Guarding Your Privacy

Tips to Prevent Identity Theft

From the Office of
Minnesota Attorney General
Lori Swanson

www.ag.state.mn.us

The Attorney General's Office answers questions about consumer issues. If you have a consumer question or complaint, contact the Attorney General's Office in writing, by phone, or visit our website:

Minnesota Attorney General's Office
445 Minnesota Street, Suite 1400
St. Paul, MN 55101

651-296-3353 or 800-657-3787
TTY: 651-297-7206 or 800-366-4812
(TTY numbers are for callers using teletypewriter devices.)
www.ag.state.mn.us

Guarding Your Privacy is written and published by the Minnesota Attorney General's Office. This edition was published in April 2013.

The Attorney General's Office is an equal opportunity employer who values diversity.

Table of Contents

Chapter 3: What to Do if You're a Victim

Take Action Immediately

Cleaning Up the Mess

Introduction

On any given day, you may find yourself writing a check at your local convenience store, using your credit card online to purchase a gift, or applying by phone for a new credit card with your favorite merchant. In each instance, although you may be unaware, you are revealing personal and unique information about yourself such as your banking information, credit card number, your Social Security number ("SSN"), along with your name, birth date, address, phone number and other contact information that uniquely identifies you. This information is a gold mine for identity thieves to use to commit fraud or theft without your knowledge. It has been estimated that four out of five victims of identity theft had no idea how an identity thief obtained their personal information.

The U.S. Federal Bureau of Investigation ("FBI") calls identity theft one of the fastest growing crimes in the United States, estimating that 500,000 to 700,000 Americans become victims each year. Identity theft is spurred on by lenders and creditors willing to grant thousands of dollars in credit in mere minutes with little or no proof of identity. In addition, you may have seen a recent rise in news reports of laptop computers containing sensitive personal information stolen or lost by careless employees, leaving personal data in the hands of potential thieves. In today's information age, an identity thief can easily, and sometimes legally, tap into your information with just the click of a computer mouse. An identity thief may simply swipe the contents of your mailbox or even rummage through your trash searching for account statements, pre-approved credit card offers or credit receipts. Armed with this information, a thief can pose as you to acquire a credit card, or siphon money from your personal savings and checking accounts.

Identity theft may take months for you to detect and sometimes years or longer to unravel. This booklet provides important information on how to protect your privacy, safeguarding your personal data and avoiding identity fraud.

Chapter 1: What is Personal Information and Identity Theft?

The Personal Information Trade

When we wonder or worry about who might be snooping in our private affairs, we often think about the government, "Big Brother," watching our homes, telephone calls, or travels; however, today there is another threat to our privacy in the network of commercial databases that keep personal information about each one of us.

Personalization

The sale, collection, and integration of personal information about consumers are new industries in the information age. There are currently over 1,000 private companies keeping comprehensive databases about individual consumers, a ten-fold increase in just five years.

These companies do not engage in the "mass marketing" of products or the researching of general demographic groups. Rather, they focus on gathering as much information as possible about specific people to engage in what is sometimes called "personalization" or "personal marketing." Technology now allows these businesses to cheaply gather information about consumers, and then sort and categorize the data, sometimes called "data mining," to isolate specific people for "target marketing" purposes.

Personal Information

The information possessed by these companies goes far beyond mere demographic data. For example, a privacy lawsuit against a marketing company revealed the types of information contained in its database. Its computer files contained more than 900 tidbits of information on individual consumers dating back more than a decade. One individual's file was reportedly 25 single-spaced pages and contained information such as her income, marital status, hobbies, medical ailments, her preferred brand of antacid tablets, whether she had dentures, and how often she had used room deodorizers, sleeping aids, and hemorrhoid remedies.

The array of information available is limited only by the technology itself. Each electronically recorded transaction – from your use of credit, debit or ATM cards to your payment of mortgage or student loans – provides a glimpse into your private life. When layered on top of one another, these pieces of information create a complete picture of you as an individual.

Here are a few examples of the personal information trade:

- One company maintains a database that operates twenty-four hours a day, gathering and processing information on 95% of American households. For a price, it will sort information based on income, lifestyle (outdoor, mechanic, intelligence, etc.), or even a profile of "ethnics who may speak their native language but do not think in that manner."
- Another company offers lists of people with particular medical conditions. In 1999, it offered for sale nearly 50 lists of individuals suffering from different medical ailments. It sells the names and addresses of 427,000 people who are clinically depressed, 1.4 million women

who have yeast infections, and one million individuals who have diabetes. It also sells lists of people with Alzheimer's Disease, birth defects, Parkinson's Disease, and "physical handicaps."

- A New York company offers the names of high school students according to GPA, religion, ethnicity, and SAT scores.
- A hospital sells the names of its patients who may be eligible for Social Security insurance to a lawyer.

No information appears to be too personal for companies to collect or too insignificant to sell. In 1999, electronic research companies were selling unlisted phone numbers for $49, Social Security numbers for $49, and bank balances for $45. A company will obtain another person's driving record for $35, trace a cell phone call for $84, or create a list of stocks, bonds, and securities for $209. This personal data is merged into a consumer tracking and information system that becomes larger every day and it is sold to whomever may be interested in buying. Each piece of information gathered, stored, and sorted by these large databases represents an erosion of your right to privacy.

The personal information trade also enables a special kind of telemarketing called pre-acquired account telemarketing. Pre-acquired account telemarketing occurs when a telemarketer calls you with the ability to charge your credit card or bank account already in their hand. Unlike most telemarketers, these companies have acquired the ability to charge your account for the product that they are selling before they call you. A typical telemarketing sale, not involving pre-acquired accounts, requires that you provide a credit card or other account number to the telemarketer, or that you send a check or sign a contract in a later transaction. Providing a signature or an account number – like paying cash – is a readily recognizable way for you, as the buyer, to give your consent or assent to a deal.

Pre-acquired account telemarketing removes these short-hand methods for you to control when you have agreed to a purchase. Instead, the telemarketer controls the method by which you provide "consent" to the transaction, making the determination whether you have actually consented to the deal. This puts the telemarketer in a privileged position, such that he or she can charge your bank account or credit card in situations where you would never have voluntarily provided your account number to the caller.

Identity Theft

Identity theft occurs in a variety of ways and has different labels. Two key variations are commonly referred to by law enforcement as "true name" or "true party" frauds and "account takeover" frauds. With "true name" or "true party" fraud, the thief pretends to be you. The thief uses pieces of your identity to obtain new credit cards from banks and retailers, open checking and savings accounts, apply for loans, establish accounts with utility companies, or rent an apartment. The thief can ultimately ring up a tab worth thousands of dollars – all in your name. In an "account takeover" fraud, the thief steals your money and/or assets. The thief obtains enough personal information about you to gain access to existing credit or bank accounts. Thieves impersonating you contact creditors and banks to order additional cards on the account and have the cards sent to their address instead of yours. The thief may also file a change of address with the postal service to divert any newly ordered credit cards or checks into his or her hands.

Identity theft is usually more complex than an ordinary case of credit card fraud. Armed with just one or two pieces of identifying information, such as your birth date or address, a thief can assume your financial identity, access your existing accounts, and obtain a wide range of services and benefits in your name.

Identity Thieves

Interviews with victims of identity theft and experts have revealed a wide range of thief profiles. Thieves may be friends, relatives, co-workers, employees at companies or organizations with personal information about you in their databanks, and, worst of all, total strangers who gain access to your personal information through any number of means.

Victims of Identity Theft

Creditworthy consumers with high incomes are the preferred prey of identity thieves, but almost any of us is a potential victim. It is impossible for you to totally eliminate the possibility of falling prey to identity fraud. To lessen the chance of becoming a victim keep a tight rein on your personal information, get off telemarketing lists, stop businesses from sharing your private information, dispose of sensitive documents safely, and closely monitor your finances.

Legal Protections Against Identity Theft

Under Minnesota and federal law, a person who knowingly transfers, possesses, or uses an identity that is not the person's own, with the intent to commit, aid, or abet any unlawful activity, is guilty of felony identity theft. In Minnesota, the maximum prison term and/or fine for violating the identity theft statute varies depending on the number and type of victims and amount of money stolen. Though laws exist to help prosecute identity theft, prevention is better.

The Federal Fair Credit Reporting Act establishes procedures for correcting mistakes on your credit report and requires that your record only be provided for legitimate business purposes.

The Fair Debt Collection Practices Act prohibits debt collectors from using unfair or deceptive practices to collect overdue bills that your creditor has forwarded for collection.

The Fair Credit Billing Act establishes procedures for resolving billing errors on your credit card accounts. The act provides the most important protection for victims of identity theft. If you notify your card issuer at the address given for "billing inquiries" within 60 days after you receive a bill with an error, the act allows you to dispute the erroneous charge.

The Truth in Lending Act limits your liability for unauthorized credit card charges on lost or stolen cards to $50 per account. If you notify your card issuer before the thief's unauthorized use, your liability will be $0. Therefore, if a company tries to sell you a credit card "protection" against unauthorized charges, you don't need it. The federal law already protects you from significant monetary liability.

The Electronic Funds Transfer Act provides protection for all transactions using your debit card or other electronic means to debit or credit an account. It also limits your liability to $500 for unauthorized electronic fund transfers.

The Identity Theft and Assumption Deterrence Act was enacted to address identity theft. Specifically, the statute makes it a federal crime when a person "knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person with the intent to commit or to aid or abet or in connection with any unlawful activity that constitutes a violation of federal law or that constitutes a felony under any applicable state or local law." Similarly, Minnesota Stat. §609.527 makes identity theft a crime

Your Personal Information is Not as Safe as You Think

Today, personal financial information is widely accessible through a variety of sources. Identity thieves legally obtain much of the information they need. Often, additional information is obtained illegally but at low risk and low cost.

Credit Bureaus

The three major credit bureaus – Experian, Equifax and TransUnion – and other credit reporting agencies, produce hundreds of millions of credit reports each year. The reports include a wealth of personal information about you including your date of birth, addresses, Social Security number, credit account information, public records and employment data.

Credit reports are easy for unauthorized people to get. All a thief needs is your name, Social Security number and a current or previous address. Credit bureaus, to their credit, only send reports to the current address displayed on the report. However, thieves anticipate this move by sending a creditor a pre-approved credit offer using your name and the thief's address. The credit reporting system is designed to automatically update your file, so the report is sent to the thief instead of you. The thief then has all the information they need to steal your identity.

Easy Access to Credit

In the United States today credit is easier to obtain than ever. We expect quick loans, which enable us to grab a surprise bargain or finance an emergency. Easy credit makes for easy crime. The credit approval process often amounts to little more than matching two bits of information on an application – a name and a Social Security number – with a credit report.

Social Security Numbers as Universal Identifiers

When Social Security numbers were first issued in 1936, the federal government assured the public that use of the numbers would be limited to Social Security programs. Today, however, the Social Security number is the most frequently used recordkeeping number in the United States. Social Security numbers are used for employee files, medical records, health insurance accounts, credit and banking accounts, university ID cards, and many other purposes. In fact, a Social Security number is now required for dependents over one year of age.

Computer records have replaced paper filing systems in most organizations. Since more than one person may share the same name, accurate retrieval of information works best if each file is assigned a unique number. Many businesses and governmental agencies believe the Social Security number is tailor-made for this purpose. Because your Social Security number is frequently used as your

identification number in business and government computer databases, information about you in one database is easily linked to other databases that contain different types of private information. Using your Social Security number as a universal identifier makes it possible for identity thieves to gain a more complete picture of your financial records and personal information.

Private Information Check List

What is a Credit Bureau?

A credit bureau is a clearinghouse for credit history information. Creditors provide the bureaus with information about how their customers pay their bills. The bureaus assemble this information along with public record information obtained from courthouses around the country. Then they turn this data into a "file" on each consumer. In return, creditors can obtain credit reports about consumers who wish to open accounts with their business or organization.

There are more than 1,000 local and regional credit bureaus throughout the United States. Most credit bureaus are either owned by, or are under contract with, one of the nation's three major credit bureaus – Experian, TransUnion and Equifax. These national agencies maintain centralized databases containing the credit records of more than 170 million Americans. Credit bureaus generate more than a half billion reports per year.

What is in a Credit Report?

Credit reports are a gold mine of information about you. The report contains your name, Social Security number, address, credit payment status and employment history. A credit report also contains legal information including liens, bankruptcy and other matters of public record. Federal and state laws restrict who has access to your sensitive information and how it can be used. Anyone with a "legitimate business purpose" can gain access to your credit history, including: those considering granting you credit, landlords, insurance companies, employers and potential employers, and companies with which you have a credit account.

Certain pieces of information cannot be included in your credit report:

- Medical information (unless you give your consent).
- Negative information, including a bankruptcy that is more than 10 years old.
- Debts that are more than 7 years old.
- Information about your age, marital status, or race cannot be included in your report if requested by a prospective employer.

How Do I Get My Free Annual Credit Report?

Experts recommend looking at your credit report every year and before making a major purchase. Every year, consumers can get a free credit report from each of the credit agencies — Equifax, TransUnion and Experian. The credit bureaus have created a centralized website, toll-free telephone number and mailing address for Minnesota consumers to order their reports. Annual reports may be requested the following way:

1. Logging on to *www.AnnualCreditReport.com*
2. Calling 877-322-8228
3. Writing to: Annual Credit Report Request Service
   P.O. Box 105281
   Atlanta, GA 30348-5281

Although consumers can only receive their Free Annual Credit Report once per year, consumers may still request additional reports. Minnesota law allows you to purchase another credit report once a year for $3 from each of the credit bureaus, separately. You are also entitled to one free copy of your report each year if (1) you're unemployed and plan to look for a job within 60 days, (2) you're on welfare, or (3) your report is inaccurate because of fraud. In addition, there is no charge for the report if a company takes adverse action against you, such as denying your application for credit, insurance or employment, and you request your report within 60 days of receiving notice of the action. To order your credit report, contact one or more of the three national credit bureaus:

Equifax
P.O. Box 105851
Atlanta, GA 30348
Phone: 800-685-1111
www.equifax.com

Experian
P.O. Box 2002
Allen, TX 75013
Phone: 888-397-3742
www.experian.com

TransUnion
2 Baldwin Place
P.O. Box 1000
Chester, PA 19022
Phone: 877-322-8228
www.transunion.com

What is Your Social Security Statement?

Your Social Security statement provides both a statement of past earnings and an estimate of future benefits you will receive from Social Security. The statement shows how much you've paid into Social Security over your working years. The statement also shows how much you can expect to receive when you retire or if you become disabled. You can also determine from the statement how much your family is entitled to receive if you die. The Social Security Administration recommends that you check your Social Security earnings at least once every three years. After that it becomes more difficult to trace the earnings. A Social Security statement is available upon request. To get a statement, call the Social Security Administration's toll-free number at 800-772-1213 (TTY 800-325-0778).

What is on My Driving Record?

Driver and Vehicle Services, a division of the Minnesota Department of Public Safety, keeps records on drivers (such as driver license and driver history information), and about vehicles (such as ownership information). Information stored about you includes your name, address, Social Security number, physical description (height, weight, eye color), date of birth, status of your driver's license, whether corrective lenses are needed for driving, and if you are an organ donor. In addition, a record is kept of any moving violations that you are convicted of and whether you have medical conditions that may affect driving.

Who Can Get the Information in My Driving Record?

The Minnesota Department of Public Safety ("DPS") restricts access to your driving record unless you expressly consent or federal law authorizes such access. You may allow entities, including businesses, to access your driving record by checking a box on your driver's license or vehicle registration application. If you do not check the box, then only those entities authorized by federal law may access your record.

Your driver's license photograph, Social Security number, and medical and disability information receive heightened protection. Without your consent, that information can be released only for use by government agencies such as law enforcers, for use by insurers to investigate claims or fraud, for use by an employer to verify that you have a commercial driver's license, or for use in legal proceedings.

Most of the remaining data in your driving record is less protected. That data can be released without your consent not only to government agencies, insurers, employers and in legal proceedings for the purposes above, but also to:

- Auto manufacturers, for uses related to auto safety, theft, emissions, alterations, recalls, advisories, market research, and performance monitoring;
- Legitimate businesses, but only in the normal course of business to verify the accuracy of personal information you submitted so as to prevent fraud or recover a debt;
- Researchers, to publish statistical reports that do not identify individuals;
- Towing companies, to notify owners of towed or impounded autos;
- Toll companies, to operate private toll transportation facilities (if Minnesota had such facilities)
- Licensed private investigators or security services, for any of these purposes; or
- Any person who has obtained your written consent.

However, if a person or business requests your driving record for a purpose other than one permitted above (by federal law), then DPS will not release your driving record unless you have expressly consented by checking a box on your license or ownership application renewal. Thus, without your consent, no commercial or business firms can access your record to add your name to direct-mail, telemarketing, or survey lists.

What is in My Medical Information Report?

Medical records are created when you receive treatment from a health professional such as a physician, nurse, dentist, chiropractor or psychiatrist. Records may include your medical history, details about your lifestyle (such as smoking or involvement in high-risk sports), and family medical history. In addition, your records contain laboratory test results, medications prescribed, and the results of surgery and other medical procedures.

A wide range of people, in and out of the health care industry, may access your medical information. Generally, access to your records is obtained when you agree to let others see them. You probably signed a blanket waiver or general consent form at some point when you obtained medical care. When you sign such a waiver, you allow the health care provider to release your medical information to insurance companies, government agencies and others.

The Medical Information Bureau ("MIB") is an organization that compiles a central database of medical information. Approximately 15 million Americans and Canadians are on file in the MIBs computers. More than 750 insurance firms use the services of the MIB, primarily to obtain information about life insurance and individual health insurance policy applicants. You are entitled to a free medical record disclosure once a year. You can get a copy by calling the Medical Information Bureau toll-free at 866-692-6901. For other questions or to correct your report, write to:

Medical Information Bureau
50 Braintree Hill Park, Suite 400
Braintree, MA 02184-8734
www.mib.com

Businesses and Other Organizations with Information About You

It is not just the government or creditors that collect and distribute information about you and your buying practices. Banks, insurance companies, charities and others have personal information about you that you may not want other people to know. You should compile a list of the businesses and organizations that have information about you. When forming new relationships with an organization or company, ask what will be done with your information and who will have access to it. Information is power in our society. Knowing who has what information about you allows you some control over how that information is used. Don't hesitate to let companies and organizations know you expect them to respect your privacy.

Sale of Personal Information by State and Local Governments

Public records containing personal information such as homeowners' documents, police and court records, utility records, and marriage and divorce records have always been available for sale in paper form. With the growing use of computer databases and the Internet, however, it is easier than ever to obtain these records for fraudulent use without leaving behind a paper trail. Public databases can now be accessed directly from many government computers and through commercial database vendors.

Chapter 2: How to Lessen Your Risk of Being a Victim

Reducing Access and Safeguarding Your Information

Unfortunately, there is no way to completely inoculate yourself from having your identity stolen, but limiting access to your information is key to reducing the risk.

Follow these suggested steps to better protect your private data.

Remove Your Name From Marketing Lists

You may remove your name, or "opt-out," from marketing or promotional lists maintained by credit bureaus, and other organizations with which you have a relationship.

Credit Bureaus. When reviewing your mail you probably noticed a number of pre-approved credit offers with other junk mail. The credit bureaus offer a toll-free number to "opt-out" of having pre-approved credit offers sent to you for two years. When credit offers are thrown in the trash, they are a potential target for thieves.

To "opt-out" of receiving pre-approved credit offers you may call **888-5-OPTOUT** (888-567-8688) or log on to *www.optoutprescreen.com* for more information.

In addition, notify the three major credit bureaus that you do not want your personal information shared for promotional purposes. To limit the amount of information credit bureaus share about you, write your own letter or use the sample letter provided in the back of this publication to notify the credit bureaus of your request. Send your letter to the following addresses:

Equifax
Attn: Information Services
P.O. Box 740123
Atlanta, GA 30374

Experian
Attn: Consumer Services
901 West Bond
Lincoln, NE 68521

TransUnion
Name Removal Option
P.O. Box 505
Woodlyn, PA 19094

Direct Marketers. The Direct Marketing Association ("DMA") is a trade association of catalogers, financial services firms, publishers, book and music clubs, online service companies, and others involved in direct and database marketing. To "opt out" of DMA mailing lists (other companies may continue to contact you) for up to five years, send your own request or use the sample letter at the back of this publication with your complete name (including variations), mailing address and telephone number, along with a check or money order made out to "DMA" in the amount of $1 for each name to:

DMAchoice
Direct Marketing Association
P.O. Box 643
Carmel, NY 10512
www.dmachoice.org

Federal law forbids a telemarketer to call you once you have asked to be put on that telemarketer's "do-not-call" list. A telemarketer who ignores your request can be held responsible for up to $500 in damages per call and $1500 per willful violation. Thus, if you do not want to be called in the future, you should tell the telemarketer that you want to be placed on that telemarketer's "do-not-call" list and that you know you are entitled under federal law to $500 per call after your request.

You should also take an inventory of banks, charities, and other organizations with which you do business. Write to these organizations telling them not to sell or give out your name. You may use the form letter prepared by this Office on page 23. If you think your name has been sold, send a letter to the company or organization and complain. Ask for the list of businesses or charities that bought your name and information. Then, write to these organizations and ask them to put you on their "do-not-mail" and "do-not-sell" lists.

Don't Be an Easy Target

When you pay bills, don't leave the envelopes containing your checks at your home mailbox for the postal carrier to collect. If stolen, your checks can provide valuable information to the thief or be altered and cashed. Your credit card payments, if acquired by a thief, contain all the information needed to steal your identity. Also, consider installing a locked mailbox at your residence to reduce the possibility of mail theft.

- When you order new checks from your financial institution, remove extraneous information such as your middle name, phone number, Social Security number or driver's license number. The fewer pieces of identifying information you have on your checks the better.
- When creating passwords and personal identification numbers (PINs), do not use any combination of numbers that could be easily detected by thieves. Don't use the last four digits of your Social Security number, your birth date, middle name, mother's maiden name, address or consecutive numbers.
- Don't toss credit card convenience checks or pre-approved credit offers in your trash or recycling bin before first tearing them into small pieces or shredding them. The solicitations can be used by "dumpster divers" to cash the checks or order credit cards in your name. Do the same with other sensitive information like credit receipts, bank statements and important bills you do not retain for your records.
- Store your canceled checks in a secure place. In the wrong hands checks could reveal a lot of information about you, including your account number, telephone number, and driver's license number. Never permit your credit card number to be written on your checks by a merchant. (It is illegal in Minnesota for any merchant to write your credit card number on your check when you are completing a purchase.)
- Carefully review your credit card statements and phone bills for unauthorized charges or fraudulent use. Scrutinize your local, long distance and cellular bills each month and report any unauthorized use to your service provider. You may contact your local telephone company to verify your long distance carrier and request a "Pic Freeze" on your account so it cannot be changed without your specific authorization. If you would like more information on a Pic Freeze, telephone billing and how to avoid phone fraud, the Attorney General's Office offers a free publication entitled *The Phone Handbook*.

Be Smart With Credit Cards

Check for fraudulent use of your credit accounts. The most important step to safeguarding your identity is to monitor your credit card statements and credit report.

- Once a year, order a free copy of your credit report from each of the three largest credit bureaus. Reduce the number of credit cards you actively use. Carry only one or two credit cards in your wallet or purse and cancel all others. Unused cards should be canceled because, even though you don't use them, the numbers are recorded on your credit report and can be used by identity thieves.
- Don't give out your credit card number or other personal information over the phone unless you know with whom you're doing business. Even then, before revealing any personal information, find out how it will be used or shared with others.
- Always take credit card and ATM receipts with you when you make a purchase or withdrawal. Monitor your mail when you are expecting a new credit card that you have applied for or a reissued credit card that has expired. Contact the issuer right away if the card does not arrive on the date expected.

The National "Do-Not-Call" Registry

In 2003, the Federal Trade Commission ("FTC") began registering consumers on a national "do not call" list. You may register up to three phone numbers (including your cell phone number) by visiting ***www.donotcall.gov*** or calling **888-382-1222**. Your phone number will remain on the registry permanently unless you later delete it from the registry. As of January 1, 2005, telemarketers covered by the National Do Not Call registry will have up to thirty-one (31) days from the date you register to stop calling you.

Some calls are exempt from the Do Not Call law. Examples of exempt calls include:

1) Calls from - or on behalf of - political organizations, charities, and telephone surveyors.
2) Calls from companies with which you have an existing business relationship.
3) Calls from companies you've given permission to call.

If your number is already registered on the National Do Not Call Registry, then you do not need to re-register with the state list. When you place your name on the national list, you will be automatically entered on the state list.

Shop Smartly Online

The Internet puts vast information at your fingertips. With a click of a mouse, it lets you buy an airline ticket, buy a book, book a hotel, send flowers to a friend, or purchase stock – often at any time of the day or night. Before you shop, though, consider the following safety tips.

- **Use a secure browser**. A browser is software you use to navigate the Internet. Your browser should comply with industry security standards. These standards encrypt or scramble the purchase information you send over the Internet, ensuring the security of your transaction. Most computers come with a browser installed, though you may also download some browsers for free.
- **Shop with companies you know.** Anyone can set up shop online under almost any name. If you're not familiar with a merchant, ask for a paper catalog or brochure to get a better idea of their merchandise and services. Determine the company's refund and return policies before you place an order.

- **Check the company's online privacy policy.** Many companies with privacy practices post a "privacy policy" on their web site. The privacy policy should disclose what information is being collected on the website, as well as how that information is being used. Before you provide any merchant with personal information, read its privacy policy. If you can't find a policy, send an email or written message to the merchant's site to get one.
- **Make sure you're at the correct website.** Online merchants may have links to other webpages selling the same product. For instance, you might go to an online bookstore to shop for a particular book and, in the course of your shopping, click on a link to "learn more about the author." The link might take you to the author's homepage where you can also order the book. You might inadvertently buy the book from the author rather than from the original bookstore, and then be bound by privacy and return policies you haven't read. Before you order a product online, be sure to check the URL (the address at the top of the page) to ensure that you are on the correct website.
- **Disclose only necessary personal information.** Don't disclose personal information such as your name, address, telephone number, email address or Social Security number until you know who is collecting the information, why they are collecting it and how they will use it. If disclosure of personal information is necessary (e.g. to deliver a product you buy), then disclose only the amount of personal information that is required to complete the transaction. If you have children, teach them to check with you before giving out personal or family information online.
- **Pay by credit or charge card.** If you pay by credit or charge card online, some companies let you pay bills and check your account status online. Before you sign up for any service, evaluate how the company is securing your financial and personal information. Many companies explain their security procedures on their website, often in their "privacy policy." If you don't see a security description, call or email the company and ask.
- **Keep a record.** Be sure to print a copy of your purchase order and confirmation number for your records. Since the Federal Mail or Telephone Order Merchandise Rule covers orders made via the Internet, your merchandise must be delivered to you within 30 days. If there are delays, the company must notify you.
- **Opt-out of information sharing.** Many companies now give you a choice on their website, often as part of their "privacy policy," as to whether and how your personal information is used. These companies allow you to decline – or to "opt-out" of – having personal information such as your email address used or shared with other companies. Exercise this option to reduce access to your personal information.
- **Keep your passwords private.** Be creative when you establish a password, and never give it to anyone. Avoid using a telephone number, birth date, or a portion of your social security number. Instead use a combination of numbers, letters and symbols.

Minnesota Security Freeze Law

A Minnesota law, effective August 1, 2006, should help citizens protect themselves from new account fraud. The law empowers any consumer to freeze his or her credit report by simply contacting a consumer reporting agency and requesting a credit report freeze. A credit report freeze will deny identity thieves access to the consumer's credit history and prevent them from obtaining new credit cards or loans under the consumer's name.

As of August 1, 2006, any Minnesotan can impose such a freeze on his or her personal credit report for any reason. Victims of identity theft can have their credit reports frozen without charge. Non-victims can proactively freeze their credit report for a $5 fee. When a credit reporting agency receives a freeze request, it must place the freeze within 3 days of the request, and provide a unique PIN to the consumer within 10 days of the request.

The consumer may then use the PIN to temporarily lift or "thaw" his or her report for a specific period of time or for a specific creditor. For example, suppose that you are looking to purchase a new car. If you know that you want to buy the car from Dealership XYZ, you may contact the credit reporting agencies and allow that specific dealership to access your credit report. Or you may request that your credit report be accessible to any creditor for a specific period of time, such as 30 days, to give you time to shop at several dealerships. After the specified time, your credit report will automatically refreeze.

Be sure to keep the PIN in a safe place. If you forget your PIN, you can get a second one for free, but will have to pay $5 for a third one. Like placing the freeze, victims of identity theft can thaw their credit reports without charge, while non-victims may be charged a $5 fee.

Because different credit issuers may use different credit reporting agencies, you will need to freeze your credit report with each of the three major credit reporting agencies. Each of the three credit reporting agencies has its own process for taking credit freeze requests. If you are a victim of identity theft, you will need to provide the credit reporting agencies with a copy of either the police report or case number documenting the theft to avoid the $5 fee.

For instructions on how to request a credit freeze, consumers may contact the credit reporting agencies as follows:

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
888-397-3742
http://www.experian.com/freeze

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
800-685-1111
https://www.freeze.equifax.com

TransUnion Security Freeze
P.O. Box 2000
Chester, PA 19022
888-909-8872
http://www.transunion.com/personal-credit/credit-disputes/credit-freezes.page

Plan Ahead

When your credit file is frozen, **no one** will be approved for new credit. In order for you to obtain new credit, you must use your PIN and contact the credit reporting agencies to thaw your file. While credit reporting agencies are to thaw credit reports in an expedited manner, thawing your file may take up to three business days. Be sure to plan ahead and temporarily thaw your credit file before applying for credit.

Credit reporting freezes are a new defense in the fight against identity theft. As this crime continues its climb to the top of law enforcement charts, you can be proactive in protecting yourself from its expensive, time-consuming consequences by freezing your credit report.

Chapter 3: What to Do if You're a Victim

The harm to victims of identity theft can be significant and long lasting. The perpetrators of these crimes severely damage your good name and your credit rating. It's up to you to clean up the mess. Until you do, you may be denied loans, a mortgage, security clearances, promotions, and employment.

Act quickly and assertively to minimize the damage. When you deal with the authorities and financial institutions, keep a detailed log of all conversations, including dates, names, and phone numbers. Note the time spent and any expenses incurred. Confirm conversations in writing. Send all correspondence by certified mail (return receipt requested) and maintain copies of all letters and documents.

Take Action Immediately

It would be convenient if there was a central number you could call to correct problems once your identity has been stolen. In the absence of a cure-all, acting quickly is the best way to minimize the damage and get you back on the right track.

Contact the Credit Bureaus

Waste no time in contacting the three major credit bureaus to request that a fraud alert be placed in your credit reports and that a note be included to inform potential creditors that you should be contacted before any additional accounts are opened.

Contact Banks and Creditors

Immediately contact the security or fraud divisions of any companies that maintain a credit or bank account for you. Close all accounts that you believe have been compromised by the identity thief and change account numbers for each account you don't cancel. Request that the creditors make your accounts accessible only through use of a password. Banks and creditors may ask you to complete and notarize fraud affidavits, which can be costly. If this is the case, ask for the bank or creditor to pay the notary fee, because the law does not require that you provide one. A written statement from you and supporting documentation should be sufficient. Report burdensome bank or creditor requirements to federal regulators.

Report the Crime

Report the crime to your local police or sheriff as soon as you are aware of the theft. Be sure to file a report with your local police or sheriff's department. For your records, keep a copy of the incident reports you filed. A law enforcement record of the incident is important because it will allow you to present your creditors and banks with proof of the crime. File a report with the Federal Bureau of Investigation and the U.S. Secret Service. Also file a complaint with the Federal Trade Commission ("FTC") and ask for a complaint number for your records. The FTC monitors identity fraud and educates consumers about the crime.

Keep Detailed Records

Keep detailed records of all interactions and contacts you have with businesses, creditors, and governmental agencies while you are reclaiming your identity. Be sure to follow up in writing and send all letters "return receipt requested" so you know your correspondence was received and by whom. Detailed records will be important later if you choose to bring an action in court to recover damages. Keeping good records also provides a written history of conversations so you don't forget important events.

Cancel Stolen Checks

If the thief steals your checks or sets up fraudulent bank accounts in your name, report it to each of the major check verification companies. Ask for stop payments on any outstanding checks that you dispute and cancel or obtain new numbers for your checking and savings accounts.

Chexsystems	888-478-6536	Attn: Consumer Relations 7805 Hudson Road, Suite 100 Woodbury, MN 55125
Certegy Check Service (previously Equifax Check Systems)	800-770-3792	Certegy Check Services P.O. Box 30046 Tampa, FL 33630
Global Payments	800-638-4600	Fraud Department 6215 West Howard Street Niles, IL 60714
TeleCheck	800-710-9898	Forgery Department P.O. Box 4451 Houston, TX 77210-4451

Cleaning Up the Mess

After you have completed the initial work to recover your identity, take control of the situation by completing this checklist to deal with the most common forms of identity theft.

Contact the Post Office

Check for fraudulent change of address requests and mail fraud. If you suspect that an identity thief has filed a change of address request for you with the post office, notify the U.S. Postal Inspector. Mail theft is a felony in the United States. You should request that the postal inspector forward all mail in your name to your address.

Review Regular Bills

Review your monthly bills, including utilities, cellular phone, long distance, gas and electric, to ensure that you have not incurred any fraudulent charges. Contact each company and report the fraud. Again be sure to follow up all contacts in writing and maintain a copy for your records.

Watch for Social Security Number Misuse

If you think someone may have misused your Social Security number, contact the Social Security Administration and request a copy of your Social Security statement. You should follow up with the Social Security Administration if you find any fraudulent use of your number that changes your earnings and benefit eligibility. As a final option, you may consider changing your Social Security number if you establish that someone else is using your number. The Social Security Administration will change your number only if you fit specific criteria. For more information about the criteria to change your Social Security number, request this federal government fact sheet: "Identity Theft And Your Social Security Number, SSA Pub. No. 05-10064."

Report Passport Theft

If you are the victim of identity theft and have a passport, notify the passport office in writing. Ask the office to be vigilant for anyone using your name to fraudulently obtain a new passport.

Clear False Criminal or Civil Judgments

Sometimes victims of identity theft are wrongfully accused of crimes committed by the impostor. If a civil judgment has been entered against you for actions taken by the identity thief, contact the court where the judgment was entered and report that you have been a victim of identity theft. If you are wrongfully prosecuted for criminal charges, contact the Federal Bureau of Investigation ("FBI"). Request information from the FBI about how to clear your name.

Attack Credit Report Fraud

If you find that there has been unauthorized access or use of your credit report, contact the Federal Trade Commission to determine your rights under the Federal Fair Credit Reporting Act.

Federal Trade Commission (FTC)
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, D.C. 20580
877-382-4357

Get Legal Help

You may want to consult a private attorney to determine what legal action to take against credit grantors and/or credit bureaus if they will not remove fraudulent entries from your credit report or if negligence is a factor. An attorney may be able to help you recover from the fraud and determine whether your rights have been violated.

The Minnesota State Bar Association
Attorney Referral Service
612-333-1183 or 800-292-4152
www.mnfindalawyer.com

Residents of Dakota, Hennepin and Ramsey counties should call the following numbers for attorney referral:

Dakota
952-431-3200

Hennepin
612-752-6666

Ramsey
651-224-1775

Contact Your Legislators

Additional laws dealing with privacy protection may currently be under consideration by the state legislature and Congress. If you are not happy with current privacy protections and fraud laws, contact your local, state and federal legislators to voice your concerns.

Don’t Give Up

Stand up for your rights. You cannot be held responsible for checks cashed or any bills that are the result of the theft of your identity. You should not live under the fear of legal action being brought against you. Your credit rating should not be affected permanently. Don’t let businesses, collection agencies or banks pressure you into paying any bill that is not your responsibility. Let them know you are willing to cooperate to resolve the situation, but don’t let anyone take advantage of you.

Sample Letter to Request a Security Freeze

You will need to freeze your credit report with each of the three major credit reporting agencies.

Date:

[Credit Reporting Agency and Address]

Dear [Credit Reporting Agency],

I would like to place a security freeze on my credit file.

My name is: _____

My former name was (if applies): _____

My current address is: _____

My address has changed in the past 5 yrs. My former address was:

_____

My Social Security Number is: _____

My date of birth is: _____

I have enclosed photocopies of a government issued identity card AND proof of residence such as a utility bill or phone bill

Check one:

☐ I am an identity theft victim and a copy of my police report (or other investigative report or complaint to law enforcement agency concerning identity theft) of identity theft is enclosed.

☐ I have included my payment of $5 to place a security freeze on my credit file.
Credit card number _____ Expiration Date _____
Money order # _____ Check #_____

Attached is the required documentation.

Yours Truly,

[Your name]

[Send items Certified Mail - Return Receipt Requested.]

Sample Letter to Restrict Sharing of Personal Information About You

ORGANIZATIONS YOU MIGHT WANT TO SEND THESE LETTERS TO INCLUDE:

- ☐ Your Bank and Other Financial Institutions
- ☐ Your Credit Card Companies
- ☐ Your Mortgage Company
- ☐ The Direct Marketing Association ($1 fee)
- ☐ Your Telephone Company
- ☐ Your Charities
- ☐ Your Department Stores and Other Merchants

To get off some mailing lists, send a letter to:
DMAchoice
Direct Marketing Association
P.O. Box 643
Carmel, NY 10512
or visit *www.dmachoice.org*

✂----------

Re: Opt-Out of Disclosure of My Personal Information

To Whom It May Concern:

I hereby opt-out of the sale, rental, distribution, exchange or other disclosure of any and all personal information you have about me. This includes but is not limited to my name, home address and phone, work address and phone, email addresses, Social Security number, drivers license number, financial account and access numbers, and my transaction history with you.

Please promptly confirm in writing that you will not disclose my personal information without my expressed consent.

Full Name: _____ Signature: _____

Address : _____ Date: _____

_____

✂----------

Re: Opt-Out of Disclosure of My Personal Information

To Whom It May Concern:

I hereby opt-out of the sale, rental, distribution, exchange or other disclosure of any and all personal information you have about me. This includes but is not limited to my name, home address and phone, work address and phone, email addresses, Social Security number, drivers license number, financial account and access numbers, and my transaction history with you.

Please promptly confirm in writing that you will not disclose my personal information without my expressed consent.

Full Name: _____ Signature: _____

Address: _____ Date: _____

_____

Additional Consumer Information

The Attorney General's Office answers questions regarding numerous consumer issues. The Attorney General's Office also provides mediation to resolve disputes between Minnesota consumers and businesses and uses information from consumers to enforce the state's civil laws.

If you have a consumer complaint, please contact the Attorney General's Office in writing:

Minnesota Attorney General's Office
445 Minnesota Street, Suite 1400
St. Paul, MN 55101

Citizens can also receive direct assistance from a consumer specialist by calling:
651-296-3353 or 800-657-3787
TTY: 651-297-7206 or TTY: 800-366-4812
(TTY numbers are for callers using teletypewriter devices.)

Additional consumer publications are available from the Attorney General's Office. Contact us to receive copies or preview the publications on our website: *www.ag.state.mn.us.*

- The Car Handbook
- Citizen's Guide to Home Building and Remodeling
- Conciliation Court
- The Credit Handbook
- Have You Looked at Your Credit Report Lately?
- The Home Buyer's Handbook
- The Home Seller's Handbook
- Landlords and Tenants: Rights and Responsibilities
- The Manufactured Home Parks Handbook
- Minnesota's Car Laws
- Private Mortgage Insurance Fact Sheet
- The Phone Handbook
- Probate and Planning: A Guide to Planning for the Future
- Reducing Unwanted Calls and Junk Mail
- Seniors' Legal Rights
- Veterans and Service Members
- Managing Your Health Care
- Other Consumer Bulletins

From the Office of
Minnesota Attorney General
Lori Swanson

Consumer Protection
445 Minnesota Street, Suite 1400
St. Paul, MN 55101

Guarding Your Privacy