

## **What is Identity Theft?**

Identity theft occurs when someone uses your name, Social Security number, credit card number or some other piece of your personal information to apply for a credit card, make unauthorized purchases, gain access to your bank accounts or obtain loans under your name. Unfortunately, most people do not know that they have been victims of identity theft until mysterious charges appear on their credit card bills or they are rejected for a mortgage because unpaid bills appear on their credit report.

## **Types of Identity Theft:**

### **Social Security Number**

Your Social Security number is the most valuable piece of your personal financial information because it is your main identifying number for employment, tax reporting, and credit history tracking purposes. If your Social Security number falls in the hands of a thief, you could face serious problems as a result. A thief could use your Social Security number to obtain employment, open credit card accounts or obtain loans under your name. The best way to protect yourself is to guard your Social Security number and provide it to others only when absolutely necessary. Some businesses request your Social Security number for general record keeping. If they do, ask how your Social Security number will be used and whether you can use any other identifying number instead.

If your Social Security number is stolen, applying for a new one may not solve your identity theft problem. For example, a new Social Security number may not ensure a new credit record because credit bureaus may combine the credit records from your old Social Security number with your new one. Moreover, even when the old credit history is not associated with your new Social Security number, the absence of any credit history under your new Social Security number may make it more difficult to obtain credit.

### **Credit Cards**

There are numerous ways in which an identity thief can make unauthorized charges on your existing credit card accounts, or open up new accounts under your name. An ordinary thief might steal your wallet or purse and try to make use of your stolen cards and checks. The more sophisticated thief can fill out a change of address form from the post office to get all your bills sent to another address. He or she can also call your credit card issuer and, pretending to be you, change the mailing address on your credit card accounts. The impostor then runs up charges on your account. Since your bills are being sent to a new address, you may not immediately realize the problem. An identity thief might also open new accounts under your name by stealing and completing a pre-approved credit card offer sent to you in the mail, using your name, date of birth and Social Security number, but a different address, on the application form. If this occurs, you may not discover that a new account has been opened under your name until the unpaid bills appear on your credit report.

Identity thieves can also obtain your credit card information from purchases you make at stores, over the telephone or online. For example, the credit card information you provide in person or over the telephone during a purchase can be improperly used to make unauthorized charges on your account. In addition, thieves can obtain your credit card number and other personal information through fraudulent or unsecured Web sites. No matter how professional looking the Web site, check the company's reliability with the Better Business Bureau before doing business with it, review the Web site's security policy, and be sure to use a secure browser if you are providing credit card information online. In the address window of your browser, check to see that the first part of the company's Web address changes from "http://" to "https://;" and also check the lower corner of the Web page to see whether a lock or key symbol appears, signifying security. Using a secure browser helps to ensure the safety of your personal data when it is being transmitted to a company's computers.

Before making online purchases, check the Web site's user agreement and privacy policy to find out how the company uses your credit card and other personal information. The user agreement and privacy policy will inform you whether the information you provide is stored in the company's database and whether you can opt out of being added to the company's mailing list or having the company share your personal information with a third party. Privacy Seal programs, such as the

Better Business Bureau's BBBOnline program, provide seals for Web sites that have met certain standards for protecting the privacy of the consumer information that they collect.

## **Check Fraud**

Identity thieves can drain your checking account by stealing your checks or your checking account number from your home or office and forging your signature, or by making counterfeit checks in your name, using a home computer. Some thieves even use cleaning solvent to remove what is already written on a check, making it payable to themselves. If your checks have been stolen or misused, immediately notify your bank, place a stop payment order, and close your checking account.

Be aware that identity thieves can also open checking accounts in your name using personal information such as your Social Security number. When they write bad checks on that account, those debts appear on your credit report.

## **Cellular Telephone Service**

Identity thieves can establish new cellular telephone service in your name or make unauthorized calls that seem to come from, and are billed to, your cellular phone. Others make unauthorized charges by using your calling card and PIN. If this occurs, contact your service provider to close your existing account, and establish another one with a new PIN.

## **Prevention**

Although there is no method for guaranteeing that identity theft will never happen to you, below are tips that can help you minimize your risk:

- Carry only the cards you actually need. Minimize the identification information and the number of cards you carry in your wallet or purse. Do not carry your Social Security card unless you need it.
- Never put your account information on the outside of an envelope or on a postcard.
- Cut up old or expired credit cards. Close all inactive credit card and bank accounts. Even though you do not use them, these accounts appear on your credit report and may be used by thieves.
- For your ATM card, choose a Personal Identification Number (PIN) different from your address, telephone number, middle name, the last four digits of your Social Security number, your birth date or any other information that could be easily discovered by thieves.
- Memorize your PIN; do not write it on your ATM card or keep it written on a piece of paper somewhere in your wallet. Statistics show that in many instances of ATM card fraud, cardholders wrote their PINs on their ATM cards or on slips of paper kept with their wallets or purses.
- Keep personal information in a safe place. If you employ outside help or are having service work done in your home, keep your personal information out of sight.
- Give your Social Security number only when absolutely necessary. Ask to use another type of identifying number whenever possible.
- Do not give out personal information over the phone, through the mail, or over the Internet unless you have initiated contact or know the business with which you are dealing.
- Compare your ATM receipts and cashed checks with your periodic bank statements to check for unauthorized transfers or charges.
- Shred credit card statements, bank statements and pre-approved credit offers when you do not need them. Consider investing in a paper shredder.
- Decrease the number of unsolicited credit card applications that you receive. The fewer credit card applications you receive, the less likely it is that one will be stolen. Call (888) 5OPT-OUT to have your name removed from the marketing lists sold by the major credit bureaus for two years, or removed permanently.
- Ask your bank about its privacy policies and information practices. Find out the circumstances under which your bank would provide your account information to a third party.
- Order a copy of your credit report from the three credit reporting agencies at least once every year to review your file for possible fraud.

## **Correcting the Action**

The most important thing to do when you discover identity fraud is to take action right away. Remember to keep records of all your telephone calls and other correspondence with companies regarding the identity fraud.

- File a report with your local police or the police in the community where the identity theft took place. Keep a copy of the police report and make note of the date of your report, in case your bank, credit card company or other company needs proof of the crime.
- If you suspect that your mail is being diverted to another address, check with your local post office to see whether an unauthorized change of address form has been filed under your name.
- Call your credit card issuers right away to check on the status of your accounts if your bills do not arrive on time. If necessary, close all your accounts. You should keep a record in a safe place, separate from your credit cards, of your account numbers, expiration dates, and the telephone numbers of each card issuer so you can report a loss quickly.
- Notify your bank at once if your ATM card has been stolen or if unauthorized transfers and withdrawals have been made on one or more of your accounts. Alert your bank if your checks are stolen or missing. When you open new bank accounts, ask that a password be used before any inquiries or changes can be made to the accounts and avoid using a PIN that may be discovered by a thief, such as your birth date or the last four digits of your Social Security number.
- Canceling your credit cards may stop impostors from using your existing accounts, but it does not stop them from opening new accounts under your name. To prevent this from occurring, if your cards may have been misused by an unauthorized party, contact the fraud departments of each of the three major credit bureaus and ask them to "flag" your file as one belonging to a possible fraud victim. This warning will include a statement that creditors should call to get your permission before approving new credit cards or loans in your name. After calling each of the three credit bureaus (listed in the Resources section of this report), you should follow up with them in writing. Keep copies of such written notices.
- Ask the credit bureaus for copies of your credit reports. You are entitled to a free copy of your credit report if you were recently denied credit or if your report is inaccurate because of fraud. Review your report carefully to make sure no unauthorized charges were made on your existing accounts and that no fraudulent accounts or loans were established in your name. In a few months, order new copies of your credit reports to verify that the inaccurate information has been removed and no new fraudulent activity has occurred.
- Contact each of the creditors for any accounts that were tampered with or falsely established in your name. Ask to speak with someone in the security or fraud department. According to the **Fair Credit Reporting Act**, you must follow up the calls with a letter to the creditor. When writing to a credit card company, be sure to send the letter to the address provided to report billing errors. Do not send it to the address where you send payments, unless you are directed to do so.