Identity Theft

A Consumer Guide

PROTECT THE GOOD LIFE

Nebraska Attorney General's Office

Consumer Affairs Response Team
1445 K Street, Room 2115
PO Box 98920
Lincoln, NE 68508
(402) 471-2682

ProtectTheGoodLife.Nebraska.gov

Dear Fellow Nebraskans,

I commend you for taking the time to educate yourself about identity theft. This type of theft can have serious consequences for a victim, including financial loss, damage to credit, and even legal issues, with impacts lasting for years. Unfortunately, many victims do not even know their identity has been stolen until their credit is destroyed.

Understanding how to detect and report identity theft is important, but you do not have to do it alone. If you need a helping hand, contact our Consumer Affairs Response Team at (402) 471-2682. This dedicated team can walk alongside you to share the steps that you can take to protect your data.

Sincerely,

Mike Hilgers
Nebraska Attorney General

Table of Contents

What Is Identity Theft?

What Is Identity Theft?

Identity theft happens when someone uses your Social Security number or other personal information to open new accounts, make purchases, or secure other benefits, such as a tax refund. In short, they pretend to be you. If someone is using your personal or financial information without your consent – that's identity theft.

Once identity thieves have your information, they can:

- Drain your bank account
- Charge your credit cards
- Open new accounts
- Use your health insurance or benefits
- File a tax refund in your name

Personal Information:

Personal information is any data that can be linked to a particular person, their computer, or device. It includes your:

- 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
- Location information from a mobile device

How Is My Personal Information Stolen?

Identity thieves may steal your:

- Wallet or purse
- Mail or garbage
- Account numbers from a business or medical office
- Paper or electronic files
- Credit report

They may also obtain your information through:

- Tricking you into giving personal information over the phone, in an email, or text
- Using a data storage device, like a skimmer, to capture your credit or debit card information during a purchase
- Hacking unsecured websites
- Malicious software (malware) that steals your data or spies on your computer
- Data breaches

Identity Theft vs. Data Breach

Identity theft and data breaches are often mentioned together but are distinct issues. A data breach happens when someone illegally gains access to confidential information. This can result in identity theft. Check the Data Breach Checklist on page 22 for steps to take if your personal information is compromised. Visit IdentityTheft.gov for more details.

Detect Identity Theft

Identity Theft Warning Signs:

- Withdrawals from your bank account that you cannot explain
- Bills or other mail stop unexpectedly
- You have trouble obtaining credit
- Calls from debt collectors about debts you don’t recognize
- Unfamiliar charges on your credit card
- Unfamiliar accounts on your credit report
- Bills for medical services you did not obtain
- Your health insurance says you reached your benefits limit and rejects your claim
- Denied healthcare coverage due to a medical condition you do not have
- Multiple tax returns filed in your name or income filed from an unfamiliar employer
- Your information was compromised in a data breach

Child Identity Theft Warning Signs:

- Your child receives bills or credit card offers
- Your child receives calls from collection agencies
- Your child is denied government benefits because someone is using their Social Security number
- The IRS sends your child a delinquent tax notice or informs them that their Social Security number was used on another tax return
- The DMV denies your child a driver's license

Your child's identity could be stolen before they ever open a credit account. 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 unnoticed for years.

If you notice these signs, act right away and protect yourself from identity theft!

Defend Against Identity Theft

How to Defend Against Identity Theft:

- Use long and strong passwords for your bank, credit card, and phone accounts. A strong password contains 10-12 characters using upper and lowercase letters, numbers, and symbols. Avoid easily guessed information.
- Enable two-factor authentication (2FA) on your accounts. Also known as multi-factor authentication, 2FA requires two different types of ID to access your account, like a password and a code sent to your phone.
- Store your Social Security number (SSN) in a safe location and only share it when necessary.
- Collect your mail every day to prevent theft. Place a hold on your mail for vacations.
- Pay attention to billing cycles, especially if regular financial statements or bills don't arrive.
- Freeze your credit reports. Details on placing a credit freeze are on page 15.
- Review your credit reports at least once a year.
- Review your credit card and bank account statements regularly for unauthorized transactions.
- Don't give out personal information unless you initiate the contact and know the person or company.
- Be aware of phishing schemes. These might include calls or emails from someone claiming to be from your bank wanting to confirm your bank account or Social Security number. Assume you are being phished until you verify otherwise.
- Keep your information safe online. Avoid using public Wi-Fi when sending personal information. Consider using a Virtual Private Network (VPN).
- Shred your documents and expired credit cards with a micro-cut shredder.
- Use the security features on your phone, like facial recognition or Touch ID, and regularly update your phone's software.

Limiting the Risk of Child Identity Theft

Steps to Protect Your Child:

- Securely store documents. Find a safe location for all paper and electronic records that show your child's personal information.
- Don't share your child's personal information, including their Social Security number, unless you know and trust the other party. Ask why it is necessary, how it will be protected, or if you can use another identifier.
- Keep online devices free of viruses and spyware that criminals can use to steal your child's data.
- Use a micro-cut shredder to shred old documents with your child's personal information.
- Consider a child credit freeze. You can freeze your child's credit until they are old enough to use it, making it harder for thieves to open new accounts. See page 15 for more.
- Find out who has access to your child's personal information at school. Verify that the records are kept in a secure location. Find out how your child's information will be used and who it will be shared with.
- 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.

  This act gives you a right to:
  - Inspect and review your child's education records
  - Approve the disclosure of personal information in your child's records
  - Ask to correct errors

Recover from Identity Theft

What to Do Right Away:

Act quickly! The longer you wait, the more time someone pretending to be you can damage your credit further.

Call the companies where you know fraud occurred. Call the fraud department. Explain that someone stole your identity and ask them to close or freeze your accounts. Change logins, passwords, and PINs.

Get your credit reports and place a fraud alert. To get your free credit reports from Equifax, Experian, and TransUnion, go to AnnualCreditReport.com or call 877-322-8228. To place a free, one-year fraud alert, contact any one of the three nationwide credit bureaus. That bureau will notify the others. This will help protect your credit by requiring an extra identity check. Review your reports for unfamiliar accounts or transactions.

Report identity theft. Contact local police if you know the thief, have helpful details for an investigation, or are asked to provide a police report by a creditor or debt collector. This can support your case and help stop further misuse. Complete an Identity Theft Report with the Federal Trade Commission at IdentityTheft.gov. Use this to clear your credit record of fraudulent transactions.

What to Do Next:

Close unfamiliar accounts opened in your name. Call the company to close the account and let them know your identity was stolen. Ask them to send you a letter confirming that you are not liable for the account and keep a copy.

Remove fraudulent charges from your accounts. Call the fraud department of the account to remove the charges. Ask them to send you a letter confirming the charges are removed and keep a copy.

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 below.

Equifax

PO Box 740256
Atlanta, GA 30374

Experian

PO Box 4500
Allen, TX 75013

TransUnion

PO Box 2000
Chester, PA 19016

Debt Collectors:

Contact the debt collector within 30 days of receiving a collection letter about identity theft-related debt. Let them know the debt isn't yours and your identity was stolen. Include copies of your police report or Identity Theft Report, along with documents that strengthen your claim.

Misused Social Security Number:

View your Social Security account at ssa.gov/myaccount. If you find errors, contact your local Social Security Administration office.

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 pay for unauthorized use of your credit card is limited to $50. If you report your credit card as lost before it's used, you are not responsible for unauthorized charges.

If someone makes unauthorized charges using your debit card number (not your card), you are not responsible if you report the problem within 60 days of receiving an account statement.

If you report your card as lost:	Your maximum loss is:
Before unauthorized charges are made	$0
Within 2 business days after you learn about the theft	$50
2+ business days after you learn about the theft but less than 60 days after your statement	$500
60+ calendar days after your statement	Possibly unlimited

Credit Freeze Requests

Credit Freeze Requests

A credit freeze restricts access to your credit report, making it harder for someone to open new accounts in your name. Creditors may review 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 for free. Place a freeze by contacting all three credit bureaus below.

Credit Bureau	Online	By Phone	By Mail
Equifax	equifax.com/personal/credit-report-services	888-298-0045	PO Box 105788 Atlanta, GA 30348
Experian	experian.com/freeze	888-397-3742	PO Box 9554 Allen, TX 75013
TransUnion	transunion.com/credit-freeze	888-909-8872	PO Box 160 Woodlyn, PA 19094

Lifting or Removing an Existing Freeze

A freeze remains in place until you ask each credit bureau to temporarily or permanently remove it. The fastest way to lift a credit freeze is online or by phone. Requests by mail may take up to 3 business days.

Freezing a Child's Credit

To freeze your child's credit, contact each of the three credit bureaus above. They may create a file for your child in order to freeze the credit. You will need legal documentation like your child's birth certificate to freeze or unfreeze credit for a child under 16. If your child is a foster child, you may need additional documentation. You can also freeze your child's credit if you are their guardian, their conservator, or have power of attorney.

Fraud Alert vs. Credit Freeze

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 free fraud alert. Fraud alerts are a good idea if your wallet, Social Security card, or other personal information is lost or stolen or your data was exposed in a data breach.

Contact one of the nationwide credit bureaus to place an alert. The credit bureau you contact will tell the other two about your alert. Be sure the credit bureaus have your current contact information so they can contact you to verify any new credit.

The alert stays on your report for one year. If someone steals your identity, you can place an extended alert that lasts seven years.

Extended Fraud Alert	Credit Freeze
Allows access to your credit report, but companies may take extra steps to verify your identity to issue new credit. Less restrictive than a credit freeze	Stops all access to your credit report unless you authorize it. This may be necessary anytime you want to obtain additional credit
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 it temporarily or permanently
Contact one of the three credit bureaus, report that your identity was stolen, and request an extended fraud alert	Contact each of the three nationwide credit bureaus and request a credit freeze

Resources

Common Credit Freeze Questions

Can I open new credit accounts if my files are frozen?
Yes, but you will need to lift the freeze temporarily. Credit freezes are free and can be lifted in as little as one hour, but plan ahead when applying for new credit. A credit freeze may take up to three business days to lift.

Does a credit freeze affect my ability to use my credit card?
No. You will be able to regularly use your cards.

Can my current creditors view my credit report if I have a freeze placed?
Yes. These companies will still be able to access your credit report.

Can a new creditor get my credit score if my credit is frozen?
No. The creditor will be unable to access your credit score or report.

Could anyone else access my credit report while it is frozen?
Your report is available to existing creditors or debt collectors acting on their behalf. Government agencies may also have access to it for court orders, subpoenas, or search warrants.

Will a freeze lower my credit score?
A credit 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, you must contact Equifax, Experian, and TransUnion individually.
Their contact information is included on page 15.

How long does my credit freeze last?
Your report will be frozen until you remove it.

Identity Theft Problems and Solutions

Problem	Solution
You find accounts opened without your knowledge	Close the accounts and reset your passwords and PINs for new accounts
Your credit or debit cards were stolen	Notify your bank or credit card company and reset your passwords and PINs
You find unfamiliar inquiries or inaccurate info on your credit report	Notify the credit bureaus and request a correction to your report
Your Social Security number (SSN) has been stolen	Contact the Social Security Administration
Your passport is lost or stolen	Contact the United States Department of State
Your name or SSN was used to obtain a driver's license	Contact the Department of Motor Vehicles
Someone filed bankruptcy in your name	File a complaint with the U.S. Attorney, the FBI, and U.S. Trustee near you
You were accused of a crime committed by someone impersonating you	File a police report
Someone has falsified change-of-address forms or stolen your mail	Report it to your local post office and notify your bank and credit card companies
A debt collector contacts you about debt that is not yours	Contact the debt collector to dispute the debt and include supporting documentation

After Identity Theft Checklist

What to Do Right Away:

- [ ] Call the companies where you know the fraud occurred and let them know your identity was stolen.
- [ ] Change your logins, passwords, and PINs for your accounts.
- [ ] Contact one of the three credit bureaus (Equifax, Experian, or TransUnion) and place a fraud alert. The bureau you contact will inform the other two.
- [ ] Request free credit report copies at AnnualCreditReport.com and review your reports for transactions you don't recognize.
- [ ] Report the identity theft at IdentityTheft.gov or 1-877-438-4338.

What to Do Next:

- [ ] Close new accounts opened in your name. Ask the business for confirmation that the account has been closed.
- [ ] Consider an extended fraud alert or credit freeze. Contact one of the three credit bureaus for more information.

Equifax	equifax.com/personal/credit-report-services	888-298-0045	PO Box 105788 Atlanta, GA 30348
Experian	experian.com/freeze	888-397-3742	PO Box 9554 Allen, TX 75013
TransUnion	transunion.com/credit-freeze	888-909-8872	PO Box 160 Woodlyn, PA 19094

After a Data Breach Checklist

Exposed Social Security Info:

- [ ] Request free credit report copies at AnnualCreditReport.com and review your reports for transactions you don't recognize.
- [ ] Take advantage of free credit monitoring if a company responsible for a data breach offers it.
- [ ] Monitor your accounts for charges you don't recognize or bills that stop coming, especially if the data breach involved a bank account or website that stored your credit or debit card number.
- [ ] Contact one of the three credit bureaus (Equifax, Experian, or TransUnion) and place a fraud alert. The bureau you contact will inform the other two.
- [ ] Consider a credit freeze. You will need to contact all three credit bureaus to do this (Equifax, Experian, and TransUnion).

Exposed Online Login or Password:

- [ ] Change exposed passwords to strong ones with 10-12 characters, using upper and lowercase letters, numbers, and symbols. Avoid easily guessed info, and change your username, if possible. Enable two-factor authentication for added security.

Exposed Bank Account Numbers or Cards:

- [ ] Close affected accounts and cards that may have been exposed or opened without your knowledge. Change logins, passwords, and PINs, and update automatic payments with your new card info.

Helpful Contacts

Nebraska Attorney General's Office
AGO.Nebraska.gov
ProtectTheGoodLife.Nebraska.gov
1445 K Street, Room 2115
PO Box 98920
Lincoln, NE 68508
(402) 471-2682

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

Social Security Administration
SSA.gov
SSA Fraud Hotline
Office of the Inspector General
PO Box 17785
Baltimore, MD 21235
SSA Fraud Hotline: 1-800-269-0271

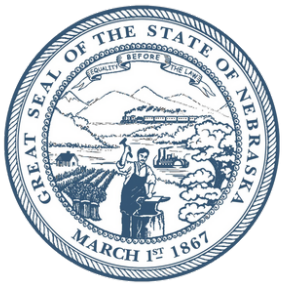
U.S. Postal Inspection Service
USPIS.gov

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

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

TransUnion.com
PO Box 2000
Chester, PA 19016
1-800-680-7289

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



Nebraska Attorney General's Office

Consumer Affairs Response Team
1445 K Street, Room 2115
PO Box 98920
Lincoln, NE 68508
(402) 471-2682

ProtectTheGoodLife.Nebraska.gov