

IDENTITY THEFT...
Don't let it happen to YOU!

Iowa Attorney General
Consumer Protection Division
Hoover State Office Building
1305 East Walnut Street
Des Moines, Iowa 50319
www.IowaAttorneyGeneral.org
Consumer@AG.State.IA.US
515-281-5926

888-777-4590

A Message from Attorney General Tom Miller

Dear fellow Iowans:

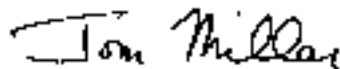
The goal of this brochure is to help you avoid becoming a victim of "identity theft." Identity theft occurs when someone obtains important personal information, such as your Social Security number, banking or credit card account numbers, to commit fraud or theft.

Today's credit identity thieves are information seekers and they don't need to steal your wallet. They obtain bits of information by sorting through trash for discarded receipts and statements, spying for your PIN number at ATM machines or telephone booths, accessing public records, and even stealing from your mailbox.

The Consumer Protection Division of my office developed this brochure to suggest steps you can take to reduce your risk of disclosing important personal information and of becoming a victim of identity theft.

I encourage you to contact my office if we can provide any more information. Please log on to our website at www.IowaAttorneyGeneral.org for valuable information on identity theft as well as other consumer issues or write to the Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, Iowa 50319, or call 515-281-5926 or 888-777-4590.

With best wishes,

A handwritten signature in black ink that reads "Tom Miller". The signature is written in a cursive style with a large, stylized "T" and "M".

Attorney General of Iowa

Tom Miller

IDENTITY THEFT... DON'T LET IT HAPPEN TO YOU!

Identity theft crimes are on the rise causing nationwide concern. Your personal identifying information can be accessed in a variety of ways. An imposter can misuse your information to open fraudulent credit card accounts, secure deposits on cars and housing, obtain employment opportunities, create insurance benefits, and rob retirement earnings. This form of financial sabotage can devastate your credit and require endless hours of telephone and written communication to resolve. In the meantime, you may experience difficulty writing checks, obtaining loans, renting apartments, and even getting hired. While following these precautionary steps is not a guarantee, it will greatly reduce your chances of becoming the next identity theft victim.

Reducing access to your personal identifying information:

1. To minimize the amount of information a thief can steal, do not carry extra credit cards, your Social Security card, birth certificate, or passport in your wallet or purse, except when needed.
2. To reduce the amount of personal information that is "out there," consider the following:
 - Remove your name from the marketing lists of the three credit reporting bureaus -- Equifax, Experian, and Trans Union. This will limit the number of pre-approved credit offers that you receive in the mail. Financial institutions mail over 3 billion pre-approved credit offer a year! When in transit or tossed into the garbage, such solicitations are a likely target of identity thieves who use them to order credit cards in your name. To remove your name:

Call toll-free **888-567-8688**

or write to:

Name Removal Option
P.O. Box 97328
Jackson, MS 39288-7328

- **ORDER YOUR FREE CREDIT REPORT**

Upon your request, a credit bureau is required to provide you with one *free* credit report during any 12-month period. The three nationwide consumer reporting companies have set up one central website, toll-free telephone number, and mailing address through which you can order your *free* annual report. To order, go to:

www.annualcreditreport.com
877-322-8228 (toll-free)
or mail a request to: Annual Credit Report Request Service P.O. Box 105281 Atlanta, GA 30348-5281

Do not contact the three nationwide consumer reporting companies individually. They are only providing free annual credit reports through the centralized website, telephone number and mailing address listed above.

You may order your reports from each of the three nationwide consumer reporting companies at the same time, or you can order from only one or two. **The law allows you to order one free copy from each of the three nationwide consumer reporting companies every 12 months.** We recommend the three separate reports at different times of the year, such as one every four months.

You want to review your credit report:

1. because the information it contains affects whether you can get a loan and how much you will have to pay in interest to borrow money.
2. to make sure the information listed is accurate, complete, and up-to-date before you apply for a loan for a major purchase like a house or car, buy insurance, or apply for a job.
3. to help guard against identity theft before it happens to YOU! Catch inaccurate or downright fraudulent information before it affects your ability to get credit, insurance, or even a job!

Under federal law, you're also entitled to a free report if a company takes adverse action against you, such as denying your application for credit, insurance, or employment, and you ask for your report within 60 days of receiving notice of the action. The notice will give you the name, address, and phone number of the consumer reporting company. You're also entitled to one free report a year if you're unemployed and plan to look for a job within 60 days; if you're on welfare; or if your report is inaccurate because of fraud, including identity theft. Otherwise, a consumer reporting company may charge you up to \$9.50 for another copy of your report within a 12-month period. This fee is often waived. (15 United States Code section 1682j(c)(3)).

To buy additional copies of your report, contact:

Credit Bureau	Report Consumer Fraud	Request Credit Report	Website Access
Equifax P.O. Box 740241 Atlanta, GA 30374-0241	800-525-6285 and write to address at left.	800-685- 1111	www.equifax.com
Experian P.O. Box 9530 Allen, TX 75013	888-397-3742 and write to address at left.	888-397- 3742	www.experian.com
Trans Union P.O. Box 6790 Fullerton, CA 92634-6790	800-680-7289 and write to address at left.	800-916- 8800	www.transunion.com

- Put your telephone number on the **National Do Not Call Registry**. The Federal Trade Commission (FTC), the Federal Communications Commission (FCC), and the states Attorney Generals are enforcing the National Do Not Call Registry to make it easier and more efficient for you to stop getting telemarketing calls you don't want. Placing your number on the registry will stop most, but not all, telemarketing calls. Registration is free.

Register online at www.DoNotCall.gov	Register up to 3 telephone numbers and you will receive a confirmation by e-mail.
Call toll-free 888-382-1222	You must call from the telephone number that you wish to register.

- Remove your name, home mailing address, home telephone number, and home e-mail address from many national lists by opting out of the Direct Marketing Association's marketing lists. The Direct Marketing Association is the largest national trade association serving the direct and interactive marketing field. This service is only available for individuals and "home" addresses (not businesses). You will be removed from the Direct Marketing Association member lists for five (5) years.

To remove your name from national mailing and telephone lists <u>free of charge</u> , write:	Direct Marketing Association P.O. Box 282 Carmel, NY 10512-0282
Or remove your name from national mailing, telephone, and e-mail lists for a \$10 fee, on-line:	www.the-dma.org

- Consider removing your name and address from the telephone book, reverse directories, and city directories. By eliminating your name from these sources, you can reduce access to your personal information from places like the Internet (which mainly use public information resources as a database), telemarketers, and identity thieves.

To block your address, call or write:	Qwest 925 High Street Des Moines, IA 50309 1-800-244-1111 www.qwest.com	No fee
---------------------------------------	------------------------------------------------------------------------------------------------------------------------	--------

To remove your information from the phone book ("non-listed"), call or write:	Qwest 925 High Street Des Moines, IA 50309 1-800-244-1111 www.qwest.com	\$2.50 monthly
To remove your information from the phone book and directory assistance ("non-published"), call or write:	Qwest 925 High Street Des Moines, IA 50309 1-800-244-1111 www.qwest.com	\$4.00 monthly
To remove your information from the city directory, call or write:	R. L. Polk Company 37001 Industrial Road Livonia, MI 48150 1-800-275-7655	Free

- Under Iowa law individuals are "assigned" a random driver's license number rather than using their Social Security number. The Social Security number is the most frequently used record keeping number in the United States. The widespread use of Social Security numbers makes invasion of privacy and fraud easier to commit. Even though you are given an assigned number, Iowa law requires you to *disclose* your Social Security number to the Department of Transportation when applying for an Iowa driver's license. In addition to being your driver's license number, an assigned number can be utilized in a variety of ways, thus protecting your Social Security number from unnecessary public disclosure. Iowa law protects your personal identifying information on your driver's license from public disclosure. (Iowa Code section 321.11) However, personal information does not include your factual driving record (such as records of conviction or occurrences of accidents). To report driver's license fraud, contact:

Iowa Department of Transportation
Office of Driver Services
Park Fair Mall
100 Euclid Avenue
Des Moines, IA 50306-9204
Phone: 515-244-8725
Phone: 800-532-1121 (toll-free within Iowa)
www.dot.state.ia.us

- If you provide your County Treasurer with an assigned driver's license number, your Social Security number will not be printed on your motor vehicle registration receipt, which you are required to carry in your vehicle. In addition, you may

consider deleting your middle name or using only your middle initial if you have a common name. Iowa law requires you to *disclose* your full name and Social Security number to the County Treasurer when applying for an Iowa title or a motor vehicle renewal.

- Iowa law allows individuals to delete their Social Security number, middle name (you may consider using a middle initial if you have a common name) and telephone number from voter registration records. (Iowa Code section 48A.11) Your local County Auditor's Office can give you or mail you a Voter Registration Application to change the information contained within your voter registration file. Fill out the entire form and simply write "delete" in the areas you want to protect from public disclosure. This form is also available in most McLeod, Qwest Dex, Telecom, or Yellow Book telephone books in the government listings.
3. Install a locked mailbox, a front door slot at your residence to reduce mail theft, or use a post office box. When you pay bills, do not leave the envelopes containing your checks at your homes mailbox for the postal carrier to pick up. If stolen, your checks can be altered and then cashed. If stolen, credit card payments contain all the necessary information an identity thief needs. Never write your credit card account number or Social Security number on your checks when making a payment. Due to an increased risk of theft and vandalism, it is best to mail bills and other sensitive items at the post office, rather than from your residence or neighborhood drop boxes.
 4. When you order new checks, consider removing "extra" information such as your Social Security number, assigned driver's license number, middle name, and telephone number. The less personal identifying information you make available, the more likely an identity thief will choose an easier target. Do not have new checks sent to your homes mailbox. Pick them up at the bank instead.

Credit cards:

5. Reduce the number of credit cards you actively use to a bare minimum. Carry only one or two of them in your wallet. Cancel all unused accounts. Even though you do not use them, their account numbers are recorded in your credit report, which is full of data that can be used by identity thieves. Cut up the unused card, return it to the credit card issuer and request that the account be "closed at customer's request".
6. Keep a list or photocopy of all your credit cards, account numbers, expiration dates, and telephone numbers of the customer service and fraud departments in a secure place (not your wallet or purse) so you can quickly contact your creditors in case your cards have been lost or stolen. Do the same with your bank accounts.
7. Never give out your credit card number or other personal information over the telephone unless you have a trusted business relationship with the company and **YOU HAVE INITIATED THE CALL**. Identity thieves have been known to call their victims with a fake story that goes something like this: "Today is your lucky day! You have been chosen by

the Publishers Consolidated Sweepstakes to receive a free trip to the Bahamas. All we need is your credit card number and expiration date to verify you as the lucky winner." Identity thieves tell you they are the IRS, your credit card fraud department, the hospital emergency room, or anyone else they can pretend to be to "panic" you in to giving up your personal information.

8. Always take credit card and ATM receipts with you. Never toss them in a public trash container.
9. You will receive "Privacy Notices" once a year from businesses that you have a financial relationship with. The Privacy Notice tells you whether the business shares information that it knows about you with other businesses. In many cases, if you fail to respond to the Privacy Notice you are allowing that business to share, sell, or trade YOUR personal information to ANYONE! So the next time you receive a Privacy Notice, read the back page and make an affirmative decision on whether you want that business to share your personal information.
10. If your credit card issuer sends random issue convenience checks, request (in writing) to be removed from the mailing list. Credit card convenience checks are easy prey for identity thieves to steal and use while, often times, the consumer is unaware that the random checks were even issued. Your credit card billing statement should contain a different address for "correspondence" to the issuer. Do not send your requests to the same address where you send your credit card payments.
11. Watch the mail when you are expecting a new credit card that you have applied for or a reissued credit card that has expired. Immediately contact the issuer if the credit card does not arrive.
12. One of the benefits for consumers using the Internet, a global network of interlinked computer networks, is the ability to purchase products and services around the clock electronically from the convenience of their home or office. One of the drawbacks is the potential for fraud and deception. Be careful when using a credit card or before providing personal information (such as your Social Security number or date of birth) on the Internet. Read the browser's and the merchant's security and/or privacy statement. Look for the words Secure Sockets Layer (SSL) or Secure Electronic Transaction (SET) to establish if the website is encrypted, which means that is secure from unauthorized parties. Look for the symbols of a padlock or key in the lower right hand corner of your browser window (whether you see a padlock or a key depends on which browser you are using). If the padlock or the key are unbroken, the website is secure. Check to see if the web address includes an "s" for example https://. The "s" indicates that the website contains SSL or SET and is secure.

Passwords and Personal Identification Numbers (PINs):

13. Avoid using common, easy to guess passwords and PINs such as the last four digits of your Social Security number, your birth date, middle name, mother's maiden name, pet's name, address, consecutive numbers, or anything else that could be discovered easily by thieves.
14. Ask your financial institution to add extra security protection to your account at no charge to you. Most will allow you to use an additional code (a number or word) when accessing your account. Do not use the common passwords and PINs listed above.
15. Memorize all of your passwords. Don't record them on anything in your wallet or purse.
16. Shield your hand when using your PIN at an ATM, a point of sale terminal at the store, or when making long distance phone calls with your phone card. "Shoulder surfers" may be spying nearby with binoculars or a video camera.

Social Security numbers:

17. Protect your Social Security number. Release it only when when required by law (such as tax forms, employment records, banking/stock/property transactions, driver's/marriage/professional license applications, etc.) or when in your best interest. If a government agency requests important personal information, including your Social Security number, a Privacy Act notice should accompany the request. (5 United States Code section 552a(e)(3)) This notice will explain whether disclosure of such information is required or requested, the use that will be made of the information, and what will happen if you refuse to provide all or any part of the information. Your Social Security number is the key to most of your personal records such as your financial accounts, medical and insurance records, and government files making it a prime target of identity thieves. You may wish to utilize an "assigned" driver's license number rather than your Social Security number whenever possible.
18. Do not have your Social Security number pre-printed on your checks. Ask that merchants not hand-write your Social Security number on your checks because of the risk of fraud. Currently, there is no law against a merchant requiring you to divulge your Social Security number before accepting a check, so you may need to be assertive. Offering an assigned driver's license number is usually an adequate substitute.
19. Review your annual *Social Security Statement* for inaccuracies or fraud. You will receive your *Statement* from the Social Security Administration automatically each year about three months before your birthday if you:
 - are age 25 or older
 - have worked in Social Security-covered employment or self-employment,

- are not yet receiving benefits
- have a current mailing address on file

If you have not received your *Statement* or have questions, check the website, write, or call:

www.socialsecurity.gov

Social Security Administration
Office of the Inspector General
210 Walnut Street, Room 293
Des Moines, IA 50309
Phone: 800-772-1213
515-283-0212

Responsible information handling:

20. Carefully review your credit card statements and phone bills, including cellular phone bills, for unauthorized charges or fraudulent use. Be aware that under current laws, your local telephone company is obliged to let other carriers use their billing systems for a fee. More and more unscrupulous third parties are billing consumers for goods such as special services, calling plans, or memberships that they did not order and do not want (commonly called "cramming"). Many unauthorized charges result from "free" trial offers which are always followed by some type of charge following the brief trial period... because the goods or services are never really "free". Scrutinize your local, long distance and cellular telephone bills each month for fraudulent or unauthorized charges. Be aware that some long distance telephone companies resort to deceptive tactics to switch your service without authorization (commonly called "slamming"). You may contact your local telephone company to verify your long distance carrier and request a "freeze" on your account so it cannot be changed without your specific authorization using a password.
21. Do not toss credit card convenience checks or pre-approved credit offers in your trash or recycling bin without first tearing them into small pieces or shredding them. They can be used by "dumpster divers" to cash the checks or order credit cards in *your* name and mail them to *their* address. Do the same with other sensitive information like credit card receipts, banking statements, utility bills, and so on. Home shredders can be purchased in most office supply and discount stores for minimal cost. By adopting responsible information handling practices, you can reduce the risk of fraud.
22. When you fill out credit or loan applications, find out how the company disposes of them. If you are not convinced that they store them in locked files and/or shred all paper records before discarding them, take your business elsewhere. Some auto dealerships, department

stores, car rental agencies, and video stores have been known to be careless with customer applications or an employee at the business with "insider access" may retrieve your personal information to sell or use fraudulently. When you pay by credit card, ask the business how it stores and disposes of the transaction slip. Avoid paying by a check or debit card if you think the business does not use adequate safeguards.

23. Store your canceled checks in a safe place. In the wrong hands, they could reveal a lot of about you, including information about your other accounts by looking through the payments you have made, so avoid writing individual account numbers on the "memo" portion of each check. Never permit your credit card number to be written onto your checks. Iowa law prohibits a merchant from recording your credit card number or expiration date as a condition of acceptance of a check for the sale of goods or services. Iowa law does NOT prohibit a merchant from requesting that you display a credit card, and it allows the merchant to record only the name and issuer (bank name) of the credit card. However, a credit card number may be requested and recorded in lieu of a deposit to secure payment in the event of loss, damage, or default. (Iowa Code section 537.8101)
24. "Privacy notices" are being mailed to consumers annually in their bank statements, credit card statements, investment reports, mortgage statements, insurance mailings and so on. The Financial Services Modernization Act (also known as Gramm-Leach-Bliley or GLB)(15 U.S.C. sections 6801-6810) requires banks and other companies that provide financial services and products to tell their customers three things:

1. **Privacy Policy:** Your financial institution must tell you the kinds of information it collects about you and how it uses that information.
2. **Right to Opt-Out:** Your financial institution must explain your ability to prevent the sale of your personal information to third parties.
3. **Safeguards:** Financial institutions are required to develop policies to prevent fraudulent access to confidential financial information. These policies must be disclosed to you.

The burden is on YOU to opt-out... that is how to say "no" if the company wants to sell you personal information to or share it with other businesses (third party non-affiliates). If you say nothing, or you throw the privacy notice in the filing cabinet or in the trash, it means "you are giving that business wide authority to sue your personal information (such as your address, birth date, Social Security number, credit rating, spending habits, and so on)." So, the next time you get a privacy notice in the mail, make an affirmative decision on how you would like to share your personal information!

25. Magazines, credit card companies, clubs and organizations, charities, manufacturers and retailers make lists of their subscribers, customers, members and donors available to other businesses for a fee. Your information is reproduced and sold in countless ways. You should always exercise caution when you are making personal identifying information available when using the Internet, mailing a rebate/survey/warranty card, entering a drawing or sweepstakes, donating money, and even subscribing to magazines.

26. When in public places, always be aware of your surroundings. Thieves commonly use a distraction in cramped public places, such as elevators, escalators and revolving doors to "bump and lift" your money, identification, and credit cards. Be especially cautious with bags and purses that can be an easy target for a thief to "grab and run."

*If you have any further questions or concerns,
or if you would like additional information, please contact:*

Iowa Attorney General Tom Miller

Consumer Protection Division

Hoover State Office Building

1305 East Walnut Street

Des Moines, IA 50319

www.IowaAttorneyGeneral.org

Consumer@AG.State.IA.US

515-281-5926

888-777-4590