Identity Theft

INTRODUCTION

In the course of a busy day, you may write a check at the grocery store, charge tickets to a ball game, rent a car, mail your tax returns, call home on your cell phone, order new checks or apply for a credit card. Chances are you don't give these everyday transactions a second thought. But someone else may.

The 1990's spawned a new variety of crooks called identity thieves. Their stock in trade are your everyday transactions. Each transaction requires you to share personal information: your bank and credit card account numbers; your income; your Social Security number (SSN); and your name, address and phone numbers. An identity thief co-opts some piece of your personal information and appropriates it without your knowledge to commit fraud or theft. An all-too-common example is when an identity thief uses your personal information to open a credit card account in your name.

Can you completely prevent identity theft from occurring? Probably not, especially if someone is determined to commit the crime. But you can minimize your risk by managing your personal information wisely, cautiously and with heightened sensitivity.

The Congress of the United States asked the Federal Trade Commission to provide information to consumers about identity theft and to take complaints from those whose identities have been stolen. If you've been a victim of identity theft, you can call the FTC's Identity Theft Hotline toll-free at 1-877-IDTHEFT (438-4338). The FTC puts your information into a secure consumer fraud database and may, in appropriate instances, share it with other law enforcement agencies and private entities, including any companies about which you may complain.

In addition, the FTC has developed the ID Theft Affidavit – a form you can use to alert companies where a new account was opened in your name. A copy of the ID Theft Affidavit is in this booklet. The company can then investigate the fraud and decide the outcome of your claim. You can find a list of some of the companies and organizations that accept or endorse the ID Theft Affidavit at www.consumer.gov/idtheft

The FTC, working in conjunction with other government agencies, has produced this booklet to help you guard against and recover from identity theft.

HOW IDENTITY THEFT OCCURS

Despite your best efforts to manage the flow of your personal information or to keep it to yourself, skilled identity thieves may use a variety of methods - low- and hi-tech - to gain access to your data. Here are some of the ways imposters can get your personal information and take over your identity.

How identity thieves get your personal information:	How identity thieves use your personal information:

They steal wallets and purses containing your identification and credit and bank cards. They steal your mail, including your bank and credit card statements, pre-approved credit offers, telephone calling cards and tax information. They complete a "change of address form" to divert your mail to another location. They rummage through your trash, or the trash of businesses, for personal data in a practice known as "dumpster diving." They fraudulently obtain your credit report by posing as a landlord, employer or someone else who may have a legitimate need for — and a legal right to — the information. They get your business or personnel records at work. They find personal information in your home. They use personal information you share on the Internet. They buy your personal information from "inside" sources. For example, an identity thief may pay a store employee for information about you that appears on an application for goods, services or credit.	They call your credit card issuer and, pretending to be you, ask to change the mailing address on your credit card account. The imposter then runs up charges on your account. Because your bills are being sent to the new address, it may take some time before you realize there's a problem. They open a new credit card account, using your name, date of birth and SSN. When they use the credit card and don't pay the bills, the delinquent account is reported on your credit report. They establish phone or wireless service in your name. They open a bank account in your name and write bad checks on that account. They file for bankruptcy under your name to avoid paying debts they've incurred under your name, or to avoid eviction. They counterfeit checks or debit cards, and drain your bank account. They buy cars by taking out auto loans in your name.

MINIMIZE YOUR RISK

While you probably can't prevent identity theft entirely, you can minimize your risk. By managing your personal information wisely, cautiously and with an awareness of the issue, you can help guard against identity theft:

- Before you reveal any personally identifying information, find out how it will be used and whether it will be shared with others. Ask if you have a choice about the use of your information: can you choose to have it kept confidential?
- Pay attention to your billing cycles. Follow up with creditors if your bills don't arrive on time. A missing credit card bill could mean an identity thief has taken over your credit card account and changed your billing address to cover his tracks.

- Guard your mail from theft. Deposit outgoing mail in post office collection boxes or at your local post office. Promptly remove mail from your mailbox after it has been delivered. If you're planning to be away from home and can't pick up your mail, call the U.S. Postal Service at 1-800-275-8777 to request a vacation hold. The Postal Service will hold your mail at your local post office until you can pick it up.
- Put passwords on your credit card, bank and phone accounts. Avoid using easily available information like your mother's maiden name, your birth date, the last four digits of your SSN or your phone number, or a series of consecutive numbers.
- Minimize the identification information and the number of cards you carry to what you'll actually need.
- Do not give out personal information on the phone, through the mail or over the Internet unless you have initiated the contact or know who you're dealing with. Identity thieves may pose as representatives of banks, Internet service providers and even government agencies to get you to reveal your SSN, mother's maiden name, financial account numbers and other identifying information. Legitimate organizations with whom you do business have the information they need and will not ask you for it.
- Keep items with personal information in a safe place. To thwart an identity thief who may pick through your trash or recycling bins to capture your personal information, tear or shred your charge receipts, copies of credit applications, insurance forms, physician statements, bank checks and statements that you are discarding, expired charge cards and credit offers you get in the mail.
- Be cautious about where you leave personal information in your home, especially if you have roommates, employ outside help or are having service work done in your home.
- Find out who has access to your personal information at work and verify that the records are kept in a secure location.
- Give your SSN only when absolutely necessary. Ask to use other types of identifiers when possible.
- Don't carry your SSN card; leave it in a secure place.
- Order a copy of your credit report from each of the three major credit reporting agencies every year. Make sure it is accurate and includes only those activities you've authorized. The law allows credit bureaus to charge you up to $9.00 for a copy of your credit report.

Your credit report contains information on where you work and live, the credit accounts that have been opened in your name, how you pay your bills and whether you've been sued, arrested or filed for bankruptcy. Checking your report on a regular basis can help you catch mistakes and fraud before they wreak havoc on your personal finances. See "Credit Reports" for details about removing fraudulent and inaccurate information from your credit report.

A SPECIAL WORD ABOUT SOCIAL SECURITY NUMBERS

Your employer and financial institution will likely need your SSN for wage and tax reporting purposes. Other private businesses may ask you for your SSN to do a credit check, such as when you apply for a car loan. Sometimes, however, they simply want your SSN for general record keeping. You don't have to give a business your SSN just because they ask for it. If someone asks for your SSN, ask the following questions:

- Why do you need my SSN?
- How will my SSN be used?
- What law requires me to give you my SSN?
- What will happen if I don't give you my SSN?

Sometimes a business may not provide you with the service or benefit you're seeking if you don't provide your SSN. Getting answers to these questions will help you decide whether

you want to share your SSN with the business. Remember, though, that the decision is yours.

CREDIT BUREAUS

Equifax – www.equifax.com
To order your report, call: 800-685-1111 or write:
P.O. Box 740241, Atlanta, GA 30374-0241
To report fraud, call: 800-525-6285/ TDD: 800-255-0056 and write: P.O. Box 740241, Atlanta, GA 30374-0241

Experian – www.experian.com
To order your report, call: 888-EXPERIAN (397-3742) or write: P.O. Box 2104, Allen, TX 75013
To report fraud, call: 888-EXPERIAN (397-3742)/ TDD:
800-972-0322 and write: P.O. Box 9532, Allen, TX 75013

TransUnion – www.transunion.com
To order your report, call: 800-916-8800 or write:
P.O. Box 1000, Chester, PA 19022
To report fraud, call: 800-680-7289/ TDD:
877-553-7803 and write: Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92634-6790

CHOOSING TO SHARE YOUR PERSONAL INFORMATION — OR NOT

What happens to the personal information you provide to companies, marketers and government agencies? They may use your information just to process your order. They may use it to create a profile about you and then let you know about products, services or promotions. Or they may share your information with others. More organizations are offering consumers choices about how their personal information is used. For example, many let you "opt out" of having your information shared with others or used for promotional purposes.

IF YOU'RE A VICTIM

Sometimes an identity thief can strike even if you've been very careful about keeping your personal information to yourself. If you suspect that your personal information has been hijacked and misappropriated to commit fraud or theft, take action immediately, and keep a record of your conversations and correspondence. You may want to use the attached form [PDF only]. Exactly which steps you should take to protect yourself depends on your circumstances and how your identity has been misused. However, three basic actions are appropriatein almost every case.

Your First Three Steps

First, contact the fraud departments of each of the three major credit bureaus.

Tell them that you're an identity theft victim. Request that a "fraud alert" be placed in your file, as well as a victim's statement asking that creditors call you before opening any new accounts or changing your existing accounts. This can help prevent an identity thief from opening additional accounts in your name.

At the same time, order copies of your credit reports from the credit bureaus. Credit bureaus must give you a free copy of your report if your report is inaccurate because of fraud, and you request it in writing. Review your reports carefully to make sure no additional fraudulent accounts have been opened in your name or unauthorized changes made to your existing accounts. Also, check the section of your report that lists "inquiries." Where "inquiries" appear from the company(ies) that opened the fraudulent account(s), request that these "inquiries" be removed from your report. (See "Credit Reports" for more information.) In a few months, order new copies of your reports to verify your corrections and changes, and to make sure no new fraudulent activity has occurred.

Second, contact the creditors for any accounts that have been tampered with or opened fraudulently.

Creditors can include credit card companies, phone companies and other utilities, and banks and other lenders. Ask to speak with someone in the security or fraud department of each creditor, and follow up with a letter. It's particularly important to notify credit card companies in writing because that's the consumer protection procedure the law spells out for resolving errors on credit card billing statements. Immediately close accounts that have been tampered with and open new ones with new Personal Identification Numbers (PINs) and passwords. Here again, avoid using easily available information like your mother's maiden name, your birth date, the last four digits of your SSN or your phone number, or a series of consecutive numbers.

Third, file a report with your local police or the police in the community where the identity theft took place.

Get a copy of the police report in case the bank, credit card company or others need proof of the crime. Even if the police can't catch the identity thief in your case, having a copy of the police report can help you when dealing with creditors.

Your Next Steps

Although there's no question that identity thieves can wreak havoc on your personal finances, thereare some things you can do to take control of the situation. For example:

- **Stolen mail.** If an identity thief has stolen your mail to get new credit cards, bank and credit card statements, pre-screened credit offers or tax information, or if an identity thief has falsified change-of-address forms, that's a crime. Report it to your local postal inspector. Contact your local post office for the phone number for the nearest postal inspection service office or check the Postal Service web site at www.usps.gov/websites/depart/inspect.
- **Change of address on credit card accounts.** If you discover that an identity thief has changed the billing address on an existing credit card account, close the account. When you open a new account, ask that a password be used before any inquiries or changes can be made on the account. Avoid using easily available information like your mother's maiden name, your birth date, the last four digits of your SSN or your phone number, or a series of consecutive numbers. Avoid using the same information and numbers when you create a PIN.
- **Bank accounts.** If you have reason to believe that an identity thief has tampered with your bank accounts, checks or ATM card, close the accounts immediately. When you open new accounts, insist on password-only access to minimize the chance that an identity thief can violate the accounts.

  In addition, if your checks have been stolen or misused, stop payment. You can contact the following major check verification companies to learn more about the services they provide in helping you track your stolen or misused checks.

SCAN: 1-800-262-7771
TeleCheck: 1-800-710-9898 or 927-0188
CrossCheck: 1-707-586-0431
Equifax Check Systems: 1-800-437-5120
International Check Services: 1-800-526-5380

If your ATM card has been lost, stolen or otherwise compromised, cancel the card as soon as you can and get another with a new PIN.

- **Investments.** If you believe that an identity thief has tampered with your securities investments or a brokerage account, immediately report it to your broker or account manager and to the Securities and Exchange Commission.

  You can file a complaint with the SEC by visiting the Complaint Center at www.sec.gov/complaint.shtml. Be sure to include as much detail as possible. If you do not have access to the Internet, write to the SEC at: SEC Office of Investor Education and Assistance, 450 Fifth Street, NW, Washington, DC 20549-0213, or call 202-942-7040.

- **Phone service.** If an identity thief has established new phone service in your name; is making unauthorized calls that seem to come from - and are billed to - your cellular phone; or is using your calling card and PIN, contact your service provider immediately to cancel the account and/or calling card. Open new accounts and choose new PINs.

  If you are having trouble getting fraudulent phone charges removed from your account, contact your state Public Utility Commission for local service providers or the Federal Communications Commission for long-distance service providers and cellular providers at www.fcc.gov/ccb/enforce/complaints.html or 1-888-CALL-FCC.

- **Employment.** If you believe someone is using your SSN to apply for a job or to work, that's a crime. Report it to the SSA's Fraud Hotline at 1-800-269-0271. Also call SSA at 1-800-772-1213 to verify the accuracy of the earnings reported on your SSN, and to request a copy of your *Social Security Statement*. Follow up your calls in writing.
- **Driver's license.** If you suspect that your name or SSN is being used by an identity thief to get a driver's license or a non-driver's ID card, contact your Department of Motor Vehicles. If your state uses your SSN as your driver's license number, ask to substitute another number.
- **Bankruptcy.** If you believe someone has filed for bankruptcy using your name, write to the U.S. Trustee in the Region where the bankruptcy was filed. A listing of the U.S. Trustee Program's Regions can be found at www.usdoj.gov/ust, or look in the Blue Pages of your phone book under U.S. Government - Bankruptcy Administration.

  Your letter should describe the situation and provide proof of your identity. The U.S. Trustee, if appropriate, will make a referral to criminal law enforcement authorities if you provide appropriate documentation to substantiate your claim. You also may want to file a complaint with the U.S. Attorney and/or the FBI in the city where the bankruptcy was filed.

- **Criminal records/arrests.** In rare instances, an identity thief may create a criminal record under your name. For example, your imposter may give your name when being

arrested. If this happens to you, you may need to hire an attorney to help resolve the problem. The procedures for clearing your name vary by jurisdiction.

If You're a Victim

1, 2, 3 - Do these three things immediately!

Contact the fraud departments of each of the three major credit bureaus and report that your identity has been stolen. Ask that a "fraud alert" be placed on your file and that no new credit be granted without your approval.

For any accounts that have been fraudulently accessed or opened, contact the security departments of the appropriate creditors or financial institutions. Close these accounts. Put passwords (***not*** your mother's maiden name) on any new accounts you open.

File a report with your local police or the police where the identity theft took place. Get a copy of the report in case the bank, credit card company, or others need proof of the crime later on.