



IDENTITY THEFT AND IDENTITY FRAUD

Identity theft and identity fraud refer to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain.

The identity thief can use a victim's name, address, date of birth, social security number, and/or mother's maiden name, to impersonate the victim. This or other information enables the thief to commit such frauds as taking over the victim's financial accounts; applying for loans, credit cards and social security benefits; renting apartments; and establishing service with utility and phone companies.

These thieves can obtain personal information from your trash, thefts of your purse or wallet, thefts from your vehicles, burglary of your home, dishonest bank employees, careless retailers who discard credit card information, on the Internet, thefts from your mailbox, and other sources.

Postal inspectors get involved because much of the criminal activity takes place through the mail. Often mail is stolen to obtain the information needed to order checks, or apply for credit cards by mail. The financial institutions often mail checks or credit cards to mail drop addresses used by the thieves.

In the United States and Canada, many people have reported that unauthorized persons have taken funds out of their bank or financial accounts or have even taken over their identities, running up vast debts and committing crimes using the victims' names. A victim's losses may include out-of-pocket financial losses and substantial additional financial costs associated with trying to restore his/her reputation in the community and correcting erroneous information for which the criminal is responsible.

If the criminal takes steps to ensure that bills for falsely obtained credit cards, or bank statements showing unauthorized withdrawals, are sent to an address other than the victim's, the victim may not become aware of what is happening until the criminal has inflicted substantial damage on the victim's assets, credit and reputation.

What can you do to avoid becoming a victim of Identity Theft?

Immediately repair any damaged or broken locking device on your mailbox.

- Promptly remove mail from your mailbox after delivery.
- Deposit outgoing mail in post office, lobby letter drops or in street collection boxes with mail pick-up scheduled later the same day.
- Do not place your outgoing mail in your mailbox for carrier pickup or in your apartment house outgoing mail slot.
- Immediately notify local police if you notice suspicious activity by a mailbox, blue collection box, or parked postal mail delivery vehicle.
- Never give personal information over the telephone, such as your social security number, date of birth, mother's maiden name, credit card number, or bank PIN code, unless you initiated the phone call. Protect this information and release it only when absolutely necessary.
- Shred pre-approved credit applications, credit card receipts, bills and other financial information you don't want before discarding them in the trash or recycling bin.
- Empty your wallet of extra credit cards and identification cards or better yet, cancel credit cards you don't use and maintain a list of the credit cards you do use.
- Order your credit report from the three credit bureaus (Equifax, Experian Information Solutions, and TransUnion) once a year to check for fraudulent activity or other discrepancies.
- Never leave receipts at bank machines, bank counters, trash receptacles, or unattended gasoline pumps. Keep track of all your paperwork. When you no longer need it, destroy it.
- Memorize your social security number and all of your passwords. Do not record them on any cards or anything in your wallet or purse.
- Sign all new credit cards upon receipt.
- Save all credit card receipts and match them against your monthly bills.

- Contact the sender if your routine financial statements are not received when expected.
- Notify credit card companies and financial institutions before you change address or phone number.
- Never loan your credit cards to anyone.
- Never put your credit card or other financial account number on a postcard or outside of an envelope.
- If you applied for a new credit card and it hasn't arrived in a timely manner, call the bank or credit card company involved.
- Report all lost or stolen credit cards immediately.
- Closely monitor expiration dates on your credit cards. Contact the credit card issuer if replacement cards are not received prior to the expiration dates.
- Beware of mail or telephone solicitations disguised as promotions offering instant prizes or awards designed solely to obtain your credit card numbers or other personal information.

Internet and On-Line Services

- Use caution when disclosing checking account numbers, credit card numbers or other personal financial data at any Web site or on-line service location unless you receive a secured authentication key from your provider.
- When you subscribe to an on-line service, you may be asked to give credit card information. When you enter any interactive service site, beware of con artists who may ask you to "confirm" your enrollment service by disclosing passwords or the credit card account number used to subscribe. **Don't give it out!**

If You Become a Victim of Identity Theft

- Contact all creditors by phone and in writing to inform them of the problem.
- Call the U.S. Postal Inspection Service at (877) 876-2455.
- Contact the Federal Trade Commission at (877) ID-THEFT (438-4338), to report the problem.
- Call the three credit bureaus' fraud units to report identity theft. Request a Fraud Alert/Victim Impact statement be placed in your credit file asking creditors to call you before opening new accounts:
Equifax Credit Bureau (800) 525-6285
Experian Information Solutions (888) 397-3742
TransUnion Credit Bureau (800) 680-7289
- Alert your banks to flag your accounts and contact you to confirm any unusual activity; request a change of PIN and a new password.
- Keep a log of all your contacts and make copies of all documents. You may also wish to contact a privacy or consumer advocacy group regarding illegal activity.
- Contact the Social Security Administration's Fraud Hotline (800) 269-0271.
- Contact the Department of Motor Vehicles to see if another license was issued in your name. If so, request a new license number and fill out a complaint form to begin the fraud investigation process.
- Contact TeleCheck at (800) 366-2425 and National Processing Co. at (800) 526-5380 if you have checks that have been fraudulently used.

On October 30, 1998, the Identity Theft and Assumption Deterrence Act of 1998 went into effect. The Act amends title 18 United States Code, Section, 1028, to address the problem of identity theft – the misappropriation of another person's identity for criminal purposes. The Act was needed since Section 1028 previously addressed only the fraudulent creation, use, or transfer of identification documents, and not the theft or criminal use of the underlying personal information. The Act criminalizes fraud in connection with unlawful theft and misuse of personal identifying information itself.