What is Identity Theft and Frequently Asked Questions

What Is Identity Theft?

Identity theft (also known as identity fraud) is the misappropriation of another person's identifying information in order to:

- obtain credit fraudulently from banks and retailers
- steal money from the victim's existing accounts
- apply for loans
- establish accounts with utility companies
- rent an apartment
- file for bankruptcy
- obtain a job
- achieve other financial gain using the victim's name

There Are Two Main Classes Of Economic Crime Related To Identity Theft:

1. Account takeover occurs when an identity thief acquires a person's existing credit or bank account information and either withdraws money or makes purchases. Victims usually learn of account takeover when they receive their monthly credit card or bank account statement.

2. In true identity theft, an identity thief uses another person's Social Security number and other identifying information to fraudulently open new accounts for financial gain. Victims may be unaware of the fraud for an extended period of time, which can allow the criminal to continue the ruse for months or even years.

FAQs

How Can A Criminal Steal My Identity?

An identity thief needs only a few strategic bits of information — your Social Security number, your birth date, perhaps your address and phone number — to commit fraud. With this and a fake driver's license (with the thief's picture where yours should be), the thief can often get instant credit in your name. The thief may provide his or her own address, claiming to have moved, and thus keeping you in the dark. The more accounts the thieves are able to open, the more "evidence" they have that your identity belongs to them.

Can You Determine Where The Identity Thief Got My Information?

We may learn the answer once the investigative phase of the victim assistance process has begun, but in many instances we can only guess where the breach occurred. Unfortunately, there are many sources for information that identity thieves can mine.

What Methods Do Identity Thieves Employ?

Theft of wallets and purses was once the most common way to obtain identity documents and account information. Today, identity thieves attack virtually every area of an individual's life, wherever personal information is stored or sent.

These are among the most common methods:

- Dumpster diving in trash bins for credit card statements, loan applications, and other documents containing names, addresses, account information, and SSNs.
- Stealing mail from unlocked mailboxes to get preapproved credit offers, credit cards, utility bills, bank and credit card statements, investment reports, insurance statements, benefits documents, and tax information.
- Impersonating a loan officer, employer, or landlord to get fraudulent access to credit files.
- Insider access to names, addresses, birth dates, and SSNs in personnel or customer files.
- Shoulder surfing at ATM machines and phone booths to capture PINs.
- Online sources of personal data, such as public records and fee-based information sites.

Are There Laws Against Identity Theft?

Yes. In 1998 Congress passed the Identity Theft and Assumption Deterrence Act (918 U.S.C. §1028), which makes it a federal felony to use another person's identification with the intent to commit unlawful activity. Federal agencies such as the Secret Service, the FBI, and the U.S. Postal Inspection Service investigate suspected violations of this law; the Department of Justice handles prosecutions. More recent federal legislation increases penalties for aggravated identity theft, workplace identity theft, or use of a stolen identity in connection with a terrorist act.

If I Become A Victim, Should I Still Worry About Protecting My Identity?

Yes. Without a disciplined approach to protecting your data, you risk repeated victimization.

If I Become A Victim, Will I Have To File A Police Report?

Yes. Contact your local police or the police in the community where the identity theft took place. Provide a copy of your ID Theft Complaint filed with Federal Trade Commission (FTC), to be incorporated into the police report. Get a copy of the police report or, at the very least, the number of the report.

What If The Police Won't Take A Report?

Some police departments may be reluctant to write a report on a crime of this kind, taking the position that since the creditor suffered the financial loss, you're not the victim. If the police are reluctant to take your report, ask to file a "Miscellaneous Incidents" report, or try another jurisdiction, like your state police. You can also check with your state Attorney General's office to find out if state law requires the police to take the reports for identity theft. Check www.naag.org for a list of state Attorney Generals.

What About Changing My Social Security Number?

In most cases, this is not advised. Over the years, that number has been attached to numerous documents, including credit reports and various other private and government records. Moreover, the Social Security Administration is reluctant to issue replacement Social Security numbers except in very complicated or extreme cases.

What Are The Risks Of Using The Internet And Other Networks?

There are three main threats to the data on your computer: malicious software, network intrusion by hackers, and physical theft.

To protect your computer against viruses, spyware, and Trojan horse programs (which let hackers control your computer), you must use antivirus software — and keep it updated. To keep intruders out, connect to the Internet through a properly configured firewall, which can be software or device-based; this is especially important if you have an "always on" Internet connection, such as a cable modem or DSL. Avoid using public computers for online banking, email account access, or other sensitive exchanges of information — keystroke loggers, web "cookies," or cached pages may be capturing your data. Similarly, be cautious in sending sensitive data over wireless networks. And be careful what you send via email — unencrypted text and attachments can be intercepted as they travel across the Internet.

Finally, beware of "phishing" and "pharming" scams, which use fake corporate email, redirected web addresses, and "cloned" corporate web pages to plant viruses and con users into providing sensitive information. Never provide identity or account information in response to an email, or if you have any doubt about the authenticity of a web site.