# IDENTITY THEFT

## A Consumer Guide

PROTECT THE GOOD LIFE

**Nebraska Attorney General's Office**

Consumer Affairs Response Team
2115 State Capitol Building
Lincoln, NE 68509

(402) 471-2682

ProtectTheGoodLife.Nebraska.gov

Dear Friends,

Anyone can become a victim of identity theft. Unfortunately, many victims do not even know they are victims until their credit is destroyed. The effects of identity theft can be devastating, and that is why it is important that you understand how to detect identity theft and repair your credit.

To minimize the damage done to your name, you must take immediate action. This guide will provide you with the tools you need to do just that. After you review the following information, please share it with your family and friends so that all Nebraskans are better prepared to prevent identity theft in the future.

Sincerely,

Mike Hilgers

Nebraska Attorney General
Mike Hilgers

# CONTENTS

If someone is using your personal or financial information without your consent to make purchases, get benefits, file taxes, or commit fraud, that's identity theft.

The information in this booklet guides you through the process of deterring, detecting, and defending against identity theft when—not if—it happens to you.



The information contained within this booklet is for educational purposes only and should not be substituted for the advice of an attorney licensed to practice law in Nebraska.

# WHAT IS IDENTITY THEFT?

## WHAT IS IDENTITY THEFT?

Identity theft happens when someone uses your Social Security number or other personal information without your consent to open new accounts, make purchases, or secure other benefits, such as a tax refund. In brief, they pretend to be you.

Once identity thieves have your personal information, they can:

- Drain your bank account;
- Run up charges on your credit cards;
- Open new utility accounts;
- Get medical treatment on your health insurance;
- File a tax refund in your name and get your refund, and;
- In extreme cases, give your name to the police during an arrest.

## PERSONAL INFORMATION (PI)

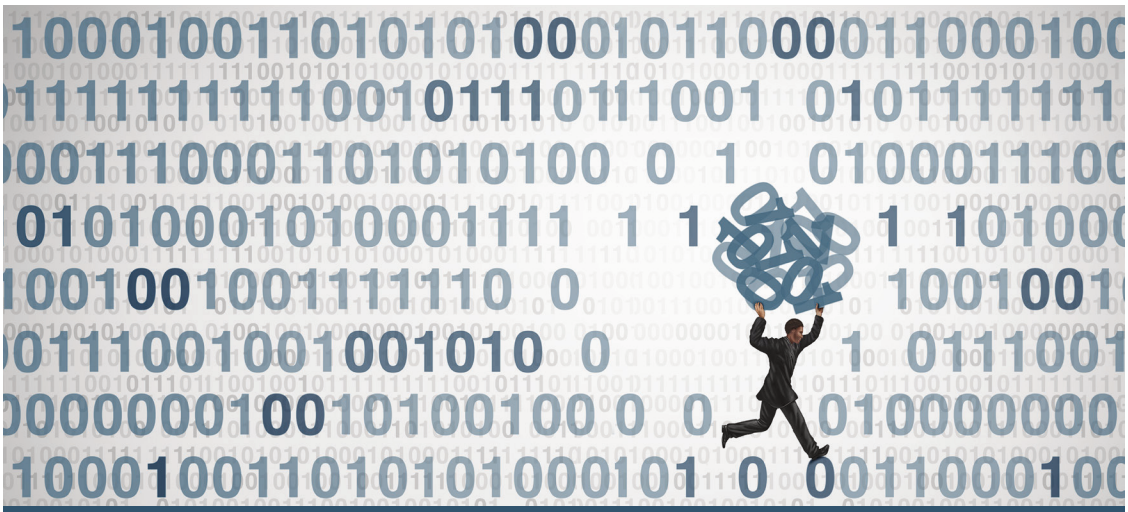
Personal information is any data that can be reasonably linked to a particular person, computer, or device. It includes but is not limited to the following:

- Full name;
- Home address;
- Email address;
- Social Security number;
- Driver's License number;
- Credit or debit card number;
- Bank account number;
- Medical insurance account number;
- Date of birth;
- Passport number;
- Internet Protocol (IP) address, and;
- Location information from a mobile device.

## HOW DO IDENTITY THIEVES GET MY PERSONAL INFORMATION?

Identity thieves are just waiting for you to make a mistake or get careless. Some of the most common ways they can steal your personal information include:

- Stealing your wallet or purse;
- Stealing your mail or garbage (“dumpster diving”);
- Stealing your account numbers from a business or medical office;
- Tricking you into giving personal information over the phone or in an email (“phishing”);
- Using a data storage device to capture the information from your credit or debit card at an ATM or during an actual purchase (“skimming”);
- Obtaining your credit report through false pretenses;
- Improperly obtaining business records by stealing paper files, hacking into electronic files, and/or bribing an employee for access to files;
- Sharing information on unsecure websites or websites compromised by hackers;
- Malicious software ("malware") designed to steal your data or spy on your computer without your knowing, and;
- Data breaches.



## IDENTITY THEFT VS. DATA BREACH

Identity theft and data breaches are often discussed together but are two separate issues.

A data breach occurs when confidential information is copied, viewed, or stolen by someone unauthorized to obtain it. The information can be personal or financial.

A data breach does not mean that your identity has been stolen; however, a data breach can lead to identity theft. See Appendix C: After a Data Breach Checklist on page 28 for a list of steps you should take and who you should contact if your personal information was potentially exposed.

For additional information on data breaches, visit www.IdentityTheft.gov/databreach.

# DETECT IDENTITY THEFT

## SIGNS YOU MAY BE A VICTIM OF IDENTITY THEFT

It is entirely possible for you to be a victim of identity theft and not even know it. Possible warning signs include:

- You see withdrawals from your bank account that you cannot explain;
- You stop receiving bills or other mail unexpectedly;
- Merchants refuse to extend you credit;
- Debt collectors call you about debts you do not recognize;
- You find unfamiliar charges on your credit card;
- You find unfamiliar accounts on your credit report;
- Medical providers bill you for services you did not use;
- Your health insurer rejects your medical claim because you have reached your benefits limit;
- A health insurer refuses to cover you because your medical records show a condition you do not have;
- The IRS notifies you that more than one tax return was filed in your name, or that you have income from an employer you do not work for, and;
- You are notified that your information was compromised by a data breach at a company where you do business or have an account.

## SIGNS YOUR CHILD MAY BE A VICTIM OF IDENTITY THEFT

Your child's identity could be stolen before they ever open a credit account. Unfortunately, criminals target children because of their clean Social Security numbers. Child identity theft is one of the worst forms of identity theft because it often goes unchecked and unnoticed for years.

Several signs can tip you off to the fact that someone is misusing your child's personal information and committing fraud. Take note or action if:

- Your child receives bills or pre-approved credit card offers;
- Your child receives calls from collection agencies;
- Your child is denied government benefits because someone else is using his or her Social Security number;
- The IRS sends your child a delinquent tax notice or informs him or her that their Social Security number was used on another tax return;
- A bank or credit card company denies your child an account, and;
- The DMV denies your child a driver's license.

# DEFEND AGAINST IDENTITY THEFT

## HOW TO DEFEND AGAINST IDENTITY THEFT

While identity theft can happen to anyone, there are things you can do to reduce your risk.

1. **Create and place complex passwords on your bank, credit card, and phone accounts.** A complex password is "long and strong" – consisting of at least ten characters and a combination of both upper and lower case letters, numbers, and symbols. Don't use a password that can be easily guessed, such as your pet's name or your birth date.

2. **Set up two-factor authentication on your accounts.** Two-factor authentication (or "2FA") adds an extra step to an account login. Single-factor authentication is when you enter only your username and one password. 2FA requires you to have two out of three types of credentials before being able to access an account. The three types are: 1) something you know, such as a personal identification number (PIN) or password, 2) something you have, such as an ATM card, phone, fob, or security key, and 3) something you are, using a biometric such as a fingerprint or voice print.

3. **Secure your Social Security number (SSN).** Don't carry your Social Security card in your wallet. Only give out your SSN when necessary.

4. **Guard your mail against theft.** Collect your mail every day. Place a hold on it when you are going to be away from home for several days. Instead of leaving your mail to be picked up in an unlocked mailbox, take it to the post office or a post office collection box.

5. **Pay close attention to billing cycles.** If bills or financial statements fail to arrive, contact the sender.

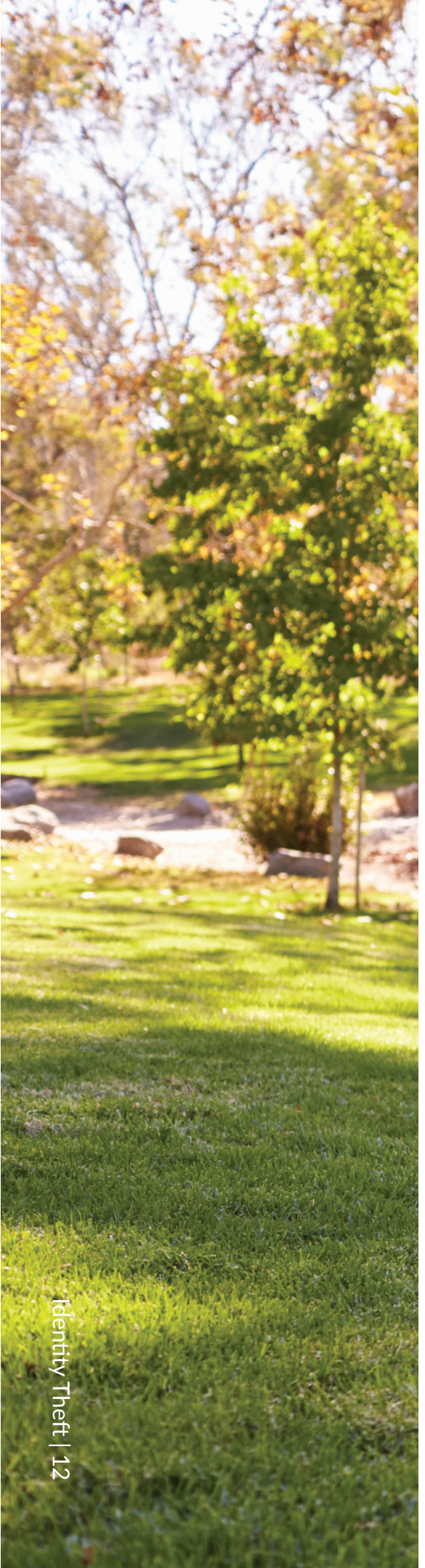
6. **Routinely review your credit card and bank account statements.** Compare receipts with account statements. Watch for unauthorized transactions.

7. **Don't give out personal information over the internet, on the phone or through the mail.** Unless you have initiated the contact or are certain of the identity of the person or company, do not give out personal information (e.g., birthdate, Social Security number, or bank account number) simply because someone asks for it.

8. **Be aware of phishing schemes.** These might include calls or emails from someone claiming to be from your bank needing to confirm your bank account or Social Security number. Be aware of promotional scams that use phony offers as a way to obtain personal information. Assume you are being phished until you verify the source of an unexpected call or email.

9. **Keep your information safe online.** Only send your personal information over a secure connection. A secure connection has an address that begins with "https" and shows a closed padlock at the beginning or end of the address.

   It should look similar to this:



- Update your software regularly. This includes your operating system software, antivirus software, and anything else you use. Cyber threats change frequently, and these updates may address emerging security issues.
- Understand that most public Wi-Fi is not secure. If you use public Wi-Fi, use a virtual private network (VPN) connection that connects your computer or mobile device to the internet, and encrypts your information to protect you from monitoring or spying. If you cannot connect by VPN, it is better to use your smartphone as a hotspot instead.
- Do not download files or click on any links sent to you by people you do not know.

10. **Review your credit reports once a year.** This is one of the best ways to catch identity theft. You are entitled to one free credit report annually from each of the three nationwide credit bureaus, e.g., Equifax, Experian, and TransUnion, and can order them online from www.annualcreditreport.com or call 1-877-322-8228. Reviewing your credit report can help you discover errors and alert you to potential fraud, such as accounts that you have not opened. Should something not look right on any of your credit reports, see Steps to Recover from Identity Theft on page 15.

11. **Freeze your credit reports.** If you are concerned about identity theft, data breaches, or someone gaining access to your credit report without your permission, consider placing a security freeze on your credit reports. Details on placing and managing a security freeze are covered in this guide on page 19.

12. **Shred your documents**. Invest in a quality micro-cut shredder and shred documents containing personal information you no longer need. Shred recipts, credit offers, account statements and expired credit cards.

13. **Use the security features on your mobile phone.** Lock your phone when not in use. Set up Touch ID or Facial Recognition and back that up with a unique PIN or pattern. Always update your phone's Operating System (OS) when prompted.

## LIMITING THE RISK OF CHILD IDENTITY THEFT

Steps you can take to protect your child's identity from misuse include:

- **Securely store sensitive documents.** Find a safe location for all paper and electronic records that show your child's personal information.

- **Limit the sharing of personal information.** Don't share your child's Social Security number unless you know and trust the other party. Ask why it is necessary and how it will be protected. Ask if you can use a different identifier, or use only the last four digits of your child's Social Security number.

- **Keep online devices free of viruses and spyware** that criminals can use to mine your child's data.

- **Properly dispose of documents no longer needed.** Shred (using a micro-cut shredder) all documents that show your child's personal information before throwing them away.

- **Consider a Child Security Freeze.** You can freeze your child's credit until they are old enough to use it. A security freeze, aka credit freeze, restricts access to your child's credit file, making it harder for identity thieves to open new accounts in your child's name. For more information, see Freezing a Child's Credit Report on page 20 of this guide.

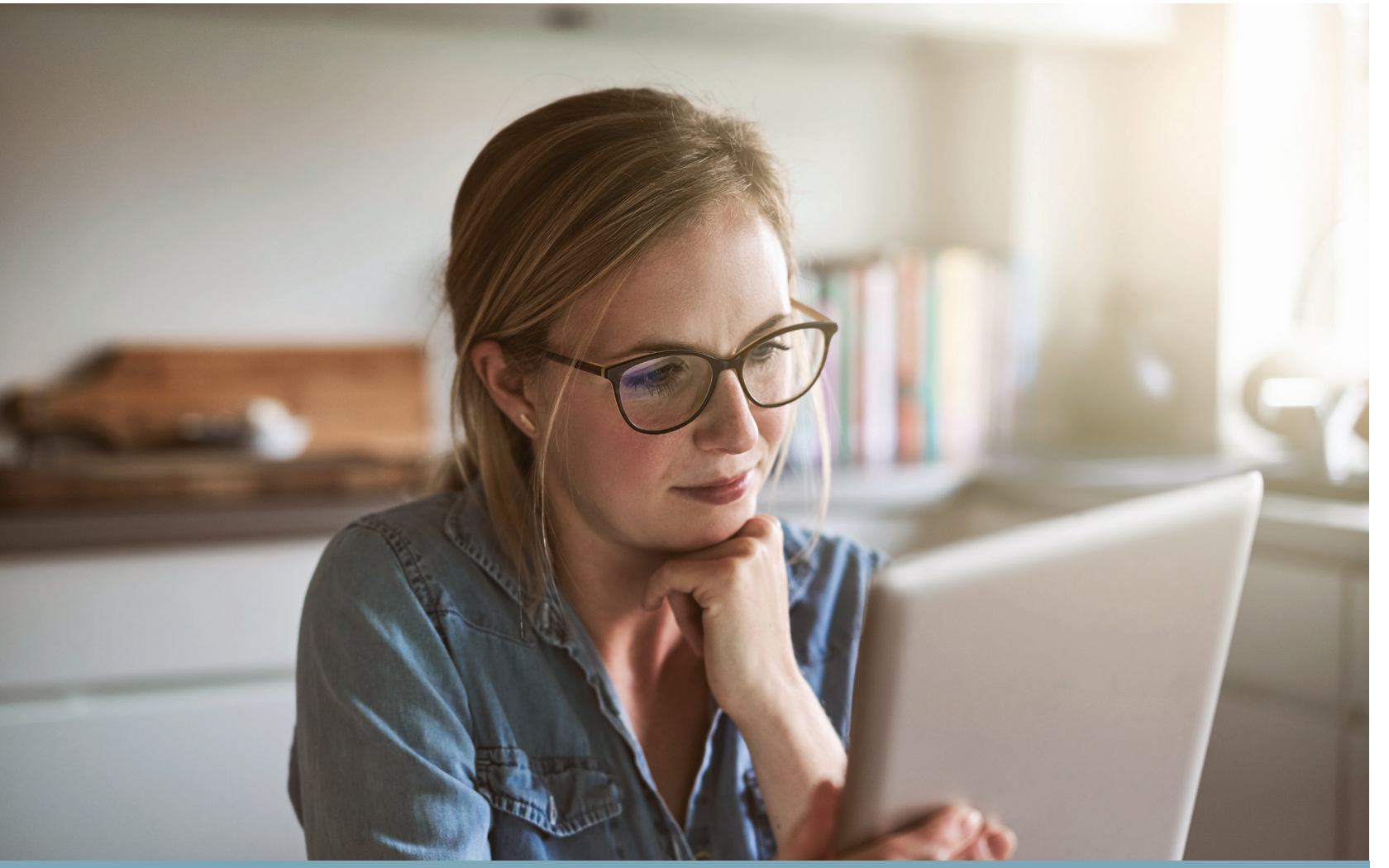
If you are a parent with a child who is enrolled in school:

- **Find out who has access to your child's personal information at school.** Verify that the records are kept in a secure location.

- **Pay attention to forms from your child's school.** Forms that ask for personal information may come home with your child, or you may get them through the mail or email. Look for terms like "personally identifiable information," "personal information," "directory information," and "opt-out." Find out how your child's information will be used, whether it will be shared, and with whom.

- **Read the notices from your child's school.** Your school will send home an annual notice that explains your rights under the federal Family Educational Rights and Privacy Act (FERPA), enforced by the U.S. Department of Education, including your right to: 1) inspect and review your child's education records, 2) approve the disclosure of personal information in your child's records, and 3) ask to correct errors in the records.

# RECOVER FROM IDENTITY THEFT



# STEPS TO RECOVER FROM IDENTITY THEFT

Act quickly! The longer you wait, the more time someone is pretending to be you and, potentially, the greater the damage to your credit.

### What to Do Right Away

**1. Call the companies where you know fraud occurred.**

- Call the fraud department. Explain that someone stole your identity.
- Ask them to close or freeze your accounts.
- Change logins, passwords, and personal identification numbers (PINs) for your accounts.

**2. Place a fraud alert and get your credit reports.**

- To place a free fraud alert, contact one of the three nationwide credit bureaus. That company must tell the other two. A fraud alert lasts one year. It will make it harder for someone to open new accounts in your name. You will receive a letter from each credit bureau confirming that they have placed a fraud alert on your file.
- To get your free credit reports from Equifax, Experian, and TransUnion, go to www.annualcreditreport.com or call 1-877-322-8228.
- Review your reports. Make a note of any account or transaction you do not recognize. This will help you report the theft to the police and/or the Federal Trade Commission.

**3. Report identity theft.**

- Contact your local law enforcement agency to report identity theft if you know the identity thief, have other information that could help a police investigation, or a creditor, debt collector, or someone else affected by the identity theft insists that you produce a police report.
- If none of the previous elements apply, complete an Identity Theft Report with the Federal Trade Commission (FTC) at www.IdentityTheft.gov. In most cases, you can use your Identity Theft Report in place of a police report to clear your account and credit record of fraudulent transactions.

## What to Do Next

4. **Close new accounts opened in your name.** Call the fraud department of each business where an account was opened. Explain that someone stole your identity. Ask the business to close the account and send you a letter confirming that the fraudulent account is not yours, that you are not liable for it, and that it was removed from your credit report. Keep this letter. Use it if the accounts appear on your credit report later on. Write down who you contacted and when.

5. **Remove bogus charges from your accounts.** Call the fraud department of each business. Explain that someone stole your identity. Tell them which charges are fraudulent. Ask them to remove the fraudulent charges and to send you a letter confirming they removed the fraudulent charges. Keep this letter. Use it if these charges result in a derogatory reference on your credit report later on. Write down who you contacted and when.

6. **Correct your credit report.** Write to each of the three nationwide credit bureaus. Include a copy of your police report or Identity Theft Report and proof of your identity, like a copy of your driver's license or state ID. Explain which information on your report is fraudulent and ask them to block that information.

   Mail your letters to each of the three credit bureaus:

**Equifax**
PO Box 740256
Atlanta, GA 30374

**Experian**
PO Box 4500
Allen, TX 75013

**TransUnion**
TransUnion Consumer Solutions
P.O. Box 2000
Chester, PA 19016

## Other Possible Steps

7. **Report a misused Social Security number.** If you suspect someone else is using your Social Security number for work, you can review your earnings history by creating an account at www.ssa.gov/myaccount. If you find errors, contact your local Social Security Administration (SSA) office.

8. **Stop debt collectors from trying to collect debts you do not owe.**
   - Write the debt collector within 30 days of getting a collection letter. Tell the debt collector someone stole your identity, and you do not owe the debt.
   - Send copies of your police report or Identity Theft Report and any other documents that detail the theft.
   - Contact the business where the fraudulent account was opened. Explain that this is not your debt. Tell them to stop reporting this debt to the credit bureaus. Ask for information about the creation of the debt. The business must give you details if you ask.
   - If you have not already, ask the three nationwide credit bureaus to block information about this debt from your credit report.
   - Write down who you contacted and when. Keep copies of any letters you send or receive.

## IDENTITY THEFT AND LIMITS ON FINANCIAL LOSSES

You have limited liability for fraudulent debts caused by identity theft.

- Under most state laws, you are not responsible for any debt incurred on fraudulent new accounts opened in your name without your permission.
- Under federal law, the amount you have to pay for unauthorized use of your credit card is limited to $50. If you report the loss to the credit card company before your credit card is used by a thief, you are not responsible for any unauthorized charges.
- If your ATM or debit card is lost or stolen, you can limit your liability by reporting the loss immediately to your bank or credit union.
- If someone makes unauthorized debits to your bank or credit union account using your debit card number (not your card), you are not responsible—if you report the problem within 60 days after they send you an account statement showing the unauthorized debits.

## IDENTITY THEFT AND LIMITS ON FINANCIAL LOSSES

| If you report your ATM or debit card lost: | Your maximum loss is: |
|---|---|
| Before any unauthorized charges are made. | $0 |
| Within 2 business days after you learn about the loss or theft. | $50 |
| More than 2 business days after you learn about the loss or theft, but less than 60 calendar days after your statement is sent to you. | $500 |
| More than 60 calendar days after your statement is sent to you. | Possibly unlimited |

# SECURITY FREEZE REQUESTS

## SECURITY FREEZE REQUESTS

A security freeze, also known as a credit freeze, restricts access to your credit file, making it harder for identity thieves to open new accounts in your name. Most creditors need to see your credit report before they approve a new account. If they cannot see your report, they may not extend the credit.

You can freeze and unfreeze your credit file for free. You can also get a free freeze for your children who are under age 16. If you are someone's guardian, conservator, or have a valid power of attorney, you can get a free freeze for that person too.

## PLACING A FREEZE ON YOUR CREDIT REPORTS

To place a security freeze on your account, you will need to contact all three nationwide credit bureaus: Equifax, Experian, and TransUnion. You can do so online, by phone, or by mail. Whether online or by phone, the credit bureau must put the freeze in place within one business day. If you request a security freeze by mail, the agency must place the freeze within three business days.

## SECURITY FREEZE CONTACT INFORMATION

| Credit Bureau | Online | By Phone | By Mail |
|---|---|---|---|
| Equifax | www.equifax.com/personal/credit-report-services/ | 888-298-0045 | Equifax Information Services LLC<br>P.O. Box 105788<br>Atlanta, GA 30348 |
| Experian | www.experian.com/freeze/center.html | 888-397-3742 | Experian Security Freeze<br>P.O. Box 9554<br>Allen, TX 75013 |
| TransUnion | www.transunion.com/credit-freeze/ | 888-909-8872 | TransUnion<br>P.O. Box 160<br>Woodlyn, PA 19094 |

## LIFTING OR REMOVING AN EXISTING FREEZE

A freeze remains in place until you ask the credit bureau(s) to temporarily lift it or remove it altogether. If you make the request online or by phone, the credit bureau(s) must lift the freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after receiving your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save time by lifting the freeze only at one particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

## FREEZING A CHILD'S CREDIT REPORT

Parents, guardians, and representatives acting on behalf of a young person (e.g., in foster care) can proactively protect a child's credit file by freezing it.

If the three nationwide credit bureaus don't have a file on the child, they will create one so they can freeze it. This record cannot be used for credit purposes. It is there just to make sure the child's record is frozen and protected against identity theft and fraud.

Depending on the adult's relationship to the child, there are different procedures to put a freeze in place. Parents need to show proof of their authority, like a birth certificate, to freeze or unfreeze the credit file for their child under 16.

A child welfare or probation agency representative acting on behalf of a young person in foster care can request a security freeze for that child. The representative must show documentation certifying that the child is in the agency's care, such as written communication or an official letter from the child welfare or probation agency or its designee.

Additional information on freezing a child's credit with each of the nationwide credit bureaus can be found online at the web addresses noted earlier in the Security Freeze Contact Information matrix included within this section of the guide.

## SECURITY FREEZE FREQUENTLY ASKED QUESTIONS (FAQS)

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

A freeze does not keep you from opening new credit accounts. But to open one, you will need to lift the freeze temporarily. If your request is made online or by phone, a credit bureau must lift a freeze within one hour. It is free to lift the freeze and free to place it again when you are done accessing your credit file.

### Does a security freeze affect my credit card so I can't buy things with it?

No. A security freeze does not affect your existing credit card(s). Your credit report will not be accessible but the freeze will not affect your credit card(s). They are two different things.

### Can a company I already have a relationship with view my credit report if I have a freeze placed?

Yes. Any company you already have an account with will still be able to access your credit report regarding the existing account but they will not be able to use your credit report to open a new account in your name.

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

No. The creditor will be unable to access your credit report or any other information derived from your file, including your credit score.

### Could someone access my credit report even though I placed a freeze on my account?

Certain entities will still have access to it. Your report can be released to your existing creditors or to debt collectors acting on their behalf. Government agencies may also have access to it in response to a court or administrative order, a subpoena, or a search warrant.

### Will a freeze lower my credit score?

No. A security freeze does not affect your credit score.

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

Yes.

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

Yes. Different credit issuers may use different credit companies. To freeze your credit reports with the three nationwide credit bureaus, specifically Equifax, Experian, and TransUnion, you must contact each one individually. Their contact information is included in the matrix found towards the beginning of this section of the guide on page 19.

### Does freezing my file mean that I will no longer receive pre-approved credit offers?

No. If you want to stop receiving prescreened offers of credit, call 888-5-OPTOUT (888-567-8688) or go online at www.optoutprescreen.com. The phone number and website are operated by the three nationwide credit bureaus. You can opt-out for five years or permanently. However, some companies send offers that are not based on prescreening, and your federal opt-out right will not stop those kinds of solicitations.

### How long does my security freeze last?

Your report will be frozen until you request its removal.

### Is there anything else I should know about a security freeze?

If you choose to place a security freeze on your credit file, be sure to plan ahead for all of your credit applications. Depending on your method of contacting any or all of the three nationwide credit bureaus, it may take up to three business days to process your request to temporarily lift a security freeze.

## FRAUD ALERTS VS. SECURITY FREEZES

A fraud alert is another tool at your disposal that can make it harder for an identity thief to open accounts in your name. If someone has misused your personal information—or if you are concerned about identity theft but have not yet become a victim—you can place a fraud alert.

You may want to place a fraud alert if your wallet, Social Security card, or other personal, financial or account information is lost or stolen. You also may want to place a fraud alert if your personal information was exposed in a data breach.

A fraud alert is free. You need only contact one of the nationwide credit bureaus to place one. The credit bureau you contact must tell the other two about your alert.

When you have an alert on your report, a business must verify your identity before it issues credit, so it may try to contact you. Be sure the credit bureaus have your current contact information so they can get in touch with you.

The alert stays on your report for one year. You can get a new one after one year.

If someone steals your identity, you can get an extended fraud alert. It lasts for seven years.

Extended fraud alerts and security freezes can help prevent further misuse of your personal information. There are important differences between the two.

This chart can help you decide which might be right for you.

| Extended Fraud Alert | Security Freeze |
|---|---|
| Permits regular access to your credit report as long as companies take reasonable extra steps to verify your identity before issuing new credit. Best if you want a less restrictive option to a security freeze but may want to know if someone is trying to use your information to open new accounts. | Stops all access to your credit report unless you authorize it by lifting or removing the freeze using a password-protected credit bureau account or a PIN. This may be necessary anytime you want to open a new account that requires a credit check. |
| Available if someone stole your identity. Free to place and remove. | Available at any time for any reason. Free to place and remove. |
| Lasts for seven years. | Lasts until you lift or "thaw" it, temporarily or permanently. |
| Place it by contacting one of the three nationwide credit bureaus.<br>• Report that someone stole your identity.<br>• Request an extended fraud alert on your credit file.<br>• Complete any necessary forms and send a copy of your Identity Theft Report (or police report). | Place it by contacting each of the three nationwide credit bureaus.<br>Ask to put a freeze on your credit report. |

# APPENDICES

## A. SYMPTOMS & SOLUTIONS

| EVENT | ACTION REQUIRED | CONTACT |
|---|---|---|
| **You find any accounts tampered with or opened without your knowledge** | Close the accounts immediately. Get new passwords and PINs for new accounts. | Credit Bureaus, creditors (banks, credit card issuers), merchants, utility and cell phone companies |
| **Your ATM card, credit cards, or checks were stolen** | Close the accounts immediately. Get new PINs and passwords for new accounts. Notify each bank and major check verification company. If your checks are stolen, put "stop-payments" on all checks remaining in the stolen checkbook. | Bank, credit card issuer, creditors, and the police |
| **You find inquiries on your credit report that you did not know about** | By phone and then in writing, notify the three credit bureaus that unauthorized credit inquiries on your credit history were made and request that those inquiries be removed. | Credit Bureaus |
| **You find inaccurate information on your credit report** | By phone and then in writing, notify the three credit bureaus and request the information be corrected. | Credit Bureaus |
| **You have reason to believe your Social Security number (SSN) has been stolen or misused** | Report your allegations to the Social Security Administration (SSA), request a copy of your Social Security Statement, and/or call SSA to verify the accuracy of the earnings reported on your SSN. | Social Security Administration |
| **An identity thief has falsified change-of-address forms, stolen your mail, or committed any other kind of mail fraud in order to get your personal information** | Report it to your local post office. Contact your credit card companies, banks, etc. to notify them that your address was fraudulently changed. Have any changes of address done only in writing. | U.S. Postal Inspection Service (USPIS) |

| EVENT | ACTION REQUIRED | CONTACT |
|---|---|---|
| **You've lost your passport, it was stolen, or you believe it is being misused** | Contact the United States Department of State through a field office or on their website. | United States Department of State (USDS) |
| **You think your name or SSN is being used to obtain a fake driver's license** | Contact the Department of Motor Vehicles (DMV). Make sure you don't use your SSN as your driver's license number. | Department of Motor Vehicles (DMV) |
| **You think an identity thief has interfered with your security investments or a brokerage account** | Report it to your broker or account manager as soon as possible. File a complaint with the U.S. Securities and Exchange Commission. | Your broker/account manager, U.S. Securities and Exchange Commission |
| **A phone service account has been opened in your name, someone is using your calling card, or unauthorized calls are being billed to your cellular phone** | Cancel your account and/or calling card. Use new PINs if you open new accounts. Put a freeze on the credit information used to open phone service accounts. | Your service provider and/or the provider servicing the new account; the National Consumer Telecom & Utilities Exchange (NCTUE) for a freeze. |
| **A debt collector contacts you trying to collect on a loan that you did not take out** | Write a letter to the debt collector. State your reasons why you dispute the debt and include supporting documentation, such as a copy of the police report, or the FTC Identity Theft Report. | Debt collector |
| **You have been wrongfully accused of having committed a crime perpetrated by someone pretending to be you** | File an impersonation report with the police. Include information that will help law enforcement distinguish you from the identity thief. | You may need the assistance of a lawyer, i.e., a criminal defense attorney (public or private) in order to clear your name. Contact the Public Defenders' Office or the State Bar Association in order to find an attorney. |
| **You believe someone has filed for bankruptcy in your name** | Write to the U.S. Trustee and include supporting documentation. File a complaint with the U.S. Attorney and/or the FBI. | U.S. trustee in the region where the bankruptcy occured, U.S. Attorney, FBI in the city the bankruptcy was filed. |

Because this is a lot of information to take in, we have provided you with a checklist to go through to make sure you have taken important steps after becoming an identity theft victim.

## B. After Identity Theft Checklist

### What to Do Right Away

**1. ☐ Call the companies where you know fraud occurred.**

- Call the fraud department. Explain that someone stole your identity.
- Change logins, passwords, and PINs for your accounts.

**2. ☐ Place a fraud alert and get your credit reports.**

To place a fraud alert, contact one of the three credit bureaus. That company must tell the other two.

| Equifax.com/personal/credit-report-services/ 1-888-298-0045 | Experian.com/help/ 1-888-EXPERIAN (888-397-3742) | TransUnion.com/credit-help 1-888-909-8872 |
|---|---|---|

- Get your free credit reports. Go to www.annualcreditreport.com or call 1-877-322-8228.
- Review your reports. Make note of any account or transaction you don't recognize. This will help you report the theft to the FTC and the police.

**3. ☐ Report identity theft.**

- Go to IdentityTheft.gov or call 1-877-438-4338. Include as many details as possible.

### What to Do Next

**4. ☐ Close new accounts opened in your name.**

- Call the fraud department of each business where an account was opened. Explain that someone stole your identity.
- Ask the business to close the account and send you a letter confirming that the fraudulent account is not yours, that you are not liable for it, and that the account was removed from your credit report.

**5. ☐ Consider an extended fraud alert or a security freeze.**

Contact the nationwide credit bureaus to request an extended fraud alert or security freezes.

| Equifax.com/personal/credit-report-services/ | Experian.com/help/ | TransUnion.com/credit-help |
|---|---|---|

# C. After a Data Breach Checklist

## Exposed Social Security Info

☐ **Get your free credit reports.**
Go to www.annualcreditreport.com or call 1-877-322-8228. Check for any accounts or charges you don't recognize.

☐ **Take advantage of free credit monitoring.**
If a company responsible for exposing your information offers you free credit monitoring, take advantage of it.

☐ **Monitor your accounts.**
Look for any charges that you don't recognize or bills that stop coming. This is especially true if the breach involved a bank account or any website where your credit or debit card number was stored.

☐ **Place a fraud alert if you notice suspicious activity.**
To place a fraud alert, contact one of the three credit bureaus. That company must tell the other two.

| | | |
|---|---|---|
| Equifax.com/personal/credit-report-services/ 1-888-298-0045 | Experian.com/fraud/center.html 1-888-397-3742 | TransUnion.com/fraud-alerts 1-888-909-8872 |

☐ **Consider a security freeze.**
You can freeze your credit report by writing to all three credit bureaus (Experian, TransUnion, and Equifax), or by visiting their websites:

| | | |
|---|---|---|
| Equifax.com/personal/credit-report-services/ | Experian.com/freeze/center.html | TransUnion.com/credit-freeze |

☐ **File your taxes early.**
Tax identity theft happens when a scammer uses your Social Security number to get a tax refund or a job.

## Exposed Online Login/Password

☐ **Change your passwords.**
Make your passwords "long and strong." If possible, also change your username. If you can't log in, contact the company. Ask them how you can recover or shut down the account. If you use the same password anywhere else, change that too.

## Exposed Bank Account Numbers or Cards

☐ **Close affected accounts and cards.**
Close accounts, debit cards and credit cards that might have been exposed or opened without your knowledge or consent. Change logins, passwords, and PINs. If you have automatic payments set up, update them with your new bank account information.

## D. Sample Letter to Credit Bureaus

You may submit your Security Freeze request in writing with each of the nationwide credit bureaus at the following addresses.

| | | |
|---|---|---|
| Equifax Security Freeze<br>P.O. Box 105788<br>Atlanta, GA 30348 | Experian Security Freeze<br>P.O. Box 9554<br>Allen, TX 75013 | TransUnion<br>P.O. Box 160<br>Woodlyn, PA 19094 |

Written requests should include the following:

- Your full name including middle initial and any suffixes;
- Social Security number;
- Complete addresses for the past two years;
- Date of birth;
- One COPY of a government issued identification card, such as a driver's license, state ID card, etc., and;
- One COPY of a utility bill, bank or insurance statement, etc.

Make sure that each copy is legible and displays your name and current mailing address and the date of issue. Send copies of any documents you wish to provide and always retain your original documents.

The credit bureaus will send you a confirmation notice once the security freeze has been added. You should also be given a personal identification number (PIN) that will be required in order to lift or remove the freeze temporarily or permanently.

## To be safe, send your letters certified mail return receipt requested.

Date:

Address:

Dear (Insert 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:

I am an identity theft victim and a copy of my official police report/ identity theft report documenting the identity theft is enclosed.

OR

I am a parent of the minor child listed above and have included a copy of their birth certificate and Social Security card or I am a guardian of the minor child and have included copies of the court documentation.

Yours Truly,

# E. Helpful Contacts

### Nebraska Attorney General's Office
ago.nebraska.gov
ProtectTheGoodLife.Nebraska.gov
2115 State Capitol
P.O. Box 98920
Lincoln, NE 68509
For complaints call:
(402) 471-2682 (Lincoln)
(800) 727-6432 (Toll-Free)

### Federal Trade Commission (FTC)
IdentityTheft.gov
FTC
Consumer Response Center
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580
1-877-ID-THEFT (1-877-438-4338)

### Credit Bureaus
EQUIFAX: Equifax.com
PO Box 740256
Atlanta, GA 30374
1-800-525-6285

EXPERIAN: Experian.com
PO Box 4500
Allen, TX 75013
1-888-EXPERIAN (397-3742)

TRANSUNION: TransUnion.com
P.O. Box 2000
Chester, PA 19016
1-800-680-7289

A free copy of your credit report is available from the website www.annualcreditreport.com

Or write to:

Central Source LLC
Annual Credit Report Request Service
P.O. Box 105281
Atlanta, GA 30348-5281
Or call: 1-877-322-8228

### National Consumer Telecom & Utilities Exchange (NCTUE)
NCTUE is a consumer reporting agency that maintains data such as payment and account history reported by telecommunications, pay TV and utility providers.

To determine if NCTUE maintains information about you, request a copy of your NCTUE Disclosure Report:

Call 1-866-349-5185
Or mail your request to
NCTUE Disclosure Report
P.O. Box 105161
Atlanta, GA 30348

To prevent someone from using your personal information to get phone or utility services you may place a security freeze on your NCTUE Disclosure Report.

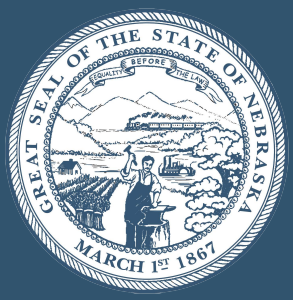
To determine the methods for placing, requesting a temporary lift or removing a security freeze:

Call 1-866-349-5355
NCTUE Security Freeze
Exchange Service Center–NCTUE
P.O. Box 105561
Atlanta, GA 30348

### Social Security Administration
ssa.gov
SSA Fraud Hotline
P.O. Box 17785
Baltimore, MD 21235
SSA Fraud Hotline: 1-800-269-0271

### U.S. Postal Inspection Service
www.uspis.gov

### Visit this Web site to find the Fraud Investigation Unit of the Nebraska DMV Legal Division:
www.dmv.nebraska.gov/legal/index




**Nebraska Attorney General's Office**

Consumer Affairs Response Team
2115 State Capitol Building
Lincoln, NE 68509

(402) 471-2682

ProtectTheGoodLife.Nebraska.gov