Placing a Security Freeze on Your Credit Report

Any consumer in Illinois may place a security freeze on his or her credit report by requesting one in writing by certified mail to the credit reporting agency. A security freeze prohibits (with certain exceptions) the credit reporting agency from releasing the consumer's credit report, or any information from it, without the consumer's express authorization.

The credit reporting agency may charge up to $10 each time it places, removes, or temporarily lifts a security freeze. Senior citizens 65 years of age or older will not be charged to place or permanently lift the security freeze, but may be charged up to $10 for each temporary lifting of a freeze.

Victims of identity theft will not be charged any fees for placing, removing, or temporarily lifting a security freeze.

HOW TO FREEZE YOUR CREDIT REPORT

A security freeze means that your credit report cannot be shared with potential creditors. A security freeze can help prevent identity theft, because most businesses will not open credit accounts without first checking a consumer's credit history. If your credit report is frozen, even someone who has your name and Social Security number probably will not be able to obtain credit in your name.

How do I place a security freeze?

To place a freeze, you must write to each of the three credit bureaus. Credit bureaus charge a $10 fee to place a security freeze, unless you are at least 65 years old, in which case there is no fee. Victims of identity theft will not be charged a fee to place the freeze.

Write to all three addresses below and include the information that follows:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013

Trans Union Security Freeze
P.O. Box 6790
Fullerton, CA 92834-6790

For each, you must:

- Send a letter by certified mail;
- If you are a victim of identity theft, you must include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft;
- Provide your full name (including middle initial as well as Jr., Sr., II, III, etc.), address, Social Security number, and date of birth;
- If you have moved in the past 5 years, supply the addresses where you have lived during that period;
- Provide proof of current address such as a current utility bill or phone bill;
- Send a photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
- If applicable, include payment by check, money order or credit card (Visa, MasterCard, American Express, or Discover cards only).

How long does it take for a security freeze to take effect?

Within five (5) business days after receiving your letter, the credit reporting agencies listed above will place a freeze on providing credit reports to potential creditors.

Within 10 business days after receiving your letter to place a freeze on your account, the credit reporting agencies will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep this PIN or password in a safe place.

Can I open new credit accounts if my files are frozen?

Yes. You can have a security freeze temporarily lifted for a specified period of time or for a specific business. There is up to a $10 charge for either temporarily lifting the security freeze or allowing a specific potential creditor to access your credit report. Victims of identity theft can temporarily lift the security freeze or allow a specific party to access their credit report at no charge. The steps to temporarily lift a security freeze or to allow a specific potential creditor to access your credit report are as follows:

- Contact the credit reporting agencies above;
- The manner by which you contact them is determined by them, but it may be by way of telephone, fax, Internet or mail;
- You must provide proper identification;
- You must provide your unique PIN or password; and
- You must specify during what time period your credit report will be accessible to potential creditors (for example: August 1 to August 5) or for which potential creditor you want the security freeze lifted (for example: Sears).

How long does it take for a security freeze to be lifted?

Credit bureaus must lift a freeze no later than three business days after receiving your request.

What will a potential creditor who requests my file see if it is frozen?

A potential creditor will see a message or a code indicating the file is frozen.

Can a potential creditor get my credit score if my file is frozen?

No. A potential creditor who requests your file from one of the three credit bureaus will only get a message or a code indicating that the file is frozen.

Can I order my own credit report if my file is frozen?

Yes.

Can anyone see my credit file if it is frozen?

When you have a security freeze on your credit file, certain entities still have access to it. Your report can still be released to your existing creditors or to collection agencies acting on their own behalf. They can use it to review or collect on your account. Other creditors may also use your information to make offers of credit. Government agencies may also have access in response to a court or administrative order, a subpoena, or a search warrant.

Do I have to freeze my file with all three credit bureaus?

Yes. Different credit issuers may use different credit bureaus. If you want to stop your credit file from being viewed, you must freeze it with Equifax, Experian, and Trans Union.

Will a freeze lower my credit score?

No.

To protect my credit, should my spouse's credit file be frozen too?

Yes.

Does freezing my file mean that I won't receive pre-approved credit offers?

No. You can stop the pre-approved credit offers by calling 1-**888-5-OPTOUT (1-888-567-8688).** Or you can do this online at **www.optoutprescreen.com**. This will stop most of the offers, such as the ones that go through the credit bureaus. The opt out request lasts for five years, or you can make it permanent.

SAMPLE CREDIT BUREAU LETTER FOR PLACING A SECURITY FREEZE
(MUST BE SENT BY CERTIFIED MAIL)

Date

(NAME OF BUREAU) Security Freeze
P.O. Box 000000
City, STATE 00000

Dear (NAME OF BUREAU):

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 years. 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).

Circle one of the following:

I have included a $10 fee to place a security freeze on my credit file.

OR

I am a senior (at least 65 years old) and the fee does not apply to me. OR
I am an identity theft victim and a copy of my police report (or other investigative report or complaint to a law enforcement agency concerning identity theft) regarding identity theft is enclosed.

Yours truly,

Your Name

LISA MADIGAN
ILLINOIS ATTORNEY GENERAL

Breach Notification

Security breaches have become increasingly common in recent years. As more and more companies use computer systems to "warehouse" their customers' personal information, the potential for "leaks" of this information increases. These leaks can occur in a number of ways. A large number of these breaches are attributable to computer hacking. Hackers break into seemingly secure computer systems and steal consumers' personal information to use for their own benefit. Another common cause of security breaches is employee misconduct. Employees violate company policy and abuse their privileges to access consumers' personal information and then use or sell it. Finally, many security breaches occur accidentally. A company unintentionally prints your Social Security number on a label that is then sent out through the mail, or a document containing the personal information of thousands of customers is accidentally released to the public.

Illinois law requires companies to notify you when there has been a breach of security and your personal information may be at risk. These notifications do not necessarily mean that your identity has been stolen, but they should be taken seriously. Illinois law requires companies that suffer breaches to notify consumers within a "reasonable time." Many larger companies stagger their notification letters, so if you know someone who received a letter before you, that does not necessarily mean that the company did not act reasonably.

Most large companies have a procedure in place that is implemented the moment they learn of a security breach. This procedure could include a special toll-free number or website with frequently asked questions or important and useful links. Many companies will work with one or all of the credit reporting agencies to set up credit monitoring services for affected consumers.

We encourage consumers to utilize the special toll-free numbers or websites set up by companies who have suffered breaches. Similarly, if the breach notification letter offers credit monitoring services, we recommend that consumers take advantage of that offer. It is probably not necessary to pay for these services, but they are often offered at no charge to affected consumers.

A security breach of your personal information will not entitle you to all of the protections that a victim of identity theft would receive, but there are still several steps you can take to protect yourself.

Breach Checklist

- **Check with your creditors.** Work with your credit card companies, banks, and other lenders to determine if any suspicious or unauthorized activity has occurred on your accounts.

- **Cancel credit cards that have been lost or stolen.**

- **Place an initial fraud alert on your credit report. Order your free copy of your credit report and review it for problems.**
  Contact the toll-free number of any of the three consumer reporting companies to place a fraud alert on your credit report. You only need to contact one of the three companies

because that company is required to contact the other two.

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

Once you place a fraud alert on your file, you are entitled to a free copy of your credit report. The credit reporting agencies will send you a letter telling you how to order your free report. When you receive your credit reports, review them carefully and look for any suspicious activity.

- **Remain alert.**
  This is always a good idea, but it is especially important in the first year following a security breach notification. Take advantage of your right to one free copy of your credit report from each of the three consumer reporting companies per year. Request a report from one of the reporting companies every four months and carefully review this report for suspicious activity.

  To obtain the free reports, consumers can call 1-877-322-8228 or order online at www.annualcreditreport.com or link to free reports from www.illinoisattorneygeneral.gov. Be on the lookout for warning signs that your information is being misused. Such signs include:
  - Receiving credit cards for which you did not apply;
  - Being denied credit or offered credit at less favorable terms for no apparent reason;
  - Receiving calls or letters from debt collectors or businesses about merchandise or services you did not buy; and
  - Missing bills and other pieces of mail.

- **Be aware that if there are unauthorized charges on your credit report, you may be the victim of identity theft.**

For more information, please contact us.

Chicago	**Springfield**	**Carbondale**
100 W. Randolph Street	500 S. Second Street	1001 E. Main Street
Chicago, IL 60601	Springfield, IL 62706	Carbondale, IL 62901
(312) 814-3000	(217) 782-1090	(618) 529-6400/6401
TTY: (800) 964-3013	TTY: (877) 844-5461	TTY: (877) 675-9339

Please visit www.IllinoisAttorneyGeneral.gov

Just Hang Up!

The Best Way to Avoid Telephone Scams Is Also the Easiest.

Every day, seniors throughout Illinois fall prey to smooth-talking con artists who call them up and tell all kinds of convincing stories to get their money.

The Office of the Illinois Attorney General wants you to know that it's shrewd, not rude, to hang up the phone when a stranger asks you to send them money or give out your personal information.

The following are some common warning signs of telephone scams. If you spot any of these signs while on the phone, don't think twice:

Just Hang Up!

THEY CONTACT YOU. When you look up the number of a reputable business on your own and call to place an order, you have a good idea who's on the other end of the deal. But when the tables are turned and someone calls you, you have no way of knowing who the person really is, where they're calling from, or what they want from you. *Just Hang Up!*

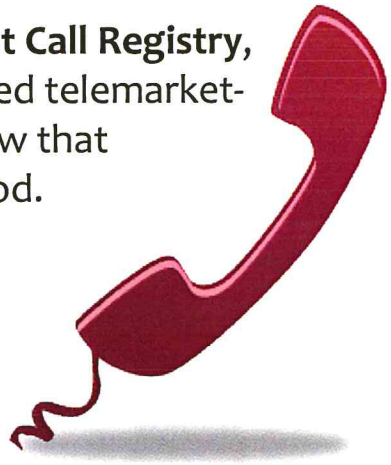
THEY WANT YOUR PERSONAL INFORMATION. Any time a stranger asks you for your bank account number, Social Security number, or other sensitive information, you should be on high alert. This is a sure sign of identity theft. ***Never*** give personal or financial information to someone you do not know. *Just Hang Up!*

Just Hang Up!

THEY PROMISE A BIG AWARD. Scammers try to lure you in with promises of unexpected riches such as a large sum of money, a vacation, or a "get rich quick" investment scheme. Remember: If it sounds too good to be true, it probably is. *Just Hang Up!*

YOU MUST PAY THEM FIRST. It is illegal for someone to require an up-front payment to claim a lottery or sweepstakes prize. Scammers will often tell you that you must wire money out of state, or even out of the country, to obtain your winnings. ***Never*** wire money to a stranger. Wiring money is just like sending cash—scammers will get the money quickly, and you won't get it back. *Just Hang Up!*

Consider placing your phone number on the **National Do Not Call Registry**, if you haven't already done so. This will block most unwanted telemarketing calls. So, once your number is on the registry, you'll know that any telemarketer who does call you is probably up to no good. You can register your home phone or cell phone online at www.donotcall.gov or by calling **1-888-382-1222 (TTY: 1-866-290-4236)** from the phone number you wish to register.



If you've fallen victim to or want to report a telephone scam, please contact the **Illinois Attorney General's Consumer Fraud Hotline** at 1-800-386-5438 (TTY: 1-800-964-3013) or **Senior Fraud Helpline** at 1-800-243-5377 (TTY: 1-800-964-3013).

LISA MADIGAN
ILLINOIS ATTORNEY GENERAL

LISA MADIGAN
ILLINOIS ATTORNEY GENERAL

BEWARE OF IRS IMPOSTORS

It's Probably a SCAM!

Illinois Attorney General Lisa Madigan warns consumers about scammers who pretend they are with the government to scare you into sending money.

DON'T BE A VICTIM

- Phony IRS scammers are targeting taxpayers around the country.
- Victims are told they owe money to the IRS and must pay immediately through a prepaid debit card or wire transfer.
- Victims are threatened with arrest, deportation or suspension of driver's or business licenses.
- If victims say no or question the scammers, the scammers may become hostile and insulting.

If you get a call like this, JUST HANG UP!

TRICKS GOVERNMENT IMPOSTORS USE

IRS scammers may...

- Use a fake name and IRS badge number.
- Know the last four digits of your Social Security number.
- Spoof a fake IRS toll-free number on caller ID.
- Send phony IRS letters by mail or email in an attempt to make you believe the fake call.
- Call back and pretend to be from the local police, FBI or Department of Motor Vehicles (DMV) to convince you that the call is legitimate.

WHAT TO DO IF YOU GET A SUSPICIOUS CALL

If you get a call...

- And you know you don't owe taxes, call the Treasury Inspector General for Tax Administration at 1-800-366-4484 to report the scam.
- And you may owe taxes, call the IRS at 1-800-829-1040 for help.
- Report the call to the Federal Trade Commission Consumer Helpline at 1-877-382-4357 or visit www.ftc.gov/complaint to report the scam. Include the phrase "IRS Telephone Scam" in your comments.

Illinois Attorney General Consumer Fraud Hotlines

Chicago	Springfield	Carbondale
1-800-386-5438	1-800-243-0618	1-800-243-0607
1-800-964-3013 (TTY)	1-800-844-5461 (TTY)	1-877-675-9339 (TTY)

SOCIAL SECURITY BENEFITS SCAM TARGETS SENIORS

The Office of the Illinois Attorney General and the Social Security Administration (SSA) are warning seniors about a new scam to steal Social Security benefits.

THE SCAM

Identity thieves are fraudulently re-routing Social Security benefits to their own bank accounts and prepaid debit cards. The identity thieves get their hands on your personal information by posing as Social Security Administration employees or health care providers working to make sure their records are accurate. The scammers call, email or send a letter asking for personal data such as your:

- Social Security number
- Birth date
- Mother's maiden name
- Bank account information

This information can then be used to steal your identity and your money. After obtaining the information, the scammers contact the Social Security Administration and request that your payments be rerouted to their accounts.

HOW TO AVOID BECOMING A TARGET

Never provide your Social Security number, bank account information or other personal information over the telephone or to someone you have just met unless you initiated the call or contact.

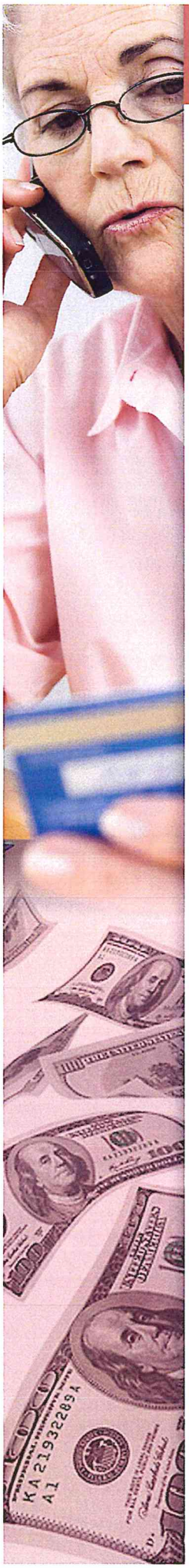
Remember, a Social Security representative or health care provider will not contact you by email, but **may reply to you** by phone or letter if you've applied for benefits or medical services.

WHEN IN DOUBT...CHECK IT OUT

Before providing any information regarding your Social Security number, call the Social Security Administration directly at 1-800-772-1213 (TTY: 1-800-325-0778) or visit your local SSA office to verify the request.

If you have been the victim of identity theft, contact the Illinois Attorney General's Identity Theft Hotline at 1-866-999-5630 (TTY: 1-877-844-5461).

LISA MADIGAN
ILLINOIS ATTORNEY GENERAL



HOW TO AVOID "THE GRANDPARENT SCAM"

Grandparents will do almost anything for their grandkids. Don't let criminals impersonating your grandkids take your money.

In a "grandparent scam," you get a call or an email from someone who claims to be your grandchild. The caller says there's an emergency and asks you to wire money immediately. The "grandchild" claims he or she has gotten into some kind of trouble: for example, they have been in an auto accident, have been mugged, need money for bail or must pay customs fees to get back into the United States from another country. The scammer says, "Grandma/Grandpa, can you please help me? But don't tell Mom or Dad." **Beware**—there's a good chance this is an imposter trying to take your money!

Scammers will often try to trick you into providing information that helps them impersonate your grandchild.

Typical conversation:

You receive a phone call from someone who greets you with, "Hi, Grandma."

You: "Hi."

Scammer: "Do you know who this is?"

You: "Jeremy?"

Scammer: "Yes, Grandma, this is Jeremy!"

Without knowing it, you supplied the scammer with the name of a grandchild. The scammer proceeds to impersonate your grandchild and asks you not to tell other family members until it's too late.

If someone calls, emails or sends a text message claiming to be a family member or a friend desperate for money, take the following steps.

Stop: Verify the emergency! Don't keep it a secret!

- Resist the urge to act immediately, no matter how dramatic the story.
- Verify the person's identity by asking questions that a stranger couldn't possibly answer.
- Call the family member at a phone number that you know to be genuine.
- Check the story out with someone else in your family or circle of friends, even if you've been told to keep it a secret.
- Don't wire money or send a check or money order by overnight delivery or courier.

Report this type of call or any strange unsolicited calls asking you to send or wire money to the Illinois Attorney General's Senior Citizen Consumer Fraud Hotline at 1-800-243-5377.

LISA MADIGAN
ILLINOIS ATTORNEY GENERAL

FRAUD ALERTS • FRAUD ALERTS • FRAUD ALERTS

Protect Yourself From Scams

The following are some of the most common scams perpetrated against seniors. Read on to familiarize yourself with these schemes and protect your finances.

IRS Scam Calls

A scam artist claims to be from the IRS and tells the caller they owe back taxes. Money must be paid immediately through a prepaid debit card or wire transfer to avoid arrest or legal consequences. The scammers spoof numbers to appear to be calling from the Washington, DC, area code 202.

Grandparents Scam

Scam artists claiming to be attorneys, paralegals and law enforcement officers frantically call saying that a grandchild is in trouble and requesting the grandparent immediately wire money or send a prepaid debit card.

Prizes/Sweepstakes/Free Gifts Scam

A scam artist mails a letter or calls you and pretends to be with Reader's Digest, Publisher's Clearing House, a government agency or a phony foreign lottery. The scam artist claims that you have "won" money and tells you that you must wire hundreds or even thousands of dollars to the scam artist to cover taxes or some other bogus fees. You wire money or send a prepaid debit card, but the prize never arrives.

Home Improvement/Doorstep Scam

A scam artist knocks on your door offering to repair something in or around your home. They ask you to pay upfront and you never see the alleged repairman again.

Charity Scam

A caller claims to collect money for needy children, veterans, or victims of a recent disaster. Always research charities before making a donation to ensure that the charity is registered with the Attorney General's office as required by law.

Mortgage/Reverse Mortgage Scam

A con artist offers you a free home, investment opportunities, or mortgage foreclosure or refinancing assistance. You may hear about such schemes through investment seminars as well as via television, radio, billboard, and mailer advertisements, and even from people you know.

Computer Tech Support Scam

The scammers may call or send an email offering to help solve your computer problems or sell you a software license. Once they are given access to your computer, they can install malicious software that can capture sensitive data, such as online banking user names and passwords; try to control your computer remotely and adjust settings to leave your computer vulnerable; request credit card information so they can bill you for phony services; or direct you to fraudulent websites and ask you to enter credit card or other personal or financial information there.

Phishing/Spoofing Scam

Scam artists claiming to represent government agencies, local utilities, charities, banks or law enforcement call, mail, email or make door-to-door solicitations requesting your personal information.

Wandering Contractors Scam

A scam artist comes to your door and pretends that you have a tree that needs trimming or a roof in need of repair to distract you while another person sneaks into your home to steal cash and valuables.

Investment/Ponzi Scheme

A scam artist encourages you to make investments and promises unrealistically high returns.

Friendship/Sweetheart Scam

A scam artist nurtures an online relationship, building trust and confidence, then convinces you to send money.

Work-At-Home Scam

A scam artist promises you big money to work from home assembling products, establishing an online business, or mystery shopping. You may invest hundreds of dollars for start-up with little, if any, return in payment.

Free Trial Offer Scam

A scam artist uses television advertisements and unwanted telephone calls offering free goods and services and then asks for your credit card information. Time passes and you don't realize that you are being billed every month for that free trial offer.

Bereavement Scam

Scammers often try to take advantage of senior citizens who have recently lost a loved one, such as a spouse. Scammers call, claim that the deceased spouse has outstanding debts that must be paid immediately, and ask for a blank check or credit card information for payment.

Illinois Attorney General Consumer Fraud Hotlines

Chicago	Springfield	Carbondale
800-386-5438	800-243-0618	800-243-0607
800-964-3013 (TTY)	877-844-5461 (TTY)	877-675-9339 (TTY)