

# Identity Theft Frequently Asked Questions

[What is identity theft?](#)

[How can a criminal steal my identity?](#)

[Can you determine where the identity thief found my information?](#)

[If I become a victim, will you be able to solve my problem?](#)

[What methods do identity thieves employ?](#)

[Are there laws against identity theft?](#)

[If I become a victim, do I still have to worry about protecting my identity?](#)

[If I become a victim, will I have to file a police report?](#)

[What if the police won't take a report?](#)

[If I become a victim, will I need a lawyer?](#)

[If a criminal has taken my identity, should I cancel my credit cards?](#)

[What about changing my Social Security number?](#)

[What are the risks of using the Internet and other networks?](#)

[What else can I do to protect my computer and computerized data?](#)

## What is identity theft?

Identity theft 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; or
- Achieve other financial gain using the victim's name.

## There are two main classes of economic crime related to identity theft:

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 statement.

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.

## 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 criminal's picture where your picture should be), the thief can get instant credit in your name. The criminal may provide his or her own address, claiming to have moved, and thus keep you in the dark. The more accounts the criminals are able to open, the more "evidence" they have that your identity belongs to them.

## **Can you determine where the identity thief found 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 information sources for identity thieves to mine.

## **If I become a victim, will you be able to solve my problem?**

For the most part, the answer is “Yes” – but with important qualifications. Normally, it is possible to guide identity theft victims systematically through the crisis period, enabling them to reclaim their identities and regain their financial security. However, many cases of identity theft entail the risk of recurrence. In particular, if your Social Security number has been misused, you should never consider yourself impervious to future abuse.

## **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 Social Security numbers
- 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 SSN’s in personnel or customer files
- Shoulder surfing at ATM machines and phone booths to capture Personal Identification Numbers (PIN)
- 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 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 stolen identity in connection with a terrorist act.

## **If I become a victim, do I still have to 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. You must file a police report and sign the Federal Trade Commission’s Identity Theft Affidavit to be accepted as a new victim account.

### **What if the police will not take my report?**

Some police departments may be reluctant to write a report on crime of this kind, taking the position that since the creditor suffered the financial loss, you are not the victim. They may insist that the creditor file the complaint. The creditor, however, may choose not to cooperate, calculating that it is not cost-effective to spend time and energy assisting the police. Nevertheless, even if the creditor will not prosecute, insist that the police take a report.

### **If I become a victim, will I need a lawyer?**

Possibly, but it is unlikely. Some identity theft victims do require services that can only be performed by an attorney. Such services normally involve going to court to remove liens placed due to fraud and/or criminal warrants resulting from the stolen identity.

### **If a criminal has taken my identity, should I cancel my credit cards?**

The best course of action depends on your circumstances. Your goal is to reduce the risk that a given account will be abused, while maximizing your own ability to use your existing credit accounts. In weighing risks and benefits, keep in mind that if you have recently become an identity theft victim, your situation may make it difficult to obtain new credit in the future.

Rather than canceling accounts, you may wish to notify the fraud department for each account and have a fraud alert placed. If a credit or debit card (or the data on it) has been lost or stolen, you may wish to cancel that card and have a new card issued that is based on the same account, but has a different number. If you have multiple credit cards, you may decide to cancel some to reduce your exposure. In any event, instruct credit card issuers and banks not to change your address without direct verification from you, in writing that originates from your present address. You should also monitor closely the monthly statements from any credit card or bank accounts you do decide to keep active.

### **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.

## What else can I do to protect my computer and computerized data?

- **Limit access to your computer to those you truly trust** - Use restrictive permission levels to protect sensitive files. Encrypt files containing sensitive information whenever possible, including backup files. And don't forget to protect your computer against physical theft – “password protection” sounds daunting, but is actually easy for a tech-savvy criminal to defeat. Use anti-virus, anti-spyware security software that updates automatically, and keep it active and current.
- **Use your computer wisely** – Turn off your computer when you are not using it. Avoid using public computers at libraries, hotels or airports for conducting personal or financial business.
- **Keep your passwords safe** – Don't share them with anyone (via the internet, over the phone, or through email) or commit them to writing.
- **Guard your personal information** – Do not reply to an email or pop-up message that asks for personal financial information and do not click on links within the message. Do not respond if you receive a message that asks you to call a phone number to update your account or provide personal information to claim a refund, prize or some other unexpected cash.
- **Monitor your credit report** – Obtain an annual FREE credit report at [www.annualcreditreport.com](http://www.annualcreditreport.com).

## Contact Us

If you feel that you are a victim of Identity Theft, please contact us at: [custserv@firstfederalbank.net](mailto:custserv@firstfederalbank.net)