

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) Contact the fraud department of at one of the following three major credit reporting agencies and ask that a fraud alert be placed in your credit file and for a free credit report (to be on the safe side, you may wish to contact all three):
 - **Equifax**® - 1-800-525-6285
P.O. Box 740241
Atlanta, GA 30374-0241
www.equifax.com
 - **Experian**® - 1-888-EXPERIAN (397-3742)
P.O. Box 9532
Allen, TX 75013
www.experian.com/fraud
 - **TransUnion**® - 1-800-680-7289
Fraud Victim Assistance Division
P.O. Box 6790
Fullerton, CA 92834-6790
www.transunion.com
Fraud victims only fvad@transunion.com
- 2) Close all accounts that are or may be affected by the identity theft.

Also regarding any checking accounts thus closed, contact the following major check verification companies and ask that retailers using their databases not accept checks drawn on the closed accounts:

- **TeleCheck**® - 1-800-710-9898 or 927-0188
- **Certegy, Ins.**® - 1-800-437-5120
- **International Check Services**® - 1-800-631-9656

- 3) File a police report and obtain a copy for submission to credit reporting agencies, creditors and others.
- 4) Contact the Federal Trade Commission to report the theft and to obtain further guidance as to how to protect yourself:
 - www.consumer.gov/idtheft
 - 1-877-IDTHEFT (438-4338)
 - Identity Theft Clearinghouse
Federal Trade Commission
600 Pennsylvania Avenue NW
Washington, DC 20580
- 5) If you know or suspect that your mail has been stolen, contact the United States Postal Service.
- 6) Keep detailed records of any theft of your identity and of your efforts to resolve the same. Log the date, time and amount of any unauthorized activity on your accounts. Log the date, time, duration and cost of any phone calls and of any mailings and keep copies.

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 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.

What are we doing to prevent fraud?

After September 11, legislation was passed to help prevent fraud. Evidence shows that credit card, debit card and similar fraud is a major source of funding for terrorists. To help prevent you from becoming a victim of fraud, all financial institutions are required to carefully verify the identity of our account owners, loan applicants, trust and individuals who purchase investment products.

This means we may ask you additional questions at the time of your transaction. We may also ask you to provide one or more types of identification (ID), such as driver's license, U.S. taxpayer ID number or other government-issued document that verifies your nationality or residence. By answering these questions and providing the required forms of identification, you can help us meet the requirements and better protect you against identity theft.

How does identity theft occur?

Surprising to most people is that identity theft is actually a very easy crime to commit.

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, financial institution 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 automatic teller machine. Thieves will also deceive or trick people into disclosing personal information through phone scams, via the mail or on the Internet.

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 use incorrect addresses or complete change of address forms on existing accounts so the victim will not be immediately aware of the crime.

Identity theft can cause its victims numerous problems. Most significantly, it can destroy the financial history you have worked so hard to obtain.

How can I protect myself from identity theft?

The following are just some of the ways you can reduce the risk of identity theft:

- Keep your credit cards, debit cards, personal identification numbers (PINs) and other passwords, checks, social security cards, other cards or documents which bear your social security number, health insurance cards, driver's license and number and other personal information where they will be safe. When disposing of these items, do so by shredding.
- Keep your deposit and withdrawal slips, credit card purchases receipts, financial institution statements, credit card statements, utility bill, medical bills, insurance information, investment updated and credit card solicitations where they will be safe. When disposing of them, do so by shredding.
- Mail bill payments and other items that contain personal information at a U.S. Postal Service drop box rather than in your curbside mailbox. Don't put any mail in your curbside mailbox until shortly before it will be picked up.
- Take your mail out of your curbside mailbox as soon as possible after it has been delivered. If you are traveling, have the U.S. Postal Service hold your mail or have someone you trust pick it up daily.
- Don't give any of your personal information in person, over the telephone or over the Internet to anyone - unless you have a very good reason to trust them.
- Don't give any of your personal information in response to an unsolicited e-mail claiming to be from your financial institution or some highly credible source. This is a technique referred to as "phishing." Be sure to validate the request before providing the information (for example, contact the customer service telephone number on your account statement to ask about the request).
- Don't give any of your personal information to any web sites that do not use encryption or other secure methods to protect it.
- Don't use PINs or passwords that are easy to guess (for example, don't use birth dates, spouse or child names).
- Examine your credit card and financial institution statements immediately upon receipt to determine whether there were any unauthorized transactions. Report any that you find immediately to the financial institution.
- Make a prompt inquiry if bills or statements are not received in a timely fashion - this could mean that they are being diverted by an identity thief.
- Obtain copies of your credit report annually from each of the three major credit reporting agencies (Equifax®, 1-800-685-1111; Experian®, 1-888-397-3742; TransUnion®, 1-800-888-4213) to be sure that they are accurate.