

Identity Theft Assistance Kit



Hearthside Bank

How to protect yourself from Identity Theft.

What to do if you suspect you may be a victim.

Contents

Introduction	3
What is Identity Theft?	4
What Do Identity Thieves Do With This Information?	4
How Do I Know If Someone Has Stolen My Identity?	4
What Can I Do To Protect My Identity?	4
Online Security Tips	5
Email Security Tips.....	6
Mobile Device Security Tips	6
Bank Account Security Tips.....	6
Scam Prevention Tips	7
Hearthside Bank Privacy Policy	8
Hearthside Bank Privacy Statement for Consumers.....	8
If You are Victim of Identity Theft	8
Step by Step Tasks	9
Communication Log.....	11
Sample Letters	12

Introduction

Hearthside Bank values the relationships we have built with you and your family and hope that you never become the victim of identity theft. But, because identity theft is such a fast-growing crime, we want you to be aware of the basic precautions you can take to protect yourself. We have created the Identity Theft Assistance Kit to help you understand Identity Theft but also to minimize the risk.

This brochure offers safety measures and tips for the following:

- Online Security Tips
- Email Security Tips
- Mobile Device Security Tips
- Bank Account Security Tips
- Scam Prevention Tips

In addition to providing you with information on how to protect your identity, we have also included important step by step instructions on how to tackle identity theft if you have become a victim.

Quick Reference	Contact Information
Hearthside Bank	606-248-1095
Credit Bureaus	
	Equifax 1-800-525-6285
	Experian 1-888-EXPERIAN (397-3742)
	TransUnion 1-800-680-7289
Federal Trade Commission Identity Theft Information	www.ftc.gov/idtheft
United States Postal Service online	1-877-438-4338 Postalinspectors.uspis.gov
US Secret Service – Find the field office near you	http://www.secretservice.gov

What is Identity Theft?

Identity theft occurs when a criminal takes your personal information – such as your name, address and Social Security Number – and uses it to establish credit and charge items to you. Thieves can steal the information necessary to commit identity theft in a number of ways:

- ✓ From discarded bills or statements
- ✓ From a lost wallet
- ✓ From stolen mail
- ✓ By obtaining a copy of your credit report
- ✓ From fraudulent Internet, telephone or text messaging scams
- ✓ From information you might disclose on the Internet

What Do Identity Thieves Do With This Information?

Once identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance. An identity thief might even file a tax return in your name and get your refund. In some extreme cases, a thief might even give your name to the police during an arrest.

How Do I Know If Someone Has Stolen My Identity?

If you noticed any of the following items, you may be victim of identity theft.

1. You may notice unexplained withdrawals from your bank account
2. You don't get your bills or other mail
3. Merchants refuse your checks
4. Debit collectors call you about debts that aren't yours
5. Medical providers bill you for services you didn't use
6. Your health plan rejects your legitimate medical claim because the records show you've reach your benefits limit
7. The Internal Revenue Service (IRS) notifies you that more than 1 tax return was filed in your name, or that you have income from an employer you don't work for
8. You get notice that your information was compromised by a data breach at a company where you do business or have an account
9. You are arrested for a crime someone else allegedly committed in your name

What Can I Do To Protect My Identity?

There are many ways that identity thieves can get your personal information. There are simple steps you can take to protect yourself and your identity. Below are some tips and basic reminders of what you should or shouldn't do to help keep your personal information secure.

Online Security Tips

Antivirus software and firewalls are not always enough to protect you from thieves. Hearthside Bank offers our customers FREE security software called Rapport. Rapport will provide additional software security to shield your online banking details from prying eyes, safeguard your identity, protect your internet banking login details, and help stop malicious attempts against you.

Below are additional tips to stay safe online:

- ✓ Use hard to guess usernames and passwords. Use combinations of letters, numbers, and special characters such as # and @. Do not use the same username and passwords as credentials for all websites.
- ✓ Protect your online passwords. Don't write them down or share them with anyone.
- ✓ Select questions and provide answers that you can easily remember and are hard to guess. Don't use security questions with easily found answers such as the name of your high school. Do not use the same security questions for all your website access. Please note that Hearthside Bank will never ask you to provide answers to your security questions, usernames or passwords via email.
- ✓ Ensure you are using secure websites for transactions or purchases check for secure symbols like a lock symbol in the lower right-hand corner of your web browser window, or "https://..." in the address of the website. The "s" indicates "secured" and means the web page uses encryption.
- ✓ Always log off from online banking or any website after using your debit card, or other sensitive information, versus using the back button. If you can't log off, close your browser to prevent any potential unauthorized access to your account information.
- ✓ Keep your browser closed when you're not using the internet.
- ✓ Avoid using unsecured wireless (Wi-Fi) for any online activity requiring a login. If you use wireless take these precautions: Change the default wireless network name or SSID, change the default password and enable encryption
- ✓ Use a current version of your web browser, as many times updates include new security features.
- ✓ Only download from trusted sources and turn on pop-up blockers.
- ✓ Keep your computer operating system and other software programs up to date to ensure the highest level of protection. Even set your operating system to receive automatic updates. The "Help" menu or the software vendor's website may be checked periodically for updates.
- ✓ Install or turn on your computer's firewall.
- ✓ Install, turn on, and keep anti-virus software up to date, along with frequently scheduled scans.
- ✓ Turn your computer off completely when not in use versus leaving it in sleep mode.
- ✓ Avoid online banking activities on public computers. Public computers (computers at internet cafes, copy centers, hotels, etc.) should be used with caution, due to shared use and possible tampering. Online banking activities, purchases and viewing or downloading documents (statements, etc.) should only be done on a computer you know is safe and secure.
- ✓ Minimize the amount of personal information published on social networking websites and use the security features offered on them.
- ✓ Business may want to utilize a separate computer for banking purposes versus other internet accessibility.

Email Security Tips

Email is an easy way to prey on people. Always be suspicious of people asking for personal information in an email. Hearthside Bank will never ask for this type of information in an email.

- ✓ Be cautious of emails from someone you don't know and delete the email without even opening it.
- ✓ Never open attachments, click on links, or respond to emails from unknown senders.
- ✓ Do not include sensitive information in emails
- ✓ If concerned or suspicious of an email, such as those requesting immediate action such as warning for billing information needed or accounts closing etc. Do not click on any link, but instead contact the sender using a telephone number or website you know is legitimate to verify the information or request, not by info in the email itself.

Mobile Device Security Tips

Mobile banking is a new and convenient way to do banking. This is another avenue that thieves might take to get your identity. Make sure you download mobile apps from reputable sources, to ensure the safety of personal information.

- ✓ Always use the keypad lock or phone lock on your mobile device when it is not in use. This password-protects your device to make it harder for someone to view your information. Be sure to store your device in a secure location.
- ✓ If using Text Banking delete text messages from Hearthside Bank or any other institution frequently. Also delete these before loaning out, discarding, or selling your mobile device.
- ✓ Never disclose personal or financial information, including account numbers, passwords, Social Security number or birth date through text message, phone call or email on your mobile device.
- ✓ Sign off when you finish using a Mobile App rather than just closing it, for additional security.

Bank Account Security Tips

Keep these safety tips in mind as you do your banking in the branch, at the ATM machine, or simply use your debit card and pin at any location.

- ✓ Report any lost or stolen debit card, credit card or checks to the bank immediately.
- ✓ Review all account statements carefully and report any fraudulent activity as soon as it's discovered.
- ✓ Use online Banking to monitor your accounts as frequently as you like.
- ✓ Don't print your driver's license number or Social Security number on your checks or any other personal information.
- ✓ Make sure to store new and cancelled checks or statements in a safe and secure location.
- ✓ Always keep your credit or debit card in a safe and secure place as if it were cash or checks
- ✓ Do not put your card number in an email.

- ✓ Do not provide your card number over the phone if you did not initiate the call.
- ✓ Destroy any old or unused debit or credit cards.
- ✓ Make sure no one sees your PIN when you enter it.
- ✓ Memorize your PIN and do not write it down.
- ✓ Only use your card at merchants you trust.
- ✓ Ensure you are using secure websites for transactions or purchases check for secure symbols like a lock symbol in the lower right-hand corner of your web browser window, or “https://...” in the address of the website. The “s” indicates "secured" and means the web page uses encryption.
- ✓ Always log off from after a purchase is made with your credit or debit card. If you can't log off, shut down your browser to prevent unauthorized access to your card information.
- ✓ Securely store or dispose of your transaction receipts.
- ✓ When using an ATM always be aware of your surroundings when withdrawing funds and watch for suspicious persons around the ATM. Make sure no one sees your PIN as you enter it. If you notice anything suspicious, come back later or use an ATM elsewhere. If you are in the middle of a transaction, cancel it; take your card and leave. Then come back at another time or use an ATM at another location. Report all crimes immediately to the owner of the ATM or local law enforcement.
- ✓ Put away any cash as soon as your transaction is complete.

Scam Prevention Tips

There are many different scams out there and new ones popping up every day. Use common sense and remember if it sounds too good to be true, it probably is.

- ✓ Promptly retrieve US Postal mail and consider paperless options to reduce chances of theft.
- ✓ Shred or destroy all personal information and mail solicitations that you aren't interested in.
- ✓ Never give personal information to a stranger who contacts you, whether by telephone, email, or even in person.
- ✓ Remember you are responsible and liable for items which you cash or deposit into your account, whether they are a check, money order, transfer, etc.
 - Don't accept payments for more than the amount of any service if expected to provide back the difference.
 - Don't accept checks from individuals you've met online.
 - Don't accept jobs in which you are paid or receive money for doing money transfers through your account.
- ✓ Be Cautious of phone or email offers of mortgage modification, foreclosure rescue, or short sale scams involving money-back guarantees, title transfers, up-front fees, or high pressure sales tactics.
- ✓ No matter how urgent someone claims a deal or job offer is, you should research and confirm its legitimacy.
- ✓ Review your Credit Report at least annually at annualcreditreport.com or by calling [877-322-8228](tel:877-322-8228).

Hearthside Bank Privacy Policy

Your privacy and security is top priority at Hearthside Bank. Your relationship with us means you provide Hearthside Bank with important personal information about you and your family. WE have always been careful to safeguard the privacy of that information. Our Privacy Statement spells out an important fact. We do not disclose nay information about you to anyone except for companies we work with to provide services to you; such as the Credit Bureau. We have never sold your name and address to another organization for any purpose nor do we ever intend to do so.

We value our customer and will continue to safeguard the confidentiality, security and integrity of all our private information.

Hearthside Bank Privacy Statement for Consumers





At Hearthside Bank, protecting the privacy and confidentiality of your personal information is important to all our employees. We value your business and the trust you put in Hearthside Bank. To offer you the financial products and services you seek, we collect, maintain and use information about you on a routine basis. The help you better understand how your personal financial information is protected; we are providing you with the following statement describing our practices and policies with respect to the privacy of customer information. In the event you terminate your customer relationship with us, or become an inactive customer, we will continue to adhere to the policies and practices described in this notice.

If You are Victim of Identity Theft

If you begin to receive suspicious bills or phone calls from creditors about unknown debts, and you have verified that the suspicious activity has occurred under your personal information without your knowledge, you will need to take the following steps:

1. Place an initial fraud alert
2. Order your credit reports
3. Create an identity theft report

Monitor your progress by creating a system to organize your papers and track deadlines.

Item	How to Track	Tips
Telephone Calls 	Create a log of all telephone calls	<ul style="list-style-type: none">* Record the date of each call and the names and telephone numbers of everyone you contact.* Prepare your questions before you call. Write down the answers.
Postal Mail 	Send letters by certified mail. Ask for a return receipt.	<ul style="list-style-type: none">* See Sample letters
Documents 	Create a filing system.	<ul style="list-style-type: none">* Keep all originals.* Send copies of your documents and reports, not originals. Make copies of your identification to include in letters.
Deadlines 	Make a timeline.	<p>List important dates, including when:</p> <ul style="list-style-type: none">* You must file request* A company must respond to you* You must send follow-up

Step by Step Tasks

If you have a computer, stop using it. Anything you type may be captured by a hacker. Go to www.hearthsidebank.com and install Rapport. Rapport will provide additional software security to shield your online banking details from prying eyes, safeguard your identity, protect your internet banking login details, and help stop malicious attempts against you.

Task	Whom to Contact	What to Do
------	-----------------	------------



- | | | |
|---|-----------------------------------|--------------------------------------|
| 1 | Local Police Office | File a Police Report - get a copy |
| 2 | Credit Card Companies | Close compromised accounts |
| 3 | Hearthside Bank | 606-248-1095 |
| | | Close compromised accounts |
| 4 | Other Banks and Investments | Close compromised accounts |
| 5 | Local Department of Motor Vehicle | May need to get new Driver's License |
| 6 | Contact Phone Service Provider | Check for fraudulent activity |
| 7 | Social Security Department | 1-800-269-0271 |
| | | If you think your SSN was used |
| 8 | Credit Bureau | Place Fraud Alert and review |
| | Equifax | 1-800-525-6285 |
| | Experian | 1-888-EXPERIAN (397-3742) |
| | TransUnion | 1-800-680-7289 |



- | | | |
|---|--|---|
| 1 | Contact U.S. Postal Inspectors Office or local post office | If crime involved stolen mail |
| | | notify of the theft, get a replacement card |
| 2 | Contact Health Insurer | |
| 3 | File complaint with FTC (Federal Trade Commission) | 1-877-IDTHEFT (438-4338) |
| | Mailing Address | TDD: 866-653-4261 |
| | | Identity Theft Clearinghouse |
| | | Federal Trade Commission |
| | | 600 Pennsylvania Avenue, NW |
| | | Washington, DC 20580 |



- | | | |
|--|----------------------------------|--|
| | Keep copies of all communication | never send out originals, make copies of everything you send out |
|--|----------------------------------|--|



- | | | |
|--|--------------------------------------|--|
| | Follow-up | In a few months, order copies of your credit report and check them |
| | Review a Free Credit Report Annually | annualcreditreport.com
877-322-8228 |

Communication Log

Keep track of all your communication, with dates, names, and notes. Keep organized with the below log.

Department	Phone Number/ Address	Contact Date(s)	Contact Name	Notes

Sample Letters

Sample dispute letter – Credit Bureau

Date

Your Name

Your Address

Your City, State, Zip

Complaint Dept

Name 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 requested 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

Name of Creditor

Billing Inquires

Address

City, State, Zip

Dear Sir or Madam,

I'm 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)*



Hearthside Bank

Middlesboro 1602 Cumberland Ave. (606) 248-1095

Harlan 185 Finance St. (606) 573-7050

102 Cumberland Ave. (606)573-1440

Harrogate 6792 Cumberland Gap Pkwy. (423)869-1095

New Tazewell 520 Fifth Ave. (423)626-2030

Jacksboro 300 Main St. (423)566-46

[www hearthsidebank.com](http://www.hearthsidebank.com)