



Tips for Preventing Identity Theft

Identity theft is a serious crime. People whose identities have been stolen can spend months or years - and their hard-earned money - cleaning up the mess thieves have made of their good name and credit record.

By understanding what identity theft is and how it occurs, you can help protect yourself from becoming a victim. If you're already a victim of identity theft, don't worry. It's never too late to take action.

What is Identity Theft?

Identity Theft refers to all types of crime in which someone wrongfully obtains and uses another person's personal data, such as their name, Social Security number, credit card number or other identifying information, in a way that involves fraud or deception, typically for economic gain.

Common Identity Theft Complaints

- Payments Card Fraud
- Unauthorized Phone or Utility Services
- Bank Fraud
- Fraudulent Loans
- Government Documents or Benefits

Popular Identity Theft Scams

- Phony Sweepstakes or counterfeit charities
- Work-at-home offers promising easy money
- Phony payment card, credit protection, or credit repair offers
- Pyramid Schemes (Where early "investors" get paid off with other people's money)
- Cut rate travel or discount magazine offers
- Scholarship Scams

How Criminals Get Your Personal Information

- Stealing wallets and purses containing your identification and credit and bank cards.
- Stealing your mail, including your bank and credit card statements, pre-approved credit offers, new checks, and tax information
- Completing a "change of address form" to divert your mail to another location
- Rummaging through your trash, or the trash of businesses, for personal data in a practice known as "dumpster diving"
- Fraudulently obtaining your credit report by posing as a landlord, employer or someone else who may have a legitimate need for, and legal right to, the information

- Finding your personal information in your home.
- Using personal information you share on the internet.
- Using E-mail scam techniques such as "Phishing" by posing as legitimate companies or government agencies you do business with.
- Obtaining your information from the work place in a practice known as "business record theft," by stealing files out of offices where you're a customer, employee, patient or student; bribing an employee who has access to your files; or "hacking" into electronic files.

How Criminals Use Your Stolen Information

- Contacting your credit card issuer, pretending to be you, and asking to change the mailing address on the credit card account. The imposter then runs up charges on your account. Because the bills are being sent to the new address, it may take some time before you realize there's a problem.
- Requesting additional credit/debit cards and new PIN to facilitate cash advance fraud.
- Opening a new credit card account, using your name, date of birth and SSN, but the thief's own mailing address. When they use the credit card and don't pay the bills, the delinquent account is reported on your credit report.
- Utilizing credit cards until 'open to buy' is exhausted, and fails to make payments causing delinquencies to be reported to credit bureaus.
- Establishing phone or wireless service in your name.
- Opening a bank account in your name and writing non-sufficient funds (NSF) checks on that account.
- Filing for bankruptcy using your name to avoid paying debts incurred in your name or to avoid eviction.
- Counterfeiting checks or debit cards to drain your bank account.
- Purchasing automobiles, boats etc. through loans obtained using your personal information.
- Giving 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.

Lost or Stolen

If your MasterCard is lost or stolen, call Emergency Services from anywhere in the world to cancel your account. Our global directory will help put you in touch with a representative who speaks your language - 24 hours a day, 365 days a year. For Commonwealth Bank issued Mastercards call 1800 011 217.

If you would like to find out more about securing your identity, payment cards and financial information, please visit our website at www.mastercard.com.

How You Can Protect Yourself from Identity Theft

- **Be very careful about to whom you give out personal identification information**, such as your mother's maiden name and your Social Security Number. Inquire into how it will be used and with whom it will be shared.
- **Never provide any personal, bank account or credit card information** to anyone who contacts you through a telephone solicitation.

- **Keep items with personal information in a safe place.** Keep a list of all credit cards, account numbers, expiration dates, and the customer service phone numbers in a secure place.
- **Tear Up or Destroy all ATM and bank receipts.** Thieves oftentimes search through your garbage to find these forms and information and use it to apply for credit in your name.
- **Minimize the number of credit cards and other items with personal information printed** on them that you carry. Cancel all inactive accounts

Steps to take when You become an ID Theft Victim

Sometimes an identity thief can strike even if you've been very careful about keeping your personal information to yourself. If you suspect that your personal information has been hijacked and misappropriated to commit fraud or theft, take these actions or steps immediately.

- **Place a fraud alert on your credit reports and review your credit reports.** Contact the three major credit bureaus (TransUnion, Experian and Equifax) to place a fraud alert on your credit report.
- **Close any account that have been tampered with or opened fraudulently.** Include all accounts with banks, credit card companies and other lenders, phone companies, utilities, ISPs, and other service providers. If your checks have been stolen or misused, close the account and ask your bank to notify the appropriate check verification service.
- **File a report with your local police or the police in the community where the identity theft took place.** Keep a copy of the report. You may need to validate your claims to creditors. If you can't get a copy, at least get the report number.
- **File a complaint with the Federal Trade Commission.** By sharing your identity theft complaint with the FTC, you will provide important information that can help law enforcement officials track down identity thieves and stop them.