



Has some clown taken over your good name?

---

## INTRODUCTION

Criminals don't always need sawed-off shotguns and ski masks to make a big haul —your social insurance security number, or a pre-approved credit card application from your trash, could be all they need.

Consumer advocates and security experts say identity theft crimes will only become more common and the criminals more daring as electronic transactions become universal.

---

### What is identity theft?

"**Identity theft**" refers to crimes in which someone wrongfully obtains and uses another person's **personal data** (*i.e., name, date of birth, social insurance number, driver's license number, and your financial identity— credit card, bank account and phone-card numbers*) in some way that involves fraud or deception, typically for economic gain (*to obtain money or goods/services*). Criminals also use identity theft to fraudulently obtain identification cards, driver licenses, birth certificates, social security numbers, travel visas and other official government papers.

**Unlike your fingerprints** (*which are unique to you and can't easily be given to, or stolen by, someone else for their use*), **your personal data can be used**, if it falls into the wrong hands, allowing criminals to profit at your expense.

On average, **most victims** don't even know their identity has been stolen until more than a **year** later.

Identity theft can have devastating consequences for you, as the victim, who may face long hours of closing bad accounts, opening new ones, and repairing your wrecked credit record. And, it may take significant out-of-pocket expenses to clear your good name. In the meantime, you may be denied jobs, loans, education, housing, and cars, or even get arrested for crimes you didn't commit. Unfortunately, the experience of thousands of victims is that it often requires months, and even years, to navigate the frustrating, identity-recovery process.



## How identity thieves **GET** your personal information:

Identity thieves can use a variety of high/low tech means to gain access to your personal information. Here are some of the ways these imposters can get your personal information and take over your identity—

- **Business Record Theft:** They get your information from businesses or institutions by stealing files out of offices where you're a customer, employee, patient or student; or bribing an employee who has access to your files; or even "hacking" into the organization's computer files.
- **Shoulder Surfing:** A "shoulder-surfing" identity thief, standing next to you in a checkout line, can memorize your name, address and phone number during the short time it takes you to write a check. An identity thief can stand near a public phone and watch you punch in your phone or credit card numbers *(or even listen in when you give your credit-card number over the phone for a hotel room or rental-car.)*
- **Dumpster Diving:** They rummage through your trash, or the trash of businesses, and landfills for personal data.
- **Under the Color of Authority:** They fraudulently obtain credit reports by abusing their employer's authorized access to credit reports, or by posing as landlords, employers or others who may have a legitimate need/right to the information.
- **Skimming:** They steal your credit/debit card account numbers as your card is processed at a restaurant, store or other business location, using a special data collection/storage device



### And through other forms of old-fashioned fraud and theft...

- Stealing wallets and purses containing identification and credit and bank cards.
- Stealing mail, including bank and credit card statements, pre-approved credit offers, new checks, or tax information.
- Completing a "change of address form" to divert your mail to another location.
- Stealing personal information from your home.
- Using personal information you share on the Internet.
- Scamming information from you, often through email, by posing as legitimate companies or government agencies.



## How identity thieves **USE** your personal information:

- Go on spending sprees using your credit and debit card account numbers to buy "big-ticket" items like computers that they can easily sell.
- Open a new credit card account, using your name, date of birth and S.I.N. When they use the credit card and don't pay the bills, the delinquent account is reported on your credit report.
- Call your credit card issuer and, pretending to be you, ask to change the mailing address on your credit card account. The imposter then runs up charges on your account. Because your bills are being sent to the new address, it may take some time before you realize there's a problem.
- Buy cars by taking out auto loans in your name.
- Establish phone or wireless service in your name.
- Counterfeit checks or debit cards, and drain your bank account.
- Open a bank account in your name and write bad checks on that account.
- File for bankruptcy under your name to avoid paying debts they've incurred under your name, or to avoid eviction.
- Give your name to the police during an arrest. If they're released from police custody, but don't show up for their court date, an **arrest warrant** is issued in **your** name.



## How can I tell if I'm a victim of identity theft?

- Monitor the balances of your financial accounts. Look for unexplained charges or withdrawals.
- Other indications of identity theft include:
  - failing to receive bills or other mail, which may signal an address change by the identity thief,
  - receiving credit cards, and/or statements of accounts, for which you did not apply
  - a lender tries to repossess a car you didn't know you owned
  - being contacted by the police after a crime is committed in your name.
  - being denied credit for no apparent reason...

If you're ever denied credit, FIND OUT WHY, especially if you haven't reviewed your credit report lately. This may be the first indication



you get that someone has stolen your identity and is racking up charges in your name.

- receiving calls or letters from debt collectors or businesses about merchandise or services you did not buy.

**REACT QUICKLY** if a creditor or merchant calls you about charges you didn't make. This, too, may be the first notice you get that someone has stolen your identity. Get as much information from them as you can and investigate immediately.

Although any of these indications could be a result of a simple error, you should not assume that there's been a mistake and do nothing. Always follow up with the business or institution.