



Morris Building & Loan

IDENTITY THEFT ASSISTANCE KIT

A self-help guide to protecting yourself and your identity

As your hometown community bank since 1917, we've worked hard to ensure our customers safety. For that reason, we have created this Identity Theft Assistance Kit. You can use it as a resource to learn more about identity theft or should you need to, use it to take action in case you suspect identity theft.

Important Contact Information

Credit Bureaus

- Equifax (800) 525-6285 www.equifax.com
- Experian (888) 397-3742 www.experian.com
- TransUnion (800) 680-7289 www.transunion.com

Telecheck (800) 710-9898

Securities & Exchange Commission (800) 732-0330

Federal Trade Commission
ID Theft Hotline (877) 438-4338 www.consumer.gov/idtheft

United States Postal Service www.usps.gov/websites/inspect

Social Security Fraud Hotline (800) 269-0271

Grundy County Sheriff (815) 942-0336

Morris Police Department (815) 942-2131

How Identity Theft Happens

You can be extremely careful about protecting your personal information, but skilled thieves have a variety of methods to get your data and use it for their own benefit.

Here are the most common ways:

- They get information from businesses by: stealing records or information while they're on the job; bribing an employee who has access to these records; hacking these records; or conning information out of employees
- They steal your mail; including bank and credit card statements, credit cards, new checks and tax information
- They may rummage through your trash, the trash of businesses or public trash dumps
- 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 (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 phone by posing as a legitimate company and claim that you have a problem with your account
- They may complete a "change of address" form to divert your mail

How Identity Thieves Use Your Personal Information

As soon as someone has your personal information, there are many ways for them to use it without your knowledge. They can:

- 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's a problem.
- Open new credit card accounts in your name. When they use the credit cards and don't pay the bills, the delinquent accounts are reported on your credit report.
- Establish phone or wireless service in your name.

How Identity Thieves Use Your Personal Information, cont.

- Open a bank account in your name and write bad checks on that account.
- File for bankruptcy under your name to avoid paying debts they've incurred under your name, or to avoid eviction.
- Buy a car by taking out an auto loan in your name.
- Forge checks or debit cards and drain your bank account.
- Get identification such as a driver's license issued with their picture, in your name.

How To Prevent Identity Theft

Morris Building & Loan works hard to protect your personal information. One of the best ways to fight identity theft is to make it more difficult to gather your information. Here are some tips:

- Carry only what you need – the less personal information you have with you, the better off you will be if your wallet or purse is stolen. Never carry your Social Security Card—leave it in a secure place and memorize the number.
- Don't put outgoing mail in or on your mailbox – thieves may use your mail to steal your identity. Drop your mail into a secure, official Postal Service collection box.
- Report lost or stolen credit cards immediately – call each credit card issuer and ask to have the stolen card accounts closed and new ones opened to replace them. Remember to update any automatic payment accounts with your new account numbers.
- Cancel any credit card accounts that you no longer use – cut up these cards and throw them out. Don't keep old credit or ATM cards around.
- Don't preprint personal information on checks – your checks should not have your driver's license, telephone or Social Security numbers printed on them.
- Report lost or stolen checks immediately – if you have Morris Building & Loan banking accounts, we will block payment on the check numbers involved. Also, review new checks to make sure none have been stolen in transit. And review your account for counterfeit checks. Make sure the checks that clear were written by you. By using Morris Building & Loan's Online Banking, this can be done electronically on a daily or weekly basis.
- Store cancelled checks safely – file your imaged statements in our Free Storage Binders and keep it in a safe place. This goes for your new checks as well.

How To Prevent Identity Theft, cont.

- Be vigilant on who you share information with – don't give out personal information on the phone, through mail or the Internet unless you've initiated the contact or are sure you know who you are dealing with. Before you share any personal information, confirm that you are dealing with a legitimate organization. Tell the caller you will call them back and then verify the number with published resources.
- Be careful with your ATM and credit card receipts – thieves can use them to access your accounts. Never throw away receipts in a public trash can.
- Guard your Personal Identification Numbers (PINs) – don't write your PINs on your ATM or credit cards and don't keep your PINs with your cards. Memorize them.
- Discard mail appropriately – thieves may pick through your trash or recycling bins to capture your personal information so be certain to tear or shred your charge receipts, copies of credit applications, insurance forms, physician statements, checks and bank statements, expired charge cards that you're discarding, and credit offers you get in the mail. Consider purchasing a home shredder or participate in Community Shred Day, sponsored by Morris Building & Loan.
- Keep track of bills – if regular bills fail to reach you, call the company to find out why. Someone may have filed a false "change of address" notice to divert your information. If your bills include suspicious items, don't ignore them. Instead, investigate immediately to stop any possible or further fraud. Look into receiving your bills electronically. Studies have shown that you are 40% less likely to be a victim of identity theft when switching to paperless billing.
- Review your credit report annually – You may now check your credit report from each of the three major credit reporting agencies for free each year. Go to www.annualcreditreport.com or call 877-322-8228.
- Protect your identity online – when conducting financial transactions, making purchases or sending personal information online, make sure the Websites you visit are secure and protect your data. Look for Websites that use Secure Socket Layer (SSL) technology to encrypt your personal information. You can also check to see if your Web session is secure by looking for a small lock symbol located in the lower corner of your Web browser window. You may also look for the letters "https://" at the beginning of the Website URL in your Web browser. The "s" means that the Web connection is secure.
- Sign up for the ID TheftBlocker, provided by Deluxe and Morris Building & Loan. Complete details are on our website at www.morrisbl.com. This service has a low monthly fee which covers consumer credit monitoring, theft detection services, and recovery assistance.

If You Are a Victim

If you are a victim of identity theft, take the following steps as soon as possible, and keep a record with the details of your conversations and copies of all correspondence.

1. Place a fraud alert on your credit reports and review your credit reports.

Placing a fraud alert can help prevent an identity thief from opening any more accounts in your name. Contact one of the toll-free fraud numbers of any of the three consumer reporting companies to place a fraud alert on your credit report. The company you call is required to contact the other two, which will place an alert on their versions of your report, too.

Equifax: Call: (800) 525-6285
 Write: Equifax Fraud Assistance
 PO Box 740241
 Atlanta, GA 30374-0241
 www.equifax.com

Experian: Call: (888) 397-3742
 Write: PO Box 9532
 Allen, TX 75013
 www.experian.com

TransUnion: Call (800) 680-7289
 Write: Fraud Victim Assistance Division
 PO Box 6790
 Fullerton, CA 92834-6790
 www.transunion.com

Once you place the fraud alert in your file, you're 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.

As soon as you receive your credit reports, review them carefully. Look for inquires from companies you haven't contacted, accounts you did not open, and debts on your accounts that you can't explain. Check that information like your SSN, addresses, name or initials, and employers are correct.

Include a victim's statement on your credit report. Tell the credit bureaus you'd like to include a statement on your report asking that creditors call you before opening any new accounts or changing your existing accounts.

2. Contact your local police.

File a report with your local police or the police in the community where the identity theft took place. Even if the police are unable to catch the thief, having a copy of the police report can help you in dealing with creditors. Obtain a copy of the police report in case your bank, credit card company or others need proof of the crime.

3. Contact the Federal Trade Commission.

Call the FTC's Identity Theft Hotline at (877) 438-4338. The FTC will put your information into a secure consumer fraud database and may, in appropriate instances, share it with other law enforcement agencies.

4. Close the accounts that you know, or believe, have been tampered with or opened fraudulently.

Call and speak with someone in the security or fraud department of each company. Follow up in writing, and include copies (not originals) of supporting documents. It's 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 PINs and passwords. 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.

If the identity thief has made charges or debits on your accounts, or on fraudulently opened accounts, ask the company for the forms to dispute those transactions.

If the company already has reported these accounts or debts on your credit report, dispute this fraudulent information.

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.

5. Check your mail carefully.

If you receive statements for accounts you do not have, contact the creditor. An identity theft may have opened an account in your name.

If you do not receive statements for any of your usual accounts (including credit, banking and investment), contact the company immediately. An identity thief may have submitted a change of address in order to redirect your statements to a different location.

If you do not receive mail you usually receive, contact the post office. An identity thief may have falsified a change of address to redirect your mail to a different location.

6. Review ALL of your accounts.

You should check transactions on credit account statements including credit cards, home equity lines of credit, bank accounts, investment accounts and telephone bills. If you find problems on one of your accounts, you should pay careful attention to all of your accounts going forward.

Sample Blocking Letter – Credit Bureau

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

Complaint Department
Name of Credit Bureau
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 circle on the attached copy of the report I received. (identify items to be blocked by name of source, such as creditors or tax court, and identify type of item, such as credit amount, 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 – Existing Accounts

Date

Your Name

Your Address

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 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 (use this 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)

Charting Your Course of Action

Use this form to record the steps you've taken to report the fraudulent use of your identity. Keep this list in a safe place for reference.

Credit Bureaus

Credit Bureau	Phone Number	Date Contacted	Contact Person	Comments
Equifax	(800) 525-6285			
Experian	(888) 397-3742			
TransUnion	(800) 680-7289			

Banks, Credit Card Issuers and other Creditors

(contact each creditor promptly to protect your legal rights)

Creditor	Address/Phone Number	Date Contacted	Contact Person	Comments
Morris Building & Loan	211 E. Jefferson St., Morris, IL 60450 815-942-3232			

Law Enforcement Authorities

Report identity theft

Agency	Phone Number	Date Contacted	Contact Person	Comments
FTC	877-438-4338			
Morris Police Dept.	815-94-2131			
Grundy Co. Sheriff	815-942-0336			