IDENTITY THEFT

Resource Guide

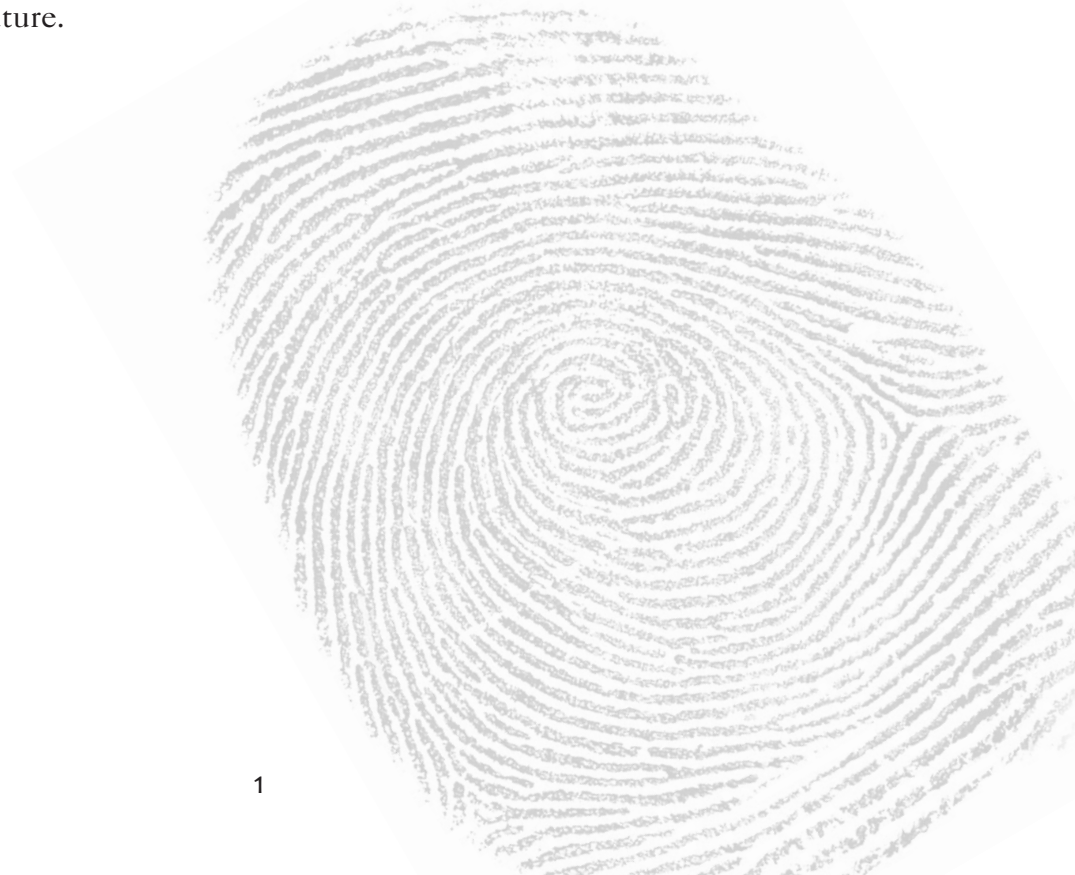
LISA MADIGAN
ILLINOIS ATTORNEY GENERAL

TABLE OF CONTENTS

INTRODUCTION

What do you do in the course of your day? How much of what you do leaves you open and vulnerable to identity theft? Maybe you call your bank on the train during your morning commute and you provide them with your Social Security number for security purposes. How many people could have overheard those numbers? While walking into your office perhaps you stop to mail a credit card application. What sort of personal information is on that application? During a break at work maybe you take a minute to pay a few bills online. Is the website you used secure, and how safe is your computer at your office? When you are finally home for the evening maybe you decide to go through some mail that has been collecting. In sorting through the pile of mail, you throw out some junk mail and some bills that you have paid. Where does that trash go and how easily could it be picked through by a stranger?

You would not leave the doors and windows to your home wide open allowing anyone to come in and take what they want. Instead we take preventative measures to protect our belongings: we lock doors and windows, install alarm systems, and stay alert. Our personal information should be treated with the same care and precautions. Tools such as fraud alerts, security freezes, and opt-outs are available to you to help lock up your personal information. The Office of the Illinois Attorney General has produced this booklet to help you learn to use these tools and to remedy the effects of an identity theft. Here you will find information concerning what steps to take, your legal rights, how to handle specific problems you may encounter on the way to clearing your name, and what to watch for in the future.



ID THEFT VICTIMS: IMMEDIATE STEPS

The process of reclaiming your credit can be frustrating, but don't give up. **The Illinois Attorney General's Identity Theft Hotline** has several resources to help you, including trained advocates to guide you through the process: **1-866-999-5630; TTY: 1-877-844-5461**. Just remember that it is critical that you act quickly to minimize any damage.

HELPFUL HINTS

As you begin this process there are a few things to keep in mind. Keeping a written record of your efforts is a must. The following are important tips to help you:

- Record dates, names, phone numbers, report or file numbers, and notes from any important conversations.
- In order to confirm, always follow up a conversation with a written communication.
- Send everything by certified mail, return receipt requested.
- Keep copies of all letters and documents. Remember never to send originals, only copies.

CONSUMER CHECKLIST

The following are the basic but essential steps one should take in nearly all instances of identity theft. **If you call our Identity Theft Hotline, the consumer advocate assigned to your case can assist you in accomplishing these steps:**

- **Report fraud to creditors.**
  Check with your credit card companies and banks to see if any new accounts have been opened in your name or if any unauthorized charges have been made. Work with these companies to immediately stop further damage. You may wish to close accounts immediately, but remember to make sure that all outstanding checks clear before you close your bank accounts. Once you verify that all legitimate checks have cleared, talk to your bank about closing compromised accounts and setting up new password-protected accounts.

  After you have notified banks and credit card companies of the fraud, you should also alert your other creditors, including phone companies, utility providers, Internet service providers, and other service providers.

- **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 credit reporting agencies to place a fraud alert on your credit report. You only need 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 2000, Chester, PA 19016

  Once you place a fraud alert on your file, you are entitled to a free copy of your credit report. The three companies use automated systems to place alerts. These automated systems generate letters advising you of your right to a credit report. Follow the instructions in the letter for receiving your free credit report because the credit reporting agencies will not send it to you unless you make a request. When you receive your credit reports, review them carefully and look for any suspicious activity.

- **File a police report.**
  Illinois law requires police departments to accept and provide reports. Get a copy of the police report or, at the very least, the number of the report. It can help you deal with creditors who need proof of the crime.

- **Decide whether you want to place a security freeze on your credit report.**
  A security freeze is different from a fraud alert. It allows you to prohibit your credit report from being released to another person without your prior express authorization. This also means that you will be unable to obtain credit without first providing the credit reporting agency with proof of your identity.

  As of June 8, 2018, security freezes are available to all Illinois residents free of charge.

- **Remain alert.**
  Remaining alert is always a good idea, but especially in the first year following a security breach notification or identity theft.

  Keep your information current with the Attorney General's office and all other agencies where you have reported the fraud.

These initial five steps are described in further detail in the next section. Remember to keep a detailed record of all correspondence. Refer back to this checklist as needed as you go through the process of reclaiming your identity.

MY IDENTITY WAS STOLEN—WHAT DO I DO?

1. REPORT THE FRAUD TO EACH OF YOUR CREDITORS AND WORK WITH THEM TO CLOSE ANY ACCOUNTS THAT HAVE BEEN TAMPERED WITH OR OPENED FRAUDULENTLY.

Call and speak with someone in the security or fraud department of each company supplying your credit. Follow up in writing, and include copies (NOT originals) of supporting documents. It is important to notify credit card companies and banks in writing. Send your letters by certified mail, return receipt requested, so you can document what the company received and when. Keep a file of your correspondence and enclosures.

When you open new accounts, use new Personal Identification Numbers (PINs) and passwords. Avoid using easily available information like your mother's maiden name, your birth date, the last four digits of your Social Security number (SSN) or your phone number, or a series of consecutive numbers.

Credit/Debit Accounts

For charges and debits on existing credit accounts, ask the representative to send you the company's fraud dispute forms. If the company doesn't have special forms, use the sample letter on page 34 to dispute the fraudulent charges or debits. In either case, write to the company at the address given for "billing inquiries," NOT the address for sending your payments.

For new unauthorized accounts, ask if the company accepts the ID Theft Affidavit (see page 41). If not, ask the representative to send you the company's fraud dispute forms.

The Fair Credit Billing Act establishes procedures for resolving billing errors on your credit card accounts, including fraudulent charges on your accounts. The law also limits your liability for unauthorized credit card charges to $50 per card. To take advantage of the law's consumer protections, you must:

- Write to the creditor at the address given for "billing inquiries," NOT the address for sending your payments. Include your name, address, account number, and a description of the billing error, including the amount and date of the error. A sample letter is on page 34.

  Send your letter so that it reaches the creditor within 60 days after the first bill containing the error was mailed to you. If an identity thief changed the address on

your account and you didn't receive the bill, your dispute letter still must reach the creditor within 60 days of when the creditor would have mailed the bill. This is one reason it's essential to keep track of your billing statements and follow up quickly if your bills don't arrive on time. You should send your letter by certified mail and request a return receipt. It becomes your proof of the date the creditor received the letter. Include copies (NOT originals) of your police report or other documents that support your position. Keep a copy of your dispute letter. The creditor must acknowledge your complaint in writing within 30 days after receiving it, unless the problem has been resolved. The creditor must resolve the dispute within two billing cycles (but not more than 90 days) after receiving your letter.

If the company already has reported these accounts or debts on your credit report, dispute this fraudulent information. See "Correcting Fraudulent Information on Credit Reports," page 8.

Stolen Checks and Fraudulent Bank Accounts

If someone has stolen your checks or set up a bank account in your name, notify the bank immediately and put stop payments on missing checks. Cancel existing accounts (but be sure to ask your bank what to do about legitimate checks that haven't cleared) and obtain new accounts with a password to be used for all transactions. Illinois holds the bank responsible for losses from a forged check, but they also require you to take reasonable care of your account. For example, you may be held responsible for the forgery if you fail to notify the bank in a timely way that a check was lost or stolen.

You should also contact these major check verification companies. Ask that retailers who use their databases not accept your checks.

TeleCheck: 1-800-710-9898
Certegy, Inc.: 1-800-437-5120

Call SCAN at 1-800-262-7771 to find out if the identity thief has been passing bad checks in your name.

Chex Systems, Inc., produces consumer reports specifically about checking accounts, and as a credit reporting agency, is subject to the Fair Credit Reporting Act. You can request a free copy of your consumer report by contacting Chex Systems, Inc.

Chex Systems, Inc.
1-800-428-9623
www.chexhelp.com
Fax: 602-659-2197
Chex Systems, Inc.
Attn: Consumer Relations
7805 Hudson Road, Suite 100
Woodbury, MN 55125

Once you have resolved your identity theft dispute with the company, ask for a letter stating that the company has closed the disputed accounts and has discharged the fraudulent debts. This letter is your best proof if errors relating to this account reappear on your credit report or you are contacted again about the fraudulent debt.

2. PLACE A FRAUD ALERT ON YOUR CREDIT REPORT AND REQUEST A COPY OF YOUR CREDIT REPORT.

Fraud alerts can help prevent an identity thief from opening any more accounts in your name. Contact the toll-free fraud number of any of the three credit reporting agencies below to place a fraud alert on your credit report. You need to contact only one of the three companies to place an alert. The company you call is required to contact the other two, and they will also place an alert on their versions of your report. As of September 21, 2018, an initial fraud alert will last for one year, and you can renew the initial alert for 7 more years.

- **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 2000, Chester, PA 19016

Once you place the fraud alert in your file, you are entitled to order free copies of your credit reports, and, if you ask, only the last four digits of your SSN will appear on your credit reports.

Once you get your credit reports, review them carefully. Look for inquiries from companies you have not contacted, accounts you did not open, and debts on your accounts that you cannot explain. Check that information such as your SSN, address(es), name or initials, and employers is correct. If you find fraudulent or inaccurate information, get it removed (see "Correcting Fraudulent Information on Credit Reports" to learn how). Continue to check your credit reports periodically, especially for the first year after you discover the identity theft, to make sure no new fraudulent activity has occurred.

In addition, you should request that a victim's statement be added to your reports so creditors know to call you before opening any new accounts or changing existing accounts.

> **A Note on Security Breach Notices:** 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 still be taken seriously. If you receive a breach notice, go through the initial steps of placing fraud alerts on your credit reports and check those reports often. Be alert for any suspicious activity on your report.

Correcting Fraudulent Information on Credit Reports

The Fair Credit Reporting Act (FCRA) establishes procedures for correcting fraudulent information on your credit report and requires that your report be made available only for certain legitimate business needs. Under the FCRA, both the credit reporting agency and the information provider (the business that sent the information to the credit reporting agency, such as a bank or credit card company) are responsible for correcting fraudulent information in your report. To protect your rights under the law, contact both the credit reporting agency and the information provider.

Credit Reporting Agency Obligations

Credit reporting agencies will block fraudulent information from appearing on your credit report if you take the following steps:

1. Send them a copy of the police report.

2. Send a letter telling them what information is fraudulent and that the information does not relate to any transaction that you made or authorized.

3. Provide proof of your identity. Proof may include your SSN, name, address, and other personal information requested by the credit reporting agency.

The credit reporting agency has four business days to block the fraudulent information after accepting your identity theft report. It also must tell the information provider that it has blocked the information. The credit reporting agency may refuse to block the information or remove the block if, for example, you have not told the truth about your identity theft. If the credit reporting agency removes the block or refuses to place the block, it must let you know.

The blocking process is only one way for identity theft victims to deal with fraudulent information. There's also the "reinvestigation process," which was designed to help all consumers dispute errors or inaccuracies on their credit reports.

Information Provider Obligations

Information providers stop reporting fraudulent information to the credit reporting agencies once you send them an identity theft report and a letter explaining that the information they are reporting resulted from identity theft. You must send your identity theft report and letter to the address specified by the information provider. Note that the information provider may continue to report the information if it later learns that the information does not result from identity theft.

If a credit reporting agency tells an information provider that it has blocked fraudulent information in your credit report, the information provider may not continue to report that information to the credit reporting agency. The information provider also may not hire someone to collect the debt that relates to the fraudulent account, or sell that debt to anyone else who would try to collect it.

Credit Monitoring Services

When you request your free credit report, Equifax, Experian, and TransUnion may attempt to sell you their credit monitoring service. This service provides email notification alerts when someone is attempting to open credit in your name. Some consumers may find that they can adequately monitor their credit by exercising their rights under federal and state laws:

- You are entitled to one free credit report from each of the three credit reporting agencies every year. This means that you can receive three reports a year—one every four months.
  - Remember, although you are "entitled" to these reports, the credit reporting agencies will not send them to you automatically. You MUST request these reports online or by calling the applicable toll-free numbers (see "Getting Your Credit Report," p. 16).
- You are entitled to one free credit report under the Fair Credit Reporting Act (FCRA) when you are the victim of identity theft.
  - Request this report 6 months after reporting the theft to the credit reporting agencies.
- Illinois law allows identity theft victims to place security freezes on their credit reports. This means that no one will be able to see your report without your permission when they run a credit check. If a reputable company cannot complete a credit check, it will not issue the credit. This is FREE.

FRAUD ALERTS

There are two types of fraud alerts: an initial alert and an extended alert.

• An initial alert stays on your credit report for at least 90 days. As of September 21, 2018, initial fraud alerts will last for 1 year. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial alert is appropriate if your wallet has been stolen or if you've been taken in by a scam. When you place an initial fraud alert on your credit report, you're entitled to one free credit report from each of the three nationwide credit reporting agencies.

• An extended alert stays on your credit report for seven years. You can have an extended alert placed on your credit report if you've been a victim of identity theft and you provide the credit reporting agency with a copy of the police report. When you place an extended alert on your credit report, you're entitled to two free credit reports within 12 months from each of the three nationwide credit reporting agencies. In addition, the credit reporting agencies will remove your name from marketing lists for pre-screened credit offers for five years—unless you ask them to put your name back on the list before then.

To place either of these alerts on your credit report, you will be required to provide appropriate proof of your identity, which may include your SSN, name, address, and other personal information requested by the credit reporting agency. To remove the fraud alert, you will need a copy of an identity theft report and proof of your identity.

3. FILE A REPORT WITH YOUR LOCAL POLICE DEPARTMENT.

You should initiate a law enforcement investigation by contacting the local law enforcement agency, which will take a police report of the matter, provide you with a copy of that report, and begin an investigation of the facts or, if the suspected crime was committed in a different jurisdiction, refer the matter to the law enforcement agency where the suspected crime was committed. Illinois law requires police departments to accept and provide reports. Get a copy of the police report or, at the very least, the number of the report. It can help you deal with creditors who need proof of the crime.

PROVING YOU'RE A VICTIM

Applications or other transaction records related to the theft of your identity may help you prove that you are a victim. For example, you may be able to show that the signature on an application is not yours. These documents also may contain information about the identity thief that is valuable to law enforcement.

By law, companies must give you a copy of the application or other business transaction records relating to your identity theft if you submit your request in writing. Be sure to ask the company representative where you should mail your request. Companies must provide these records at no charge to you within 30 days of receipt of your request and your supporting documents. You also may give permission to any law enforcement agency to get these records, or ask in your written request that a copy of these records be sent to a particular law enforcement officer. The company can ask you for:

• **Proof of your identity.** This may be a photocopy of a government-issued ID card, the same type of information the identity thief used to open or access the account, or the type of information the company usually requests from applicants or customers, and

• **A police report and a completed affidavit,** which may be the Identity Theft Affidavit (see page 41) or the company's own affidavit.

4. PLACE A SECURITY FREEZE ON YOUR CREDIT REPORT.

Security freezes are available to all Illinois residents. A security freeze prevents third parties from accessing your credit report without your express authorization.

To obtain more information on how to place a security freeze on your credit reports, see page 13.

Placing a Security Freeze

As of September 21, 2018, credit reporting agencies are required to provide at least 3 different methods for you to request a security freeze: toll-free telephone number, secure electronic method, and written request by mail. For all methods to request a freeze, you must provide the credit reporting agency with proper identification.

A credit reporting agency shall place a security freeze on your credit report no later than 1 business day after receiving your freeze request by toll-free telephone number or secure electronic method and 3 business days after receiving your written request by mail. Upon placing the security freeze on your credit report, the credit reporting agency also must send you, within 5 business days, written confirmation of the security freeze and information on how to lift the freeze, including the way they intend to verify your identity.

Temporarily Lifting a Security Freeze

If you want your credit report to be accessed for a specific period of time while a freeze is in place, you must contact the consumer credit reporting agency using a point of contact designated by the consumer reporting agency, and request that the freeze be temporarily lifted. In order to do so you will again have to provide proper identification, including the method of identification they provided to you at the time you placed the freeze. A credit reporting agency has 1 hour in which to comply with your request to lift your security freeze if you request the temporary lift by toll-free telephone number or secure electronic method. If you request the temporary lift by mail, the credit reporting agency has 3 business days after receiving your request.

Removing a Security Freeze

A security freeze will remain in place until you request that it be removed. To remove your security freeze, you must provide proper identification, including the method of identification they provided to you at the time you placed the freeze. A credit reporting agency has 1 hour in which to comply with your request to lift your security freeze if you request the temporary lift by toll-free telephone number or secure electronic method. If you request the temporary lift by mail, the credit reporting agency has 3 business days after receiving your request.

5. REMAIN ALERT.

There are many precautionary measures you can take to ensure that your personal information remains protected. One of the most important steps is to monitor your own credit report and look for suspicious activity. **Take advantage of your right to one free copy of your credit report from each of the three credit reporting agencies 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, call 1-877-322-8228 or order online at www.annualcreditreport.com.

Free reports can also be accessed by going to www.illinoisattorneygeneral.gov, clicking on the section labeled “Protecting Consumers,” and then clicking on the link titled “How to Obtain a Free Credit Report.”

HOW TO FREEZE YOUR CREDIT FILES

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

How do I place a security freeze?

To place a freeze, you must contact each of the credit bureaus directly. You may contact them in writing via U.S. mail, telephone, or secure electronic method. Before using the credit bureaus' websites to place a security freeze, please ensure that your antivirus software and firewall protection are up to date, and that you are accessing the internet via a secure internet connection as opposed to an open wifi connection.

Write to all 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

TransUnion Security Freeze
P.O. Box 2000
Chester, PA 19016

For each, you must:

- 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 over the prior 5 years;
- Provide proof of current address, such as a current utility bill or phone bill; and
- Send a photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.).

Instructions for placing a security freeze via credit bureau websites:

Link to Equifax website: www.equifax.com/personal; navigate to the security freeze link and follow the instructions.

Link to Experian website: www.experian.com; navigate to the security freeze button and follow the instructions.

Link to TransUnion website: www.transunion.com; navigate to the security freeze option and follow the instructions.

Link to Innovis website: www.innovis.com; navigate to the security freeze button and follow the instructions.

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. The steps to temporarily lift a security freeze are as follows.

You must:

- Contact the credit reporting agencies above by toll-free telephone number, secure electronic method, or in writing by U.S. mail;
- Provide proper identification; and
- Specify during what time period you want your credit report to be accessible to potential creditors (e.g., August 1 to August 5).

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

A credit reporting agency shall place a security freeze on your credit report no later than 1 business day after receiving your freeze request by toll-free telephone number or secure electronic method and 3 business days after receiving your written request by mail. Upon placing the security freeze on your credit report, the credit reporting agency also must send you, within 5 business days, written confirmation of the security freeze and information on how to lift the freeze, including the way they intend to verify your identity.

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

A credit reporting agency has 1 hour in which to comply with your request to lift your security freeze if you request the temporary lift by toll-free telephone number or secure electronic method. If you request the temporary lift by mail, the credit reporting agency has 3 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 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 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, TransUnion, and Innovis.

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 888-5OPTOUT (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.

What law requires security freezes?

The Illinois security freeze law is located at 815 ILCS 505/2MM. As of September 21, 2018, security freezes are governed by 15 U.S.C. §1681c-1.

HOW CAN I PREVENT IT FROM HAPPENING AGAIN?

Once resolved, most cases of identity theft stay resolved. Occasionally, however, some victims do have recurring problems.

WARNING SIGNS OF IDENTITY THEFT

Keep watch for warning signs of identity theft to prevent revictimization.

- Failing to receive bills or other mail. Follow up with creditors if your bills do not arrive on time. A missing bill could mean an identity thief has taken over your account and changed your billing address to cover his or her tracks.
- Receiving credit cards for which you did not apply.
- Being denied credit, or being offered less favorable credit terms, like a high interest rate, for no apparent reason.
- Getting calls or letters from debt collectors or businesses about merchandise or services you did not buy.

GETTING YOUR CREDIT REPORT

Free Annual Credit Reports
To order your free annual report from one or all of the national credit reporting agencies, visit www.annualcreditreport.com, call toll-free 1-877-322-8228, or complete the Annual Credit Report Request Form and mail it to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The request form may be found at the back of this booklet, or you can print it from www.annualcreditreport.com or www.ftc.gov/credit. Do not contact the three nationwide credit reporting agencies individually. They provide free annual credit reports only through www.annualcreditreport.com, 1-877-322-8228, and Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

Other Consumer Rights to Free Reports
Under federal law, you're entitled to a free report—in addition to your one free report per year—if a company takes adverse action against you based on your report, such as denying your application for credit, insurance, or employment, and you request your report within 60 days of receiving notice of the action. The notice will give you the name, address, and phone number of the credit reporting agency. You're also entitled to one additional free report a year if you're unemployed and plan to look for a job within 60 days; you're on welfare; or your report is inaccurate because of fraud. Otherwise, a credit reporting agency may charge you up to $9.50 for another copy of your report within a 12-month period.

To buy a copy of your report, contact:

- Equifax: 1-800-685-1111; www.equifax.com
- Experian: 1-888-EXPERIAN (1-888-397-3742); www.experian.com
- TransUnion: 1-800-916-8800; www.transunion.com

GENERAL SAFEGUARDS

Take the following general safeguards to protect yourself.

- Place passwords on your credit card, bank, and phone accounts. Avoid using easily available information like your mother's maiden name, your birth date, the last four digits of your SSN or your phone number, or a series of consecutive numbers. When opening new accounts, you may find that many businesses still have a line on their applications for your mother's maiden name. Ask if you can use a password instead.

- Secure personal information in your home, especially if you have roommates, employ outside help, or are having work done in your home.

- Ask about security procedures in your workplace or at businesses, doctor's offices, or other institutions that collect your personally identifying information. Find out who has access to your personal information and verify that it is handled securely. Ask about the disposal procedures for those records as well. Find out if your information will be shared with anyone else.

- Don't give out personal information on the phone, through the mail, or on the Internet unless you've initiated the contact or are sure you know who you're dealing with. Before you share any personal information, confirm that you are dealing with a legitimate organization. Check an organization's website by typing its URL in the address line, rather than cutting and pasting it, or call customer service using the number listed on your account statement or in the telephone book. Also, many companies post scam alerts when their name is used improperly.

- Treat your mail carefully. Deposit your outgoing mail in post office collection boxes or at your local post office, rather than in an unsecured mailbox. Promptly remove mail from your mailbox. If you are planning to be away from home and cannot pick up your mail, call the U.S. Postal Service at 1-800-275-8777 to request a vacation hold. The Postal Service will hold your mail at your local post office until you can pick it up or are home to receive it.

- Dispose of trash carefully. To thwart an identity thief who may pick through your trash or recycling bins to capture your personal information, tear or shred your charge receipts, copies of credit applications, insurance forms, physician statements, checks and bank statements, expired charge cards that you are discarding, and credit offers you get in the mail.

- To opt out of receiving offers of credit in the mail, call: 1-888-5-OPTOUT (1-888-567-8688). The three nationwide credit reporting agencies use the same toll-free number to let consumers choose not to receive credit offers based on their lists. Note: You will be asked to provide your SSN, which the credit reporting agencies need to match you with your file.

- Do not carry your SSN card; leave it in a secure place.
- Ask to use other types of identifiers besides your SSN. Give your SSN out only when absolutely necessary. Illinois law prohibits your SSN from being used as your policy number for health insurance purposes.
- Carry only the identification information and the credit and debit cards that you'll actually need when you go out.
- Be cautious when responding to promotions. Identity thieves may create phony promotional offers to get you to give them your personal information.
- Keep your purse or wallet in a safe place at work; do the same with copies of administrative forms that have your sensitive personal information.

KEEPING YOUR COMPUTER AND THE PERSONAL INFORMATION IT STORES SAFE

- Virus protection software should be updated regularly, and patches for your operating system and other software programs should be installed to protect against intrusions and infections that can lead to the compromise of your computer files or passwords. Ideally, virus protection software should be set to automatically update each week. The Windows operating system also can be set to automatically check for patches and download them to your computer.
- Do not open files sent to you by strangers, or click on hyperlinks or download programs from people you don't know. Be careful about using file-sharing programs. Opening a file could expose your system to a computer virus or a program known as "spyware," which could capture your passwords or any other information as you type it into your keyboard.
- Use a firewall program, especially if you use a high-speed Internet connection like cable, DSL, or T-1 that leaves your computer connected to the Internet 24 hours a day. The firewall program will allow you to stop uninvited access to your computer. Without it, hackers can take over your computer, access the personal information stored on it, or use it to commit other crimes.
- Use a secure browser—software that encrypts or scrambles information you send over the Internet—to guard your online transactions. Be sure your browser has the most up-to-date encryption capabilities by using the latest version available from the manufacturer. You also can download some browsers for free over the Internet. When submitting information, look for the "lock" icon on the browser's status bar to be sure your information is secure during transmission.

- Try not to store financial information on your laptop unless absolutely necessary. If you do, use a strong password—a combination of letters (upper and lower case), numbers, and symbols. A good way to create a strong password is to think of a memorable phrase and use the first letter of each word as your password, converting some letters into numbers that resemble letters. For example, "I love Felix; he's a good cat," would become "1LFHA6c." Do not use an automatic log-in feature that saves your user name and password, and always log off when you're finished. That way, if your laptop is stolen, it is harder for a thief to access your personal information.

- Before you dispose of a computer, delete all the personal information it stored. Deleting files using the keyboard or mouse commands or reformatting your hard drive may not be enough because the files may stay on the computer's hard drive, where they may be retrieved easily. Use a "wipe" utility program to overwrite the entire hard drive.

- Look for website privacy policies. They should answer questions about maintaining accuracy, access, security, and control of personal information collected by the site, how the information will be used, and whether it will be provided to third parties. If you don't see a privacy policy—or if you can't understand it—consider doing business elsewhere.

ACTIVE DUTY ALERTS FOR MILITARY PERSONNEL

If you are a member of the military and away from your usual duty station, you may place an active duty alert on your credit reports to help minimize the risk of identity theft while you are deployed. Active duty alerts are in effect on your report for one year. If your deployment lasts longer, you can place another alert on your credit report. When you place an active duty alert, you'll be removed from the credit reporting companies' marketing list for pre-screened credit card offers for two years unless you ask to go back on the list before then.

For contact information for the credit reporting agencies, see page 4. The process for getting and removing an alert, and a business's response to your alert, are the same as that for an initial alert (see page 9). You may use a personal representative to place or remove an alert.

PROTECTING YOUR SOCIAL SECURITY NUMBER

You cannot always avoid giving out your Social Security number. Your employer and financial institutions, for instance, will need your SSN for wage and tax reporting purposes.

Other businesses may ask you for your SSN to do a credit check if you are applying for a loan, renting an apartment, or signing up for utilities. Sometimes, however, they simply want your SSN for general record keeping.

If someone asks for your SSN, ask:

- Why do you need my SSN?

- How will my SSN be used?
- How do you protect my SSN from being stolen?
- What will happen if I don't give you my SSN?

If you don't provide your SSN, some businesses may not provide you with the service or benefit you want. Getting satisfactory answers to these questions will help you decide whether you want to share your SSN with the business. The decision to share is yours.

Illinois Law Protects Your Social Security Number

- The Illinois Consumer Fraud and Deceptive Business Practices Act has recently been amended to afford you the following protections:
    - A person may not print your SSN on an insurance card, but rather must select an identification number unique to the holder of the card.
    - A person may not publicly post or publicly display your SSN.
    - A person may not print your SSN on any card required for you to access products or services provided by that person or entity.
    - A person may not require you to transmit your SSN over the Internet, unless the connection is secure or your SSN will be encrypted.
    - A person may not require you to use your SSN to access an Internet website, unless a password or unique personal identification number or other authentication device is also required to access the Internet website.
    - A person may not print your SSN on any materials that are mailed to you, unless state or federal law requires your SSN to be on the document to be mailed.
- Department of Revenue is now required to directly notify you, as a taxpayer, if they suspect another person has used your SSN to register a business or pay taxes and fees.
- Department of Natural Resources is phasing in new Conservation ID (CID) numbers to replace your SSN on hunting and fishing licenses. Your SSN will be on file with DNR but will not appear on the actual license.
- Protections for students:
    - A school district may not provide a student's SSN to a business or financial institution that issues credit or debit cards.
    - The University of Illinois, University of Southern Illinois, Illinois State University, Northern Illinois University, Eastern Illinois University, Western Illinois University, Chicago State University, and Governors State University may not provide a student's SSN to a business or financial

institution that issues credit or debit cards. These schools are also prohibited from printing an individual's SSN on any card or other document required for the individual to access products or services provided by the institution.

- An Illinois community college may not provide a student's SSN to a business or financial institution that issues credit or debit cards.

ADDITIONAL STEPS YOU MAY NEED TO TAKE

Depending on the extent and type of identity theft that you have experienced, additional steps may be necessary in order to protect yourself.

Bank Accounts and Fraudulent Withdrawals

Different laws determine your legal remedies based on the type of bank fraud you have suffered. For example, Illinois state laws protect you against fraud committed by a thief using paper documents, like stolen or counterfeit checks. But if the thief used an electronic fund transfer, federal law applies. Many transactions may seem to be processed electronically but are still considered "paper" transactions. If you're not sure what type of transaction the thief used to commit the fraud, ask the financial institution that processed the transaction.

Fraudulent Electronic Withdrawals

The Electronic Fund Transfer Act provides consumer protections for transactions involving an ATM or debit card, or other electronic ways to debit or credit an account. It also limits your liability for unauthorized electronic fund transfers. You have 60 days from the date your bank account statement is sent to you to report in writing any money withdrawn from your account without your permission. This includes instances when your ATM or debit card is "skimmed"—that is, when a thief captures your account number and PIN without your card being lost or stolen.

If your ATM or debit card is lost or stolen, report it immediately because the amount you can be held responsible for depends on how **quickly** you report the loss.

- If you report the loss or theft within two business days of discovery, your losses are limited to $50.
- If you report the loss or theft after two business days, but within 60 days after the unauthorized electronic fund transfer appears on your statement, you could lose up to $500 of what the thief withdraws.
- If you wait more than 60 days to report the loss or theft, you could lose all the money that was taken from your account after the end of the 60 days.

Note: Most card issuers voluntarily have agreed to limit or waive consumers' liability for unauthorized use of their debit cards, no matter how much time has elapsed since the discovery of the loss or theft of the card. Contact your card issuer for more information.

The best way to protect yourself in the event of an error or fraudulent transaction is to call the financial institution and follow up in writing—by certified letter, return receipt requested—so you can prove when the institution received your letter. Keep a copy of the letter you send for your records.

After receiving your notification about an error on your statement, the institution generally has 10 business days to investigate. The institution must tell you the results of its investigation within three business days after completing it and must correct an error within one business day after determining that it occurred. If the institution needs more time, it may take up to 45 days to complete the investigation—but only if the money in dispute is returned to your account and you are notified promptly of the credit. At the end of the investigation, if no error has been found, the institution may take the money back if it sends you a written explanation.

Fraudulent Checks and Other "Paper" Transactions

If your checks are rejected by a merchant, it may be because an identity thief is using the Magnetic Information Character Recognition (MICR) code (the numbers at the bottom of checks), your driver's license number, or another identification number. The merchant who rejects your check should give you its check verification company contact information so you can find out what information the thief is using. If you find that the thief is using your MICR code, ask your bank to close your checking account and open a new one. If you discover that the thief is using your driver's license number or some other identification number, work with your Department of Motor Vehicles or other identification issuing agency to get new identification with new numbers. Once you have taken the appropriate steps, your checks should be accepted.

Note:

- The check verification company may or may not remove the information about the MICR code or the driver's license/identification number from its database because this information may help prevent the thief from continuing to commit fraud.
- If the checks are being passed on a new account, contact the bank to close the account. Also contact Chex Systems, Inc. at 1-800-428-9623 to review your consumer report to make sure that no other bank accounts have been opened in your name.
- Dispute any bad checks passed in your name with merchants so they don't start any collections actions against you.

Stolen Driver's License or Other Government-Issued Identification

Contact the agency that issued the license or other identification document. Follow its procedures to cancel the document and get a replacement. Ask the agency to flag your file so that no one else can get a license or any other identification document from them in your name.

WHY DID IT HAPPEN TO ME?

Despite your best efforts to manage the flow of your personal information or to keep it to yourself, skilled identity thieves may use a variety of methods to gain access to your data.

HOW IDENTITY THIEVES GET YOUR PERSONAL INFORMATION

- They get information from businesses or other institutions by:
    - stealing records or information while they are on the job;
    - bribing an employee who has access to these records;
    - hacking these records; or
    - conning information out of employees.
- They may steal your mail, including bank and credit card statements, credit card offer letters, new checks, and tax information.
- They may rummage through your trash, the trash of businesses, or public trash dumps in a practice known as "dumpster diving."
- They may get your credit reports by abusing their employer's authorized access to them, or by posing as a landlord, employer, or someone else who may have a legal right to access your report.
- They may steal your credit or debit card numbers by capturing the information in a data storage device in a practice known as "skimming." They may swipe your card for an actual purchase, or attach the device to an ATM machine where you may enter or swipe your card.
- They may steal your wallet or purse.
- They may steal personal information they find in your home.
- They may steal personal information from you through email or via phone by posing as legitimate companies and claiming that you have a problem with your account. This practice is known as "phishing" online, and "pretexting" by phone.

HOW IDENTITY THIEVES USE YOUR PERSONAL INFORMATION

- They may call your credit card issuer to change the billing address on your credit card account. The imposter then runs up charges on your account, and because your bills are being sent to a different address, it may be some time before you realize there is a problem.

- They may open new credit card accounts in your name. When they use the credit cards and do not pay the bills, the delinquent accounts are reported on your credit report.

- They may establish phone or wireless service in your name.

- They may open a bank account in your name and write bad checks on that account.

- They may counterfeit checks or credit or debit cards, or authorize electronic transfers in your name, and drain your bank account.

- They may file for bankruptcy under your name to avoid paying debts they've incurred under your name, or to avoid eviction.

- They may buy a car by taking out an auto loan in your name.

- They may get identification such as a driver's license issued with their picture, in your name.

- They may get a job or file fraudulent tax returns in your name.

- They may give your name to the police during an arrest. If they don't show up for their court date, a warrant for arrest is issued in your name.

RESOLVING SPECIFIC PROBLEMS

BANKRUPTCY FRAUD

U.S. Trustee (UST)—www.usdoj.gov/ust
If you believe someone has filed for bankruptcy in your name, write to the U.S. Trustee in the region where the bankruptcy was filed. A list of the U.S. Trustee Program's Regional Offices is available on the UST website, or check the Blue Pages of your phone book under U.S. Government Bankruptcy Administration. In your letter, describe the situation and provide proof of your identity. The U.S. Trustee will make a criminal referral to law enforcement authorities if you provide appropriate documentation to substantiate your claim. You also may want to file a complaint with the U.S. Attorney and/or the FBI in the city where the bankruptcy was filed. The U.S. Trustee does not provide legal representation, legal advice, or referrals to lawyers. That means you may need to hire an attorney to help convince the bankruptcy court that the filing is fraudulent. The U.S. Trustee does not provide consumers with copies of court documents. You can get them from the bankruptcy clerk's office for a fee.

CRIMINAL VIOLATIONS

Illinois law gives victims of criminal identity theft an expedited route to getting their names cleared of crimes they didn't commit. Under the procedure, victims can petition a court for an expedited determination of their factual innocence. The procedure is available to identity theft victims where:

- The perpetrator was arrested for, cited for, or convicted of a crime under the victim's identity; or
- A criminal complaint has been filed against the perpetrator in the victim's name; or
- The victim's identity has been mistakenly associated with a criminal conviction.

The prosecuting attorney can petition the court for the determination, or the court can even act on its own motion. You, as the identity theft victim, can also petition the court for the determination on your own.

If the court determines that the petition has value and that there is no reasonable cause to believe that the identity theft victim committed the offense, or if the court finds that the victim's identity has been mistakenly associated with a record of criminal conviction, the court shall find the victim factually innocent of that offense. If the victim is found factually innocent, the court shall issue an order certifying this determination.

After a court has issued a determination of factual innocence under this law, the court may order the name and associated personal identifying information contained in the court records sealed, deleted, or labeled to show that the data is impersonated and does not reflect the defendant's identity.

DEBT COLLECTORS

The Fair Debt Collection Practices Act prohibits debt collectors from using unfair or deceptive practices to collect overdue bills that a creditor has forwarded for collection, even if those bills don't result from identity theft. To stop a debt collector from contacting you, send a letter to the collection agency within 30 days after you received written notice of the debt, telling them that you do not owe the money. Include copies of documents that support your position. Including a copy (NOT original) of your police report may be useful. If you do not have documentation to support your position, be as specific as possible about why the debt collector is mistaken. Once the debt collector receives your letter, the company may not contact you again, with two exceptions: they can tell you there will be no further contact and they can tell you that the debt collector or the creditor intends to take some specific action.

A collector can renew collection activities only if it sends you proof of the debt. For example, if the debt you are disputing originates from a credit card you never applied for, ask for a copy of the application with the applicant's signature. Then, you can prove that it's not your signature. If you tell the debt collector that you are a victim of identity theft and it is collecting the debt for another company, the debt collector must tell that company that you may be a victim of identity theft.

While you can stop a debt collector from contacting you, that will not get rid of the debt itself. To dispute the debt, it is important to contact the company that originally opened the account; otherwise, that company may send it to a different debt collector, report it on your credit report, or initiate a lawsuit to collect on the debt.

A debt collector or collection agency must cease collection of a debt and conduct a review of the debt upon notice by the consumer that the debt is the result of identity theft. A consumer alleging identity theft must submit to the debt collector or collection agency a copy of the police report regarding the specific debt being collected, as well as a written statement that the debtor claims to be the victim of identity theft with respect to the specific debt being collected by the debt collector. The debt collector or debt collection agency may recommence debt collection activities only upon making a good faith determination that the information does not establish that the debtor is not responsible for the specific debt in question.

INVESTMENT FRAUD

U.S. Securities and Exchange Commission (SEC)—www.sec.gov
The SEC's Office of Investor Education and Assistance serves investors who complain to the SEC about investment fraud or the mishandling of their investments by securities professionals. If you believe that an identity thief has tampered with your securities investments or a brokerage account, immediately report it to your broker or account manager and to the SEC.

You can file a complaint with the SEC's Complaint Center at www.sec.gov/complaint.shtml. Include as much detail as possible. If you don't have Internet access, write to the SEC at: SEC Office

of Investor Education and Assistance, 450 Fifth Street, NW, Washington, DC 20549-0213. For answers to general questions, call 202-942-7040.

MAIL THEFT

U.S. Postal Inspection Service (USPIS)—postalinspectors.uspis.gov
The USPIS is the law enforcement arm of the U.S. Postal Service, and investigates cases of identity theft. The USPIS has primary jurisdiction in all matters infringing on the integrity of the U.S. mail. If an identity thief has stolen your mail to get new credit cards, bank or credit card statements, pre-screened credit offers, or tax information, or has falsified change-of-address forms or obtained your personal information through a fraud conducted by mail, report it to your local postal inspector. You can locate the USPIS district office nearest you by calling your local post office, checking the Blue Pages of your telephone directory, or visiting postalinspectors.uspis.gov.

PASSPORT FRAUD

U.S. Department of State (USDS)—www.travel.state.gov/passport/passport_1738.html
If you've lost your passport, or believe it was stolen or is being used fraudulently, contact the USDS through their website, or call a local USDS field office. Local field offices are listed in the Blue Pages of your telephone directory.

PHONE FRAUD

If an identity thief has established phone service in your name, is making unauthorized calls that seem to come from—and are billed to—your cellular phone, or is using your calling card and PIN, contact your service provider immediately to cancel the account and/or calling card. Open new accounts and choose new PINs. If you're having trouble getting fraudulent phone charges removed from your account or getting an unauthorized account closed, contact the appropriate agency below.

For local service, contact the Illinois Commerce Commission at:
527 East Capitol Avenue
Springfield, IL 62701
(217) 782-7295

For cellular phones and long distance, contact the Federal Communications Commission (FCC) at www.fcc.gov. The FCC regulates interstate and international communications by radio, television, wire, satellite, and cable. Call 1-888-CALL-FCC (TTY: 1-888-TELL-FCC) or write Federal Communications Commission, Consumer Information Bureau, 445 12th Street, SW, Room 5A863, Washington, DC 20554. You can file complaints online at www.fcc.gov, or email your questions to fccinfo@fcc.gov.

SOCIAL SECURITY NUMBER MISUSE

Social Security Administration (SSA)—www.ssa.gov
If you have specific information of SSN misuse that involves the buying or selling of Social Security cards, may be related to terrorist activity, or is designed to obtain Social Security benefits, contact the SSA Office of the Inspector General. You may file a complaint online at www.

socialsecurity.gov/oig, by phone at 1-800-269-0271 (fax: 410-597-0118), or by mail at SSA Fraud Hotline, P.O. Box 17768, Baltimore, MD 21235.

You also may call SSA toll-free at 1-800-772-1213 to verify the accuracy of the earnings reported on your SSN, request a copy of your Social Security Statement, or get a replacement SSN card if yours is lost or stolen. Follow up in writing.

SSA publications:

- Social Security: Your Number and Card (SSA Pub. No. 05-10002)
  www.ssa.gov/pubs/10002.html
- Identity Theft And Your Social Security Number (SSA Pub. No. 05-10064)
  www.ssa.gov/pubs/10064.html

STUDENT LOANS

Contact the school or program that opened the student loan to close the loan. At the same time, report the fraudulent loan to the U.S. Department of Education. Call the Inspector General's Hotline toll-free at 1-800-MIS-USED, visit http://www.ed.gov/about/offices/list/oig/misused/index.html, or write Office of Inspector General, U.S. Department of Education, 400 Maryland Avenue, SW, Washington, DC 20202-1510.

Scholarship Telemarketing Fraud Scheme
The Office of Inspector General at the U.S. Department of Education has become aware of a potential fraud scheme involving persons claiming to represent the U.S. Department of Education who are calling students and offering them scholarships or grants. These callers request a bank or credit card account number saying the information will be used to charge a $249 processing fee. The Department of Education does not charge a processing fee to obtain federal education grants. DO NOT give your financial information to individuals making these claims. If you receive one of these calls, please contact the Office of Inspector General immediately.

If you have provided bank or credit card information to the callers, you should take the following steps:

- Immediately contact your bank, explain the situation, and request that the bank monitor or close the compromised account.
- File a police report.
- Report the fraud to the U.S. Department of Education, Office of Inspector General hotline at 1-800-MIS-USED (1-800-647-8733) or oig.hotline@ed.gov. Special agents in the Office of Inspector General investigate fraud involving federal education dollars.

- Contact the Federal Trade Commission at 1-877-FTC-HELP or http://www.ftc.gov/scholarshipscams.

TAX FRAUD

Internal Revenue Service (IRS)—www.treas.gov/irs/ci
The IRS is responsible for administering and enforcing tax laws. Identity fraud may occur as it relates directly to your tax records. Visit www.irs.gov and type in the IRS key word "Identity Theft" for more information. If you have an unresolved issue related to identity theft, or you have suffered or are about to suffer a significant hardship as a result of the administration of the tax laws, visit the IRS Taxpayer Advocate Service website at www.irs.gov/Advocate or call 1-877-777-4778. If you suspect or know of an individual or company that is not complying with the tax law, report it to the Internal Revenue Service Criminal Investigation Informant Hotline by calling 1-800-829-0433 or visiting www.irs.gov and typing in the IRS key word "Tax Fraud."

Generally, identity thieves use someone's personal data to steal his or her financial accounts and run up charges on the victim's existing credit cards, but you need to be aware of some other potential areas where this type of fraud may occur as they relate directly to your tax records.

- Undocumented workers or some other individuals may use your Social Security number to get a job.

  That person's employer would report W-2 wages earned using your information to the IRS so it might appear that you did not report all of your income on your return.

- An identity thief may file a tax return using your Social Security number to receive a refund.

- If the thief already filed a return using your Social Security number, the IRS will believe that you already filed and received your refund, and the return you just submitted is a second copy or duplicate.

If you do receive a notice from the IRS that leads you to believe someone may have used your Social Security number fraudulently, please notify the IRS immediately by responding to the name and number printed on the notice or letter. Be alert to possible identity theft if the notice or letter states that more than one tax return for you was filed, or the IRS records indicate you received wages from an employer unknown to you.

- If you receive a notice, contact the IRS either by phone or in writing as directed in that notice. IRS tax examiners will work with you and other agencies, such as the Social Security Administration, to help resolve the problem.

- You should also know that the IRS does not request personal taxpayer information through email. If you do receive this type of request, it may be an attempt from identity thieves to get your private tax information.

APPENDIX A

FEDERAL LAW

The Identity Theft and Assumption Deterrence Act, enacted by Congress in October 1998 (and codified, in part, at 18 U.S.C. §1028) makes identity theft a federal crime.

Under federal criminal law, identity theft takes place when someone "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."

Under this definition, a name or Social Security number is considered a "means of identification." So is a credit card number, cellular telephone electronic serial number, or any other piece of information that may be used alone or in conjunction with other information to identify a specific individual.

Violations of the federal crime are investigated by federal law enforcement agencies, including the U.S. Secret Service, the FBI, the U.S. Postal Inspection Service, and the Social Security Administration's Office of the Inspector General. Federal identity theft cases are prosecuted by the U.S. Department of Justice. For the purposes of the law, the FCRA defines identity theft to apply to consumers and businesses.

Drivers Privacy Protection Act

The Drivers Privacy Protection Act (DPPA) requires all states to protect the privacy of personal information contained in an individual's motor vehicle record. This information includes the driver's name, address, phone number, Social Security number, driver identification number, photograph, height, weight, gender, age, certain medical or disability information and, in some states, fingerprints.

The DPPA required states to provide notice and opt-out procedures before a state could make its drivers license and motor vehicle license lists available to direct marketers, among others. The Shelby Amendment turned the act on its head and required that states offer notice and opt-in before making the lists available. If an individual has not given consent to the release of a motor vehicle record, the DPPA limits sharing of the information once it is obtained. Information may be shared with other approved users only for permitted uses.

ILLINOIS STATE LAW

Identity Theft is a Crime in Illinois

A person commits the offense of identity theft when he or she knowingly:

- uses any personal identifying information or personal identification document of another person to fraudulently obtain credit, money, goods, services, or other property; or
- uses any personal identification information or personal identification document of another with intent to commit any felony theft or other felony violation of State law; or
- obtains, records, possesses, sells, transfers, purchases, or manufactures any personal identification information or personal identification document of another with intent to commit or to aid or abet another in committing any felony theft or other felony violation of State law; or
- uses, obtains, records, possesses, sells, transfers, purchases, or manufactures any personal identification information or personal identification document of another knowing that such personal identification information or personal identification documents were stolen or produced without lawful authority; or
- uses, transfers, or possesses document-making implements to produce false identification or false documents with knowledge that they will be used by the person or another to commit any felony theft or other felony violation of State law.

Penalties for identity theft depend on the value of the theft.

Personal Information Protection Act

- Notice to Affected Illinois Residents and Data Security Standards: Any government agency, corporation, university, retail store, or other entity that handles nonpublic personal information is required to:
  - notify each Illinois resident who may be affected by a breach of security; and
  - as of January 1, 2017, also is required to use reasonable security standards to protect the nonpublic personal information from unauthorized access or disclosure.
- Notice to Illinois Attorney General- As of January 1, 2017, the following entities must notify the Office of the Illinois Attorney General if they suffer a breach:
  - entities that are required to comply with federal health privacy law (HIPAA, or Health Insurance Portability and Accountability Act); and
  - Illinois state government agencies.
- Failure to comply with the Personal Information Protection Act is a violation of the Illinois Consumer Fraud and Deceptive Business Practices Act.

Security Freezes

A security freeze prohibits a credit reporting agency from releasing the consumer's credit report or any information from it without the express authorization of the consumer. When a security freeze is in place, information from a consumer's credit report cannot be released to a third party without prior express authorization from the consumer.

To place a security freeze on your account:

- Make a request to a consumer credit reporting agency by toll-free telephone number, secure electronic method, or U.S. mail.

More information about obtaining a security freeze on your account:

- A credit reporting agency cannot charge a fee for placing, removing, or temporarily lifting a security freeze on a credit report.
- The agency has 1 business day after receiving a freeze request by toll-free telephone number or secure electronic method and 3 business days after receiving a written request from the consumer to place a freeze on the account.
- The agency must send a written confirmation of placement of the security freeze to the consumer within 5 business days and must provide the consumer with instructions on how to remove the freeze, including a method of verifying your identity.

Police Departments Must Accept and Provide Reports

- If you learn or reasonably suspect that your personal identifying information has been unlawfully used by another, you can initiate a law enforcement investigation by contacting the local law enforcement agency, which will take a police report of the matter, provide you with a copy of that report, and begin an investigation of the facts or, if the suspected crime was committed in a different jurisdiction, refer the matter to the law enforcement agency where the suspected crime was committed for an investigation of the facts.

Sale and Distribution of Personal Information

- The Secretary of State shall not disclose or otherwise make available to any person or entity any personally identifying information obtained by the Secretary of State in connection with a driver's license, vehicle, or title registration record, with limited exceptions.
- The state policy follows the Federal Drivers Privacy Protection Act, but does not contain an opt-in provision.

Other Protections Passed by the Legislature

- Illinois businesses are prohibited from denying a person credit or utility services, or from increasing a person's credit limits, based solely on their status as an identity theft victim.
- The unauthorized copying and transmitting of any financial transaction devices, such as credit and debit cards, or other devices used to make a payment, get cash, or make a deposit, is a Class A misdemeanor.

APPENDIX B

SAMPLE BLOCKING LETTER— CREDIT REPORTING AGENCY

Date
Your Name
Your Address
Your City, State, Zip Code

Complaint Department
Name of Credit Reporting Agency
Address
City, State, Zip Code

Dear Sir or Madam:

I am a victim of identity theft. I am writing to request that you block the following fraudulent information in my file. This information does not relate to any transaction that I have made. The items also are circled on the attached copy of the report I received. (Identify item(s) to be blocked by name of source, such as creditors or tax court, and identify type of item, such as credit account, judgment, etc.)

Enclosed is a copy of the law enforcement report regarding my identity theft. Please let me know if you need any other information from me to block this information on my credit report.

Sincerely,
Your Name

Enclosures: (List what you are enclosing.)

SAMPLE DISPUTE LETTER—FOR EXISTING ACCOUNTS

Date
Your Name
Your Address
Your City, State, Zip Code
Your Account Number

Name of Creditor
Billing Inquiries
Address
City, State, Zip Code

Dear Sir or Madam:

I am writing to dispute a fraudulent (charge or debit) on my account in the amount of $_____. I am a victim of identity theft, and I did not make this (charge or debit). I am requesting that the (charge be removed or the debit reinstated), that any finance and other charges related to the fraudulent amount be credited, as well, and that I receive an accurate statement.

Enclosed are copies of (use this sentence to describe any enclosed information, such as a police report) supporting my position. Please investigate this matter and correct the fraudulent (charge or debit) as soon as possible.

Sincerely,
Your Name

Enclosures: (List what you are enclosing.)

SAMPLE LETTER TO EQUIFAX —FOR PLACING A SECURITY FREEZE

Date

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

Dear Equifax:

I would like to place a security freeze on my credit file. My name is:

My former name was (if applicable):

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.

Yours truly,

Your Name

SAMPLE LETTER TO TRANSUNION—FOR PLACING A SECURITY FREEZE

Date

TransUnion Security Freeze
P.O. Box 2000
Chester, PA 19016

Dear TransUnion:

I would like to place a security freeze on my credit file. My name is:

My former name was (if applicable):

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.

Yours truly,

Your Name

SAMPLE LETTER TO EXPERIAN—FOR PLACING A SECURITY FREEZE

Date

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

Dear Experian:

I would like to place a security freeze on my credit file. My name is:

My former name was (if applicable):

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.

Yours truly,

Your Name

APPENDIX C

INSTRUCTIONS FOR COMPLETING THE ID THEFT AFFIDAVIT

To make certain that you do not become responsible for any debts incurred by an identity thief, you must prove to each of the companies where accounts were opened or used in your name that you didn't create the debt.

A group of credit grantors, consumer advocates, and attorneys at the Federal Trade Commission (FTC) developed an ID Theft Affidavit to make it easier for fraud victims to report information. While many companies accept this affidavit, others require that you submit more or different forms. Before you send the affidavit, contact each company to find out if they accept it. It will be necessary to provide the information in this affidavit anywhere a new account was opened in your name. The information will enable the companies to investigate the fraud and decide the outcome of your claim. If someone made unauthorized charges to an existing account, call the company for instructions.

This affidavit has two parts:

- **Part One: the ID Theft Affidavit.** This is where you report general information about yourself and the theft.

- **Part Two: the Fraudulent Account Statement.** This is where you describe the fraudulent account(s) opened in your name. Use a separate Fraudulent Account Statement for each company you need to contact. When you send the affidavit to the companies, attach copies (NOT originals) of any supporting documents (for example, driver's license or police report). Before submitting your affidavit, review the disputed account(s) with family members or friends who may have information about the account(s) or access to them.

Complete this affidavit as soon as possible. Many creditors ask that you send it within two weeks. Delays on your part could slow the investigation. Be as accurate and complete as possible. You may choose not to provide some of the information requested. However, incorrect or incomplete information will slow the process of investigating your claim and absolving the debt. Print clearly.

When you have finished completing the affidavit, mail a copy to each creditor, bank, or company that provided the thief with the unauthorized credit, goods, or services you describe. Attach a copy of the Fraudulent Account Statement with information only on accounts opened at the institution to which you are sending the packet, as well as any other supporting documentation you are able to provide.

Send the appropriate documents to each company by certified mail, return receipt requested, so you can prove that it was received. The companies will review your claim and send you a written response telling you the outcome of their investigation. Keep a copy of everything you submit. If you are unable to complete the affidavit, a legal guardian or someone with power of attorney may

complete it for you. Except as noted, the information you provide will be used only by the company to process your affidavit, investigate the events you report, and help stop further fraud.

If this affidavit is requested in a lawsuit, the company might have to provide it to the requesting party. Completing this affidavit does not guarantee that the identity thief will be prosecuted or that the debt will be cleared.

If you haven't already done so, follow the checklist on page 3 of this booklet to protect yourself.

These instructions and the ID Theft Affidavit can be accessed via our website at: www.illinoisattorneygeneral.gov/consumers/ID_Theft_Affidavit_Instructions_and_Form.pdf.

DO NOT SEND AFFIDAVIT TO THE FTC

ID Theft Affidavit

Victim Information

(1) My full legal name is

_____
(First) (Middle) (Last) (Jr., Sr., III)

(2) (If different from above) When the events described in this affidavit took place, I was known as

_____
(First) (Middle) (Last) (Jr., Sr., III)

(3) My date of birth is _____
(day/month/year)

(4) My Social Security number is _____

(5) My driver's license or identification card state and number are _____

(6) My current address is _____

City _____ State _____ Zip Code _____

(7) I have lived at this address since _____
(month/year)

(8) (If different from above) When the events described in this affidavit took place, my address was

_____

City _____ State _____ Zip Code _____

(9) I lived at the address in Item 8 from _____ until _____
(month/year) (month/year)

(10) My daytime telephone number is (_____) _____

My evening telephone number is (_____) _____

How the Fraud Occurred

Check all that apply for items 11 - 17:

(11) ☐ I did not authorize anyone to use my name or personal information to seek the money, credit, loans, goods or services described in this report.

(12) ☐ I did not receive any benefit, money, goods or services as a result of the events described in this report.

(13) ☐ My identification documents (for example, credit cards, birth certificate, driver's license, Social Security card, etc.) were ☐ stolen ☐ lost on or about _____.
(day/month/year)

(14) ☐ To the best of my knowledge and belief, the following person(s) used my information (for example, my name, address, date of birth, existing account numbers, Social Security number, mother's maiden name, etc.) or identification documents to get money, credit, loans, goods or services without my knowledge or authorization:

_____ Name (if known)	_____ Name (if known)
_____ Address (if known)	_____ Address (if known)
_____ Phone number(s) (if known)	_____ Phone number(s) (if known)
_____ Additional information (if known)	_____ Additional information (if known)

(15) ☐ I do NOT know who used my information or identification documents to get money, credit, loans, goods or services without my knowledge or authorization.

(16) ☐ Additional comments: (For example, description of the fraud, which documents or information were used or how the identity thief gained access to your information.)

_____

_____

_____

_____

_____

(Attach additional pages as necessary.)

Victim's Law Enforcement Actions

(17) (check one) I ☐ am ☐ am not willing to assist in the prosecution of the person(s) who committed this fraud.

(18) (check one) I ☐ am ☐ am not authorizing the release of this information to law enforcement for the purpose of assisting them in the investigation and prosecution of the person(s) who committed this fraud.

(19) (check all that apply) I ☐ have ☐ have not reported the events described in this affidavit to the police or other law enforcement agency. The police ☐ did ☐ did not write a report. In the event you have contacted the police or other law enforcement agency, please complete the following:

_____	_____
(Agency #1)	(Officer/Agency personnel taking report)
_____	_____
(Date of report)	(Report number, if any)
_____	_____
(Phone number)	(Email address, if any)
_____	_____
(Agency #2)	(Officer/Agency personnel taking report)
_____	_____
(Date of report)	(Report number, if any)
_____	_____
(Phone number)	(Email address, if any)

Documentation Checklist

Please indicate the supporting documentation you are able to provide to the companies you plan to notify. Attach copies (NOT originals) to the affidavit before sending it to the companies.

(20) ☐ A copy of a valid government-issued photo identification card (for example, your driver's license, state-issued ID card or your passport). If you are under 16 and don't have a photo ID, you may submit a copy of your birth certificate or a copy of your official school records showing your enrollment and place of residence.

(21) ☐ Proof of residency during the time the disputed bill occurred, the loan was made or the other event took place (for example, a rental/lease agreement in your name, a copy of a utility bill or a copy of an insurance bill).

(22) ☐ A copy of the report you filed with the police or sheriff's department. If you are unable to obtain a report or report number from the police, please indicate that in Item 19. Some companies only need the report number, not a copy of the report. You may want to check with each company.

Signature

I certify that, to the best of my knowledge and belief, all the information on and attached to this affidavit is true, correct, and complete and made in good faith. I also understand that this affidavit or the information it contains may be made available to federal, state, and/or local law enforcement agencies for such action within their jurisdiction as they deem appropriate. I understand that knowingly making any false or fraudulent statement or representation to the government may constitute a violation of 18 U.S.C. § 1001 or other federal, state, or local criminal statutes, and may result in imposition of a fine or imprisonment or both.

_____ _____
(Signature) (Date signed)

_____
(Notary)

[Check with each company. Creditors sometimes require notarization. If they do not, please have one witness (non-relative) sign below that you completed and signed this affidavit.]

Witness:

_____ _____
(Signature) (Printed name)

_____ _____
(Date) (Telephone number)

Fraudulent Account Statement

Completing this Statement

- Make as many copies of this page as you need. **Complete a separate page for each company you're notifying and only send it to that company.** Include a copy of your signed affidavit.
- List only the account(s) you're disputing with the company receiving this form. **See the example below.**
- If a collection agency sent you a statement, letter or notice about the fraudulent account, attach a copy of that document (**NOT** the original).

I declare (check all that apply):

☐ As a result of the event(s) described in the ID Theft Affidavit, the following account(s) was/were opened at your company in my name without my knowledge, permission or authorization using my personal information or identifying documents:

Creditor name/address (The company that opened the account or provided goods or services)	Account number	Type of unauthorized credit/goods/services provided by creditor (if known)	Date issued or opened (if known)	Amount/value provided (The amount charged or the cost of the goods/services)
Example Example National Bank 22 Main Street Chicago, IL 60601	01234567-89	auto loan	01/05/20012	$25,500.00

☐ During the time of the accounts described above, I had the following account open with your company:

Billing name _____

Billing address _____

Account number _____

Annual Credit Report Request Form

You have the right to get a free copy of your credit file disclosure, commonly called a credit report, once every 12 months, from each of the nationwide consumer credit reporting companies, Equifax, Experian and TransUnion.

For instant access to your free credit report, visit www.annualcreditreport.com.

For more information on obtaining your free credit report, visit www.annualcreditreport.com or call 877-322-8228.

Use this form if you prefer to write to request your credit report from any, or all, of the nationwide consumer credit reporting companies. The following information is required to process your request. **Omission of any information may delay your request.**

Once complete, fold (do not staple or tape), place into a #10 envelope, affix required postage and mail to:
Annual Credit Report Request Service P.O. Box 105281 Atlanta, GA 30348-5281.

Please use a Black or Blue Pen and write your responses in PRINTED CAPITAL LETTERS without touching the sides of the boxes like the examples listed below:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z 0 1 2 3 4 5 6 7 8 9

Social Security Number: ___ - ___ - ____

Date of Birth: ___ / ___ / ____
Month / Day / Year

Fold Here

First Name | **M.I.**

Last Name | **JR, SR, III, etc.**

Current Mailing Address:

House Number | **Street Name**

Apartment Number / Private Mailbox | **For Puerto Rico Only: Print Urbanization Name**

City | **State** | **ZipCode**

Previous Mailing Address (complete only if at current mailing address for less than two years):

House Number | **Street Name**

Fold Here

Apartment Number / Private Mailbox | **For Puerto Rico Only: Print Urbanization Name**

City | **State** | **ZipCode**

Shade Circle Like This → ●

Not Like This → ⊗ ✓

I want a credit report from (shade each that you would like to receive):

- ◯ **Equifax**
- ◯ **Experian**
- ◯ **TransUnion**

◯ **Shade here if, for security reasons, you want your credit report to include no more than the last four digits of your Social Security Number.**

If additional information is needed to process your request, the consumer credit reporting company will contact you by mail.

Your request will be processed within 15 days of receipt and then mailed to you.

Draft

OFFICE DIRECTORY

Main Offices

Chicago Main Office
100 West Randolph Street
Chicago, IL 60601
(312) 814-3000
TTY: (800) 964-3013

Springfield Main Office
500 South Second Street
Springfield, IL 62701
(217) 782-1090
TTY: (877) 844-5461

Carbondale Main Office
601 South University Avenue
Carbondale, IL 62901
(618) 529-6400/6401
TTY: (877) 675-9339

Regional Offices

Chicago West Reg Ofc
306 North Pulaski Road
Chicago, IL 60624
(773) 265-8808
TTY: (866) 717-8804

East Central Illinois Reg Ofc
1776 East Washington Street
Urbana, IL 61802
(217) 278-3366
TTY: (217) 278-3371

Chicago South Reg Ofc
8100 S. Stony Island, Ste. C
Chicago, IL 60617
(773) 768-5926
TTY: (866) 717-8798

Northern Illinois Reg Ofc
Zeke Giorgi Center
200 South Wyman Street, Ste. 307
Rockford, IL 61101
(815) 967-3883
TTY: (815) 967-3891

West Central Illinois Reg Ofc
628 Maine Street
Quincy, IL 62301
(217) 223-2221
TTY: (217) 223-2254

Metro East Illinois Reg Ofc
201 West Pointe Drive, Ste. 7
Belleville, IL 62226
(618) 236-8616
TTY: (618) 236-8619

Office of the Illinois Attorney General

Identity Theft Hotline

1-866-999-5630

TTY: 1-877-844-5461

www.IllinoisAttorneyGeneral.gov

Copied by the authority of the State of Illinois. 09/18
This material is available in alternate format upon request.