



Defending Yourself Against Identity Thieves

Identity theft occurs when someone uses personal information such as your name, Social Security number or bank account number without your knowledge to commit fraud or theft.

How Do Identity Thieves Get My Personal Information?

Skilled identity thieves use a variety of methods to gain access to your personal information, such as:

- Stealing your ID cards, credit cards and bank cards.
- Stealing your mail, including account statements, pre-approved credit card offers and tax information.
- Buying your personal information from sources such as employees at stores, restaurants, hospitals or hotels.
- Getting your information off the Internet.
- Rummaging through your trash or the trash of businesses or dumps in a practice known as “dumpster diving.”
- Stealing credit and debit card numbers as your card is processed by using a special information storage device in a practice known as “skimming.”
- Completing a change of address form to divert your mail to another location.
- Posing as a legitimate business person or government official to acquire your personal identifiers in a practice known as “pretexting.”

How Do Identity Thieves Use My Personal Information?

Identity thieves typically open new bank or credit card accounts in your name or change the mailing address for your existing accounts so they can use them without your knowledge. The thieves can then go on spending sprees using your credit and debit card accounts or with new accounts they create to buy “big-ticket” items like computers that they can easily sell. When the thieves use the accounts without paying the bills, the delinquent accounts are noted on your credit report.

Identity thieves can also use personal identifiers stolen from victims in the following ways:

- To take out auto loans in your name.
- To establish utility, phone or wireless service in your name.
- To counterfeit checks or debit cards and drain your bank account.
- To open a bank account in your name and write bad checks on that account.
- To file for bankruptcy under your name to avoid paying debts they’ve incurred or to avoid eviction.
- To give your name to the police during an arrest. If the thieves are released and don’t show up for their court date, an arrest warrant could be issued in your name.

How Can I Keep My Personal Information Safe?

To minimize your risk of becoming a victim of identity theft, follow these basic guidelines.

- If you are asked to disclose personal information, ask the requester how the information will be used and if they will share your information with anyone else.

- Know when your mail gets delivered and pick it up as soon as possible. Consider purchasing a secure mailbox that is difficult for thieves to gain access to. Never allow your mail to build up while you are out of town.
- Know when your bills are due to arrive. If they are late, contact your creditors.
- Keep your personal information and all items containing your personal information (such as account statements, receipts and forms) in a secure location. When you no longer need these items, tear them up or shred them before throwing them away.
- Leave your Social Security card in a safe place. Do not disclose your Social Security number unless it is absolutely necessary.

Protect Your Credit Cards and Bank Debit Cards While Shopping

- Carry only the credit or debit cards you know you'll need on a given day.
- When using a credit or debit card to make a purchase, be aware of where your card goes and try not to get distracted during the transaction.
- Get your credit or debit cards back immediately after a purchase. Always take receipts with you. When eating at a restaurant, don't leave receipts on the table—be sure your server picks up the original.
- Never throw receipts in a public trash container.
- Watch out for “*shoulder surfers*” when using ATMs.

Protect Your Credit Information

- Don't choose a PIN that uses easily identifiable information such as your street address, children's names or digits from your birth date, Social Security number or telephone number.
- Memorize all your passwords. Never write your PIN (personal identification number) on the back of your card or on a piece of paper in your wallet or handbag.
- Don't give your account number over the phone unless you initiated the call to make a purchase and you're sure the company is reputable.
- Keep a list or photocopy of all of your credit cards, the account numbers, expiration dates and telephone numbers of the customer service and fraud departments in a secure place at home. Should you lose your wallet or handbag, you will be able to contact your creditors and report the loss. Do the same with your bank account information.

Protect Your Social Security Number

- Give out your Social Security number only when absolutely necessary and don't put your Social Security number on any document unless it is legally required.
- Don't write your Social Security number on a personal check at a store or on applications for memberships such as at video rental shops or grocery stores.
- Don't have your Social Security number printed on your driver's license.

Protect Your Identity When Shopping Online

- Use a secure browser.
- Shop with companies you know.
- Keep your password(s) private.
- Keep a record of all transactions.

How Can I Tell if I'm a Victim of Identity Theft?

- Finding unexplained charges or withdrawals in your financial statements.
- Failing to receive bills or other mail signaling an address change by the identity thief.
- Receiving credit cards for which you did not apply.
- Receiving a denial of credit for no apparent reason.
- Receiving calls from debt collectors or companies about merchandise or services you didn't buy.
- Requesting and reviewing your credit reports from the three largest credit bureaus (Equifax, Experian and TransUnion) on a yearly basis looking for accounts you know are not yours.

What Should I Do If I Become a Victim of Identity Theft?

- If you're a victim of identity theft, take immediate action to prevent continued use of your personal information.
- Report the identity theft to the police. *Note: A law in Illinois passed through the efforts of Illinois Attorney General Lisa Madigan requires that police take your report.*
- Contact each of the three major credit reporting agencies (Equifax, Experian and TransUnion) and report the theft to their fraud units.
- Call your creditors and financial institutions. Close all accounts that have been opened or accessed by identity thieves. Ask for passwords to secure new accounts.
- Call the Office of the Illinois Attorney General to request an "Identity Theft Victim Kit."

For more information, please contact us.

Chicago
100 W. Randolph Street
Chicago, IL 60601
(312) 814-3000

Springfield
500 S. Second Street
Springfield, IL 62701
(217) 782-1090

Carbondale
601 South University Avenue
Carbondale, IL 62901
(618) 529-6400/6401

For individuals with communication disabilities, simply dial 7-1-1

Please visit www.IllinoisAttorneyGeneral.gov

