



How can I protect myself from
Identity Theft?

What Is Identity Theft?

Identity theft is the unlawful use of another person's identification. Identity theft may take many forms. Common methods of identity theft include credit card or other bank fraud, phone or utility service theft, and the taking of government documents or benefits. However, thieves are finding new ways of using the identity of their victims every day.

How Does Identity Theft Occur?

Surprising to most people is that identity theft is actually a very easy crime to commit. In fact, over 1,400 people are victimized each day. That being the case, it is important for you to know how these thieves operate so you can protect your personal information.

At the heart of the crime is the thief obtaining information that most people would assume only the true owner of the information would know. Common examples are social security numbers, driver's license numbers, bank account numbers, mother's maiden names, and passports.

Thieves obtain this information in numerous ways. Some thieves will steal wallets, purses, and even mail. Others will listen and/or watch a person conduct personal business, such as talking on the telephone or getting cash from an automated teller machine. Thieves will also deceive or trick people into disclosing personal information through phone scams, via the mail, or on the Internet.

Very aggressive thieves will even obtain personal information by using a process referred to as "pretext calling." Pretext calling occurs when an individual contacts an entity in possession of a customer's personal information and cons the entity in to releasing the information by acting as the customer or

someone authorized to have the customer's information.

Once a thief has possession of the information, the thief will apply for credit cards, loans, phone services, or just about any other service where economic gain can be realized without actual payment. When applying for credit cards, loans, or other services, thieves will often intentionally use incorrect addresses or complete change of address forms on existing accounts so that the victim will not be immediately aware of the crime.

How Does Identity Theft Affect Me?

Identity theft can cause its victims numerous problems. Most significantly, it can destroy the financial history you have worked so hard to obtain. Repairing your credit history can require significant time and money. Thieves can even file for bankruptcy in your name.

Since thieves use a "purchase now, pay later" approach, you may not be able to stop a thief until thousands of dollars of debt have been attributed to you. Also, because thieves often try to prevent bills from reaching you by either changing the address on your account or creating a new account with a false address, you may not know that your identity is being used by a thief for months or even years. By this time, your financial history could be ruined.

How Can My Financial Institution Help Protect My Identity?

The Gramm-Leach-Bliley Act directs the Board of Governors of the Federal Reserve System and other federal agencies to ensure that financial institutions have policies, procedures, and controls in place to prevent

the unauthorized disclosure of customer financial information, and to deter and detect fraudulent access to such information.

We have adopted numerous policies and practices to help protect your personal information. For example, we have:

- Taken steps to verify the identity of new account and loan applicants
- Established fraud prevention procedures, such as training our employees to identify common criminal practices, including the submission of change of address forms with credit or debit card applications
- Established a comprehensive information security program
- Established written policies and procedures to control access to customer information

How Can I Protect Myself From Identity Theft?

The following list of tips is not exclusive, but should give you a good start in identifying ways to protect your personal information and data.

- Closely monitor your credit card and financial institution account activity
- Watch what you discard, how you discard it, and where you discard it
- Dispose of utility bills, credit card statements, insurance information, doctor bills, bank statements, and investment updates carefully

- Tear everything before disposing of it, especially preapproved credit card solicitations; even consider a paper shredder
 - Don't use disposal units that offer ready access to people you do not know or trust
 - If your disposal service has curbside pick up, consider putting the trash out first thing in the morning rather than the night before
 - Watch what information you give out to others on the phone and over the Internet
 - Pay close attention to whom you give your personal information. Always ask yourself: Who really needs to know your social security number, driver's license number, passwords, personal identification numbers (PINs), account numbers, date of birth, or mother's maiden name?
 - Guard your personal information
 - Limit the information on your personal checks (for example, driver's license number, social security number, and address)
 - Do not give someone you do not know or trust your deposit or withdrawal slips or your checks
 - Keep your credit card receipts in a safe place—don't leave receipts in your shopping bags
 - Do not carry around your social security card
-

- Only give personal information to web sites that use encryption or other secure methods to protect your information
- Use a firewall if you have a high speed Internet connection; Firewall software can be purchased on-line or at most computer software retail locations
- Have the United States Postal Service hold your mail when you are on vacation, or have a close friend or relative pick it up each day
- Deposit bills and other items in the mail at a United States Postal Service drop box or at a United States Postal Service facility rather than curbside
- If you use a curbside or rural mailbox, consider putting your mail out in the morning rather than leaving it in the box overnight
- Do **not** use passwords on your accounts that are easy to guess (for example, do not use a date of birth, child's name, or pet name)

What Should I Do If My Identity Has Been Stolen?

In the event that you suspect your identity has been stolen or you are, in fact, certain that it has been stolen, follow these simple steps:

- 1) Immediately contact the Federal Trade Commission:
 - <http://www.ftc.gov>
 - 1-877-IDTHEFT (877-438-4338)

- Consumer Response Center, F.T.C., 600 Pennsylvania Avenue NW, Washington, DC 20580
- 2) Contact the three major credit reporting agencies to put yourself on Fraud Alert and request a copy of your credit report:
 - Equifax®—P.O. Box 740250, Atlanta, GA 30374-0250 or call 800-525-6285
 - Experian®—P.O. Box 1017, Allen, TX 75013 or call 888-EXPERIAN (888-397-3742)
 - TransUnion—P.O. Box 6790, Fullerton, CA 92634 or call 800-680-7289
 - 3) Cancel all accounts that have fraudulent activity or are at risk
 - 4) Contact your local law enforcement agency
 - 5) If your mail has been stolen, contact the United States Postal Service
 - 6) Keep detailed records of your efforts to resolve any theft of your identity
 - Log the date, time, and amount of any unauthorized activity on your accounts
 - Log the date, ~~time~~, duration, and cost of any phone calls
 - Log the date and cost of any mailings