



Identity Theft



Please note that this Information Paper only provides basic information and is not intended to serve as a substitute for personal consultations with a Legal Assistance Attorney.

INTRODUCTION

In the course of a busy day, you may rent a car, mail your tax returns, change service providers for your cell phone, or apply for a credit card. In each transaction, you reveal bits of personal information, such as your bank and credit card account numbers; your income; your Social Security number (SSN); and your name, address, and phone number. In the wrong hands, that information can be used to commit fraud or theft.

Identity theft is a serious crime. People whose identities have been stolen can spend time and money cleaning up the mess that thieves have made of their good name and credit record. They may also be denied job opportunities, and loans for education, housing, or vehicles. Although you cannot completely protect yourself from identify theft, there are measures you can take to reduce your risk.

HOW IDENTITY THEFT OCCURS

Skilled identity thieves use a variety of means to access to your personal information. These include stealing your wallet or purse, obtaining your credit report by posing as a landlord or someone else who may have a legal right to that report, stealing your mail, and “dumpster diving.”

Once identity thieves have your personal information, they may use it to commit fraud or theft. For example, they may open new credit card accounts in your name; change the billing address on your already-existing credit card accounts; open bank accounts in your name and write bad checks; counterfeit checks or credit or debit cards, or authorize electronic transfers in your name, and drain your bank account; or get a job or file fraudulent tax returns in your name.

IF YOUR PERSONAL INFORMATION HAS BEEN LOST OR STOLEN

You can minimize the risk of identity theft if you act quickly.

1) Contact your bank and credit card companies. Consider closing those accounts and, when opening new accounts, create new passwords. Further, when creating passwords, avoid using common choices, such as your mother’s maiden name or your birth date.

2) Contact the three nationwide consumer reporting agencies (page 2). Place an initial fraud alert on your credit reports. An alert can help stop someone from opening new credit accounts in your name.

3) Contact any government agencies who have issued you identification cards. Follow their procedures to cancel those documents and receive replacements. Request that each respective agency flag your file so that no one else may receive an identification document in your name.

4) Watch for signs that your information is being misused.

If an identity thief is opening new credit accounts in your name, those accounts are likely to show up on your credit report. You can order your credit report from the three nationwide consumer reporting companies, which are listed below. Monitor the balances of your financial account, and watch for unexplained charges or withdrawals. Other indications of identity theft include failure to receive bills or mail; receiving credit cards for which you did not apply; denial of credit for no apparent reason; receiving calls from debt collectors or companies regarding items you did not buy.

If your information has been misused, file a report with the police, and file a complaint with the Federal Trade Commission (FTC).

IDENTITY THEFT VICTIMS: IMMEDIATE STEPS

If you are a victim of identity theft, take the following four steps as soon as possible, and keep records of your conversations and copies of all correspondence. Additionally, obtain a copy of the FTC publication, *Take Charge: Fighting Back Against Identity Theft*, which further describes what to do in such a situation. The guide also includes an ID Theft Affidavit, which many companies will ask you to use in reporting relevant information. For more information, see www.consumer.gov/idtheft.

1. Place a fraud alert on your credit reports, and review your credit reports.

Fraud alerts can help prevent an identity thief from opening any more accounts in your name. Contact the toll-free fraud number of any of the three consumer reporting companies below to place a fraud alert on your credit report. You need to contact only one of the three companies to place an alert. The company you call is required to contact the other two, which will also place an alert on their versions of your report.

- **Equifax:** 1-800-525-6285; www.equifax.com; P.O. Box 740241, Atlanta, GA 30374-0241
- **Experian:** 1-888-EXPERIAN (397-3742); www.experian.com; P.O. Box 9532, Allen, TX 75013
- **TransUnion:** 1-800-680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790

Once you place the fraud alert, you are entitled to order free copies of your credit reports. You can also request that only the last four digits of your SSN appear on your credit reports. Once you receive your credit reports, review them carefully. Look for inquiries from companies that you have not contacted, accounts you did not open, and debts on your accounts that you cannot explain. Verify information such as your SSN, address(es), name or initials, and employers. If you find fraudulent or inaccurate information, contact the consumer reporting companies. Continue to check your credit reports periodically, particularly during the first year after you discover the identity theft.

2. Close the accounts that you know or believe have been tampered with or opened fraudulently.

Call and speak to someone in the security or fraud department of each company. Follow up in writing, and include copies (NOT originals) of supporting documents. *It is important to notify credit card companies and banks in writing.* Send your letters by certified mail, return receipt requested, so you can document what the company received and when. Keep a file of your correspondence and enclosures.

When you open new accounts, use new Personal Identification Numbers (PINs) and passwords. Avoid using easily available information like your mother's maiden name or your birth date.

If the identity thief has made charges or debits on your accounts, or on fraudulently opened accounts, ask the company for the forms to dispute those transactions.

For charges and debits on existing accounts, ask the representative to send you the company's fraud dispute forms. If the company does not have special forms, write a letter to dispute the fraudulent charges or debits. In either case, write to the company at the address given for "billing inquiries" (NOT the address for sending your payments).

For new unauthorized accounts, ask if the company accepts the ID Theft Affidavit. If not, ask the representative to send you the company's fraud dispute forms. If the company already has reported these accounts or debts on your credit report, dispute this fraudulent information.

Once you have resolved your identity theft dispute with the company, ask for a letter stating that the company has closed the disputed accounts and has discharged the fraudulent debts. This letter is your best proof if errors relating to this account reappear on your credit report or you are contacted again about the fraudulent debt.

3. File a report with your local police or the police in the community where the identity theft took place.

After doing so, obtain a copy of the police report, or at the very least, the number of the report. It can help you communicate with creditors who need proof of the crime. If the police are reluctant to take your report, ask to file a "Miscellaneous Incidents" report, or try another jurisdiction, such as your state police. You also can check with your state Attorney General's office to find out if state law requires the police to take reports for identity theft. Check the Blue Pages of your telephone directory for the phone number or go to www.naag.org for a list of state Attorneys General.

4. File a complaint with the Federal Trade Commission.

By sharing your identity theft complaint with the FTC, you will provide important information that can help law enforcement officials across the nation track down identity thieves.

You can file a complaint online at www.consumer.gov/idtheft. Alternatively, you can call the FTC's Identity Theft Hotline, toll-free: 1-877-ID-THEFT (438-4338); TDD: 202-326-2502; or write: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Be sure to call the Hotline to update your complaint if you have any additional information or problems.

ACTIVE DUTY FRAUD ALERTS

If you are a member of the military and away from your usual duty station, you may place an active duty alert on your credit reports. To do so, contact any one of the three major consumer reporting companies (page 2). Active duty alerts can help minimize the risk of identity theft while you are deployed. When a business sees the alert on your credit report, it must verify your identity before issuing any credit.

To place an alert on your credit report, or to have it removed, you will need to provide appropriate proof of your identity, including your SSN, name and address. You may use a personal representative to place or remove an alert. Active duty alerts remain in effect for one year, unless you request that it be removed earlier. If your deployment lasts longer than one year, you may place another alert on your credit report.

For further information or help feel free to make an appointment with a Legal Assistance Attorney, DSN 421-4152, Civ 0711-729-4152.

REVIEWED BY: CPT Sean A. Marvin, Chief, Legal Assistance
DATE: 16 November 2010

References:

Federal Trade Commission Website - <http://www.consumer.gov/idtheft/>

JAG Website - <http://www.jagcnet.army.mil/legal> (click on Money Matters, followed by Personal Financial Privacy Information, and then scroll down until you see Identity Theft)