Identity Theft Assistance Kit

A self-help guide to protecting yourself and your identity

Stillman Bank works hard to serve and protect our customers' identities and ensure their safety. That's why we have a privacy policy and strict code of conduct that our employees must abide by.

That's also why we've prepared this Identity Theft Assistance Kit. Use it as a resource to learn more about identity theft and the choices you can make to better protect yourself. Use it also as a guide to help you take any action you need in case you suspect identity theft.

Important Contact Information

Credit Bureaus

- Equifax 1-800-525-6285
- Experian 1-888-397-3742
- TransUnion 1-800-680-7289

TeleCheck 1-800-710-9898

Securities and Exchange Commission 1-800-732-0330

Federal Trade Commission Identity Theft Hotline 1-877-438-4338

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

Social Security Fraud Hotline 1-800-269-0271

For more information on identity theft, visit the Federal Trade Commission consumer website at **www.consumer.gov/idtheft**, or call toll-free **1-877-438-4338**.

CONTENTS

Identity Theft 101	**3**
How to Protect Yourself	**5**
If You Become a Victim	**9**
Sample Letters	**13**
Identity Theft Worksheet	**15**

How Identity Theft Happens

No matter how careful you are about protecting your personal information, no one is completely safe from identity theft. Skilled thieves, like pickpockets, burglars and computer hackers have many ways (both low- and high-tech) to get hold of your important data and use it for their own benefit.

Here are some of the most common ways identity thieves can gain access to your information. They:

- Steal wallets and purses containing your identification, credit and bank cards.
- Steal your mail, such as bank and credit card statements, pre-approved credit offers, telephone bills and tax information.
- Complete a “change of address form” to divert your mail.
- Rummage through your trash, or the trash of businesses, for personal data in a practice known as “dumpster diving.”
- Fraudulently obtain your credit report by posing as a landlord, employer, or someone else who may have a legitimate need for and a legal right to the information.
- Get your business or personal records at work.
- Find personal information in your home.
- Use personal information you share on the Internet.
- Obtain information through email phishing attempts from you

How Identity Thieves Use Your Personal Information

Once someone has your personal information, there are many ways they can use it without your knowledge. They can:

- Call your credit card issuer pretending to be you and ask to change the mailing address on your credit card account. The imposter then runs up charges on your account. And because your bills are being sent to the new address, it may take some time before you realize there's a problem.

- Open a new credit card account, using your name, date of birth and Social Security number. When they use the credit card and don't pay the bills, the delinquent account is reported on your credit report.

- Establish phone or wireless service in your name.

- 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 in your name, or to avoid eviction.

- Forge counterfeit checks or debit cards and drain your bank account.

- Buy cars by taking out auto loans in your name.

How To Prevent Identity Theft

At Stillman Bank, we work hard to protect your personal information. We believe that one of the best ways to fight identity theft is to prevent it from happening in the first place. Here are some of the options available to you to help prevent someone from stealing your important information.

Carry only what you need.

The less personal information you have with you, the better off you will be if your purse or wallet has been stolen.

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.

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.

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.

Don’t preprint personal information on checks.

Your checks should not have your driver’s license, telephone or Social Security numbers on them.

Report lost or stolen checks immediately.

If you have Stillman Bank 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 Stillman Online this can be done electronically on a weekly basis. You can also sign up for E-statements and receive all bank statements electronically.

Store canceled checks safely.

File your image statements in a secure place. This goes for your new checks as well.

Be alert to telephone scams.

If you are called, be wary about providing personal information. Notify the appropriate financial institutions of any suspicious phone inquiries made in their name asking for account information to “verify a statement” or “award a prize.” Tell the caller you will call them back, and then verify the number with published sources.

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. Also be comfortable with the ATM surroundings, if possible use an ATM at a Stillman Bank location to gain assurance that security precautions are in place. Never use an ATM where you feel uncomfortable.

Guard your Personal Identification Numbers (PINs).

Don’t write your PINs on your ATM, debit or credit cards and don’t keep your PINs with your cards. Memorize them.

Discard mail appropriately.

If you receive financial solicitations that you're not interested in, tear them up before throwing them away, so thieves can't use them to assume your identity. Destroy any other financial documents, such as bank statements or invoices, before disposing of them. Consider a home paper shredder for all sensitive documents.

Keep your information private.

Don't give out financial information such as checking account and credit card numbers and especially your Social Security number on the phone unless you initiate the call and know the person or organization you're dealing with. Don't give out personal information to anyone, even someone claiming to be from Stillman Bank.

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 to his or her address. If your bills include suspicious items, don't ignore them. Instead, investigate immediately to head off any possible or further fraud. Look into receiving your bills electronically through Stillman Web Pay. Studies have shown that you are 40% less likely to be a victim of identity theft when switching to paperless billing and e-delivery methods.

Review your credit report.

Periodically contact the major credit reporting companies to review your file and make certain the information is correct. See if they have online inquiry such as the Stillman credit card to review your balances on a regular basis for any unusual purchases. You can obtain an annual copy of your credit report at www.annualcreditreport.com. Review it and report anything suspicious or inaccurate, this not only protects you but also keeps your credit in shape.

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

from Internet theft. 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 usually located in the lower corner of your web browser window. Current versions of leading web browsers indicate when a webpage is encrypted for transmission by using this symbol. 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. For example, Stillman Online uses 256-bit encryption, the highest level of protection available as well as a multifactor process when you log on. You will be given a recognizable picture and even challenge questions if anything abnormal occurs. Another online safety feature is your password. Every time you log on, you are required to enter your ID and password. For your safety, you should not reveal your password to anyone. Our website is protected by Verisign so you know it is the authentic website. Always maintain up-to-date virus and firewall protection on your computer. Perform routine scans and be diligent if anything is detected.

Stillman Bank uses multiple layers of security to protect you. That’s why we require separate user name and password combinations to access Stillman Online, Stillman Web Pay and accessing your credit card information via www.stillmanbank.com.

Never respond to an email that asks you to verify account information, name or Social Security number. Stillman Bank will never ask for this information unless you initiate the call. Such emails are referred to as “phishing” and can result in the sender stealing your identity or initiating bogus transactions to your accounts.

How To Deal With Identity Theft

You can recover from identity theft. In fact, if you suspect that you may be a victim, you've already taken an important first step by downloading this document.

Here are some important steps you can take to help reclaim your identity:

1. Call the credit bureaus.

Contact the fraud departments of each of the three major credit bureaus. They maintain reports that track the credit accounts that have been opened in your name and how you pay your bills. You should call first and then follow up in writing.

See the sample credit bureau letter in the Sample Letter section.

Equifax	Call 1-800-525-6285 Write: Equifax Fraud Assistance P.O. Box 105069 Atlanta, GA 30348 www.equifax.com
Experian	Call 1-888-397-3742 Write: P.O. Box 949 Allen, TX 75013-0949 www.experian.com
TransUnion	Call 1-800-680-7289 Write: P.O. Box 6790 Fullerton, CA 92834 www.tuc.com

2. Request that a fraud alert be placed in your credit bureau file.

This will alert potential creditors that you may have been the victim of identity theft and that your credit history may not yet be completely corrected.

3. Include a victim's statement.

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

4. Ask for copies of your credit reports.

If you are a victim of identity theft, credit bureaus must give you a free copy of your report to check for inaccuracies.

5. Review your credit reports carefully.

Make sure that no additional fraudulent accounts have been opened or unauthorized changes made. Check the inquiry section of the report. When inquiries appear from companies that opened fraudulent accounts, request that the inquiries be removed from your report.

6. Perform periodic reviews.

In a few months, order a new copy of your credit report to verify your corrections and changes. After reviewing your credit report, you may find that accounts were opened in your name at other banks or lenders. Call the companies where the accounts were opened to report fraudulent accounts, and then follow up in writing. Include copies of documents that support your position. See the sample credit bureau letter in the Sample Letter section.

7. 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.

8. Contact the Federal Trade Commission.

Call the Federal Trade Commission's (FTC) Identity Theft Hotline at 1-877-ID THEFT (1-877-438-4338). The FTC will put your information into a secure consumer fraud database and may, in appropriate instances, share it with other law enforcement agencies.

9. Check your mail carefully.

If you receive statements for accounts you do not have, contact the creditor. An identity thief 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.

10. Review ALL 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.

11. Contact other creditors.

Creditors can include credit card, phone and other utility companies, and banks and other lenders. Ask to speak with someone in the company's security or fraud department and follow up with a letter. Credit card companies require that you contact them in writing. A sample dispute letter can be found in the Sample Letter section.

Close accounts that have been tampered with and open new ones with new PINs and passwords. Avoid using easily available information for a password like a date of birth or Social Security number.

12. Review your bank accounts.

If an identity thief has tampered with your savings or checking account or ATM card, close the account immediately. Open a new account and ask that a password be required to obtain any information. And avoid using easily available information for a password. If your checks were stolen or misused, either place a stop payment on the range of missing checks or close the account.

Also, contact the major check verification companies to request that they notify retailers that use their database.

TeleCheck: 1-800-710-9898
Certegy: 1-800-437-5120

13. Review your investment accounts.

If an identity thief has tampered with your securities, investments or brokerage account, immediately report it to your broker or account manager and to the Securities and Exchange Commission at 1-800-SEC-0330 (1-800-732-0330).

14. Contact your telephone service provider.

If an identity thief has established a new phone or cellular service in your name, contact your service provider immediately to cancel the account. If you have trouble getting fraudulent phone charges removed from your account, contact your state Public Utilities Commission for local service providers or the Federal Communications Commission for long distance service providers.

15. Contact your local Postal Inspector.

If an identity thief has stolen your mail to obtain credit or falsified change of address forms, that's a crime. Report it to your local Postal Inspector. You can learn how to contact your local Postal Inspection Service office by contacting your local post office or by visiting the United States Postal Service online at www.usps.gov/websites/depart/inspect.

16. Contact the Social Security Department.

If you believe someone is using your Social Security number to apply for a job or to work, contact the Social Security Fraud Hotline at 1-800-269-0271. You can also contact the Social Security Department at 1-800-772-1213 to verify the accuracy of the earnings reported on your Social Security number and to request a copy of your Social Security statement.

17. Contact your local Department of Motor Vehicles.

If you suspect your name is being used by an identity thief to get a driver's license or ID card, contact your local Department of Motor Vehicles.

Sample dispute letter – Credit Bureau

Date Your Name Your Address Your City, State, Zip

Complaint Department Name of Credit Bureau Address City, State, Zip

Dear Sir or Madam:

I am writing to dispute the following information in my file. The items I dispute are circled on the attached copy of the report I received. (Identify item(s) disputed by name of source, such as creditors or tax court, and identify type of item, such as credit account, judgment, etc.)

This item is (inaccurate or incomplete) because (describe what is inaccurate or incomplete and why). I am requesting that the item be deleted (or request another specific change) to correct the information.

Enclosed are copies of (use this sentence if applicable and describe any enclosed documentation, such as payment records or court documents) supporting my position. Please investigate this (these) matter(s) and (delete or correct) the disputed item(s) as soon as possible.

Sincerely,

Your Name

Enclosures: (List what you are enclosing)

Sample dispute letter –Credit Card Issuers

Date Your Name Your Address Your City, State, Zip Your account number

Name of Creditor Billing Inquiries Address City, State, Zip

Dear Sir or Madam:

I am writing to dispute a billing error in the amount of $_____ on my account. The amount is inaccurate because (describe the problem). I am requesting that the error be corrected, that any finance or other charges related to the disputed 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 sales slips or payment records) supporting my position. Please investigate this matter and correct the billing error as soon as possible.

Sincerely,

Your Name

Enclosures: (List what you are enclosing)

Action Taken Worksheet

Credit Bureaus – Report Fraud

Bureau Phone Date Contacted Contact Comments

Equifax 1-800-525-6285

Experian 1-888-397-3742

TransUnion 1-800-680-7289

Banks, Investment Companies, Credit Card Issuers and Other Creditors (Contact each creditor promptly to protect your legal rights)

Bank Address & Phone Date Contact Comments

Stillman Bank 815-645-2266
Or your local office

Law Enforcement Authorities – Report Identity Theft

Agency	Phone	Date	Contact	Case #	Comments
Federal Trade Commission	1-877-438-4338				
Ogle County Sheriff	815-732-6666				
Rockford Police	815-987-5800				
Winnebago County Sheriff	815- 987-5800				
Local Police					