, apply for loans, open utility services and on and on.



Identity theft can occur in a number of different ways. But if you know what to look for and how it happens, you can minimize your overall risk. Here are a few common scenarios to watch out for:

- Lost or stolen wallet or checkbook
 - The most commonly reported source of information used to commit fraud is a lost or stolen wallet or checkbook. Stolen wallets and checkbooks usually contain a number of credit and debit cards, in addition to other personal documentation. Using these items, a thief can get enough information to obtain credit under the victim's name, or sell the information to an organized crime ring.

- Dumpster diving
 - Thieves rummage through trash cans for pieces of non-shredded personal information that they can use or sell.
- Mail Theft
 - Crooks search mailboxes for pre-approved credit card offers, bank statements, tax forms, or convenience checks. They also look for credit card payment envelopes that have been left for postal carriers to pick-up.
- Inside Resources
 - Half of all identity fraud is committed by friends, family members, relatives, employees, and live-in caregivers with access to privileged information. Information such as personal records, payroll information, insurance files, account numbers or sales records can be sources for theft.
- Imposters
 - Many have fallen victim to identity theft by individuals who fraudulently posed as someone who had a legitimate or legal reason to access the victim's personal information (e.g., a landlord or employer asking for background information).
- Documents in the home
 - Unfortunately, identity thieves can gain legitimate access into someone's home and personal information through household work, babysitting, healthcare, friends, or roommates.
- Online date
 - Although most identity theft occurs through traditional methods, such as the ones outlined above, risks still exist online. Be cautious when sending information electronically over the Web. Account information sent through email, or online chat, can be easily intercepted by thieves.



- ⇒ Don't have your driver's license number or Social Security number printed on your checks.
- ⇒ Don't carry your Social Security card or birth certificate in your wallet or purse.
- ⇒ Try not to carry more than one credit card in your wallet; or carry only the credit cards you plan to use.
- \Rightarrow Don't carry credit card receipts. Keep them safe or destroy them.
- ⇒ When choosing passwords, think of something that is not obvious. The best choice is a combination of upper and lower case letters as well as numbers.
 - \circ $\,$ Do not use your mother's maiden name as a password.
 - Change the passwords often.
 - Don't carry account passwords with your cards or write them on the cards.
- ⇒ When you have applied for a new card, keep your eye on the mail and the calendar. If the card does not arrive within the appropriate time, call the credit card company.

- \circ Shred all credit card offers mailed to you that you don't intend to apply for.
- ⇒ Sign up for direct deposit of payroll to prevent paper checks from ending up in the wrong hands.
- ⇒ Never give your credit card number or bank account information to anyone calling you.
- ⇒ Ask to have your checks mailed to your bank, not to your home.
- ⇒ Lock your mailbox. Don't leave outgoing mail in your mailbox; drop it off at the post office or Postal Service mail box instead.
 - Do not allow mail to go uncollected. Retrieve it promptly.
- ⇒ When paying with your credit card, encourage clerks to check your identification.
- \Rightarrow Review monthly bills carefully for unexplained charges.
 - Request electronic versions of bills, statements, and checks instead of paper.
- ⇒ Shred all documents with account numbers before disposing of them.
- ⇒ Order only from secure, reputable Internet sites.
 - Only use your credit card on the internet if it will be encrypted.
- ⇒ Order your credit report from three major credit bureaus and make sure the information is correct.
- ⇒ Make photocopies of the items in your wallet (both sides). Keep this photocopy in a safe place.
- ⇒ Prior to discarding a computer, make sure all personal information is deleted from its hard drive.
- ⇒ Be aware of your surroundings when entering your Personal Identification Umber (PIN) at an ATM.
- ⇒ Make sure you take receipts with you after your purchase.



In many cases involving identity theft, months pass before the victim is aware of any wrongdoing. Simply monitoring your credit card and account statements on a weekly basis can greatly decrease your identity theft risk. In fact, the majority of identity theft crimes are self-detected. And according to a recent report by the Better Business Bureau, accessing accounts online provides earlier identity theft detection compared to monitoring monthly statements and bills.



- Report lost or stolen credit cards immediately.
- Cancel all inactive credit card accounts
- When using your credit card do not volunteer any personal information.
- Closely monitor the expiration dates on your credit cards. Contact the credit issuer if the replacement card is not received prior to your credit cards expiration date.
- Sign all new credit cards upon receipt.
- Match your credit card receipts against monthly bills to make sure there are no unauthorized charges.

If it Happens to You

One of the most frightening and overwhelming types of fraud is identity theft. If you've been or think you've been a victim of identity theft, there is a proven process in place that can help you resolve your problem and help you protect yourself from further harm.

If you think you're a victim of identity theft, it's important to act quickly to minimize your losses.

Follow these steps to minimize the damage and stop the thief:



Step 1: Call for free, confidential counseling

If you are a victim of identity theft, you can get help now through a unique partnership with the consumer network Call for Action. Victims of identity theft can receive access to free, confidential counseling by calling 1-866-ID-HOTLINE (1-866-434-6854). This important hotline is staffed by trained counselors who are ready to walk you through step-by-step the process of getting your identity back. You can also go to Call for Action's web site to request assistance.

Step 2: Contact credit bureau

Immediately place a "fraud alert" on your credit reports with a toll-free call to one of the three national credit bureaus (see below for contact information). Fraud alerts can stop an identity thief from opening more accounts in your name. They also ensure you will be contacted before any new account is opened or an existing account changed.

Note that one call to any of the three credit bureaus will be enough to place your fraud alert – the company you call is required to contact the other two, within twenty-four hours. All three of the credit bureaus will be on alert.

When placing a fraud alert, be sure to have the following information available to prove your identity:

Name Social Security number Address

You may be required to provide personal information as requested.

In addition to placing fraud alerts, the bureaus will:

Opt you out from all pre-approved offers of credit for up to five years.

Provide a free copy of your credit reports. This can help you identity any new accounts that may have been opened. Pay particular attention to the section of the report that list inquires from new companies. Contact these companies immediately and have them remove any pending or new accounts from their system.

Equifax www.equifax.com 800-525-6285 (Fraud Hotline) 800-685-1111 (Report Order) P.O. Box 740250 Atlanta, GA 30374

Experian <u>www.experian.com</u> 888-397-3742 (Fraud Hotline) 888-397-3742 (Report Order) P.O. Box 9556 Allen, TX 75013

TransUnion www.transunion.com 800-680-7289 (Fraud Hotline) 800-916-8800 (Report Order) P.O. Box 6790 Fullerton, CA 92634

Step 3: File a Police Report

Your report should be filed with your local sheriff/police department or the sheriff/police where the identity theft took place.

In Wisconsin stealing someone's identity is a violation of State Statute 943.20: *Misappropriation of personal identifying information or personal identification documents*.

Keep your copy of the report or the report number as proof of the crime. It can help you deal with creditors and file Identity Theft reports.

Step 4: Contact creditors' fraud departments

You should close any accounts that have been tampered with or opened without your permission.

Call and speak with someone in the security or fraud department of each creditor and describe your identity theft problem. Follow up with a letter or affidavit – be sure to include copies (not originals) of supporting documents. It's important to notify credit card companies and banks in writing.

Take advantage of the Federal Trade Commission's ID Theft Affidavit (PDF, 46k), a standard form that helps simplify the identity theft reporting process. Victims can use it to report to different organizations, such as the three major credit bureaus and banks or creditors. – anywhere an account has been opened under the victim's name. This is very important for credit card issuers, since the consumer protection law requires cardholders to submit disputes in writing. It may prove helpful to the investigating officer of the local sheriff or police department you have filed your complaint with to provide him or her with a copy of the affidavit.

Federal Trade Commission Consumer Response Center 600 Pennsylvania Avenue, N.W. Washington, DC 20580 1-877-IDTHEFT www.consumer.gov/idtheft/

It is also a good idea to send all correspondence by certified mail, return receipt requested and keep a file of all your letters and enclosures.

QUICK TIP: after you have closed a fraudulent account with a creditor, always ask the creditor for a letter confirming that they have closed the account and discharged the debts. Make sure to keep this letter in your files for future reference, as you may need it if the account reappears on your credit report.

Step 5: File a complaint with the Federal Trade Commission (FTC)

The FTC handles complaints from victims of identity theft, provides information to those victims, and refers complaints to major credit reporting and law enforcement agencies for further action, as well as investigate companies for violations of laws the agency enforces.

To file a complaint, fill out the online complaint form found at the FTC website.

MORE QUICK TIPS: here are some helpful hints to organize your case:

- Have a plan
 - You can never be too prepared. Have a list of questions and make sure they're all answered before you end your call.
- Take names
 - Write down the name, title and contact information of everyone you talk to, what he or she tells you, and when the conversation occurred.
- Follow up
 - Contact everyone you have spoken with in writing. Use certified mail, return receipt requested as documentation.
- Keep documentation
 - Make copies of all correspondence or forms you send, and keep originals of supporting documents, like police reports and letters to and from creditors – send copies only. In some cases you may need these documents to prove that you're a victim of identity theft.
- Maintain good records
 - Set up a filing system for easy access to your paperwork and keep old files even if you believe your case is closed.