Identity Theft

Emergency Repair Kit

Heritage Bank
Brilliant banking.™

www.heritagebankonline.com

Member FDIC

Identity Theft Emergency Repair Kit

I Think I'm a Victim of Identity Theft! What Should I Do?

If you suspect someone has attempted to steal your identity, or is trying to do so now, you need to take immediate action to limit the damage and protect your good name. The most critical factor in dealing with identity theft loss is **time**.

There are steps you can take to manage the situation, so it's important for you to understand what Identity Theft is, how it might have happened to you and what you can do about it. It's also equally important to learn how to monitor your credit files to help stop identity theft from happening to you again in the future.

That's what the Identity Theft Emergency Repair Kit is all about—helping you take the steps necessary to quickly reclaim your identity, while notifying everyone who needs to know about your loss. This will help limit your personal liability and begin restoring your good credit.

What is Identity Theft and How Did I Become a Victim?

You probably weren't even aware you were a victim until very recently. A criminal obtained your personal information—social security number, birth date, possibly your Drivers' License or Passport and used it to "steal" your identity and name. These identity thieves may have even used that information to gain access to your bank and credit card accounts, open new accounts or obtain credit in your name.

How Did Thieves Get My Personal/Financial Information?

There are a number of ways your identity may have been stolen. Your purse or wallet may have been taken. Perhaps mail was taken from your mailbox. They may have even searched through your trash for discarded bills, bank or credit card statements.

Fake e-mails, web sites or phone calls requesting "verification" of your account numbers, passwords and personal information may have tricked you into divulging information. Credit card companies or stores may have had credit card records stolen by computer hackers and sold on the internet.

How Do These Thieves Use My Identity?

Identity thieves may have opened bank and credit accounts in your name. They often use all of the available credit or write checks to obtain cash. Your own bank accounts and credit accounts may have been drained of any available cash and credit. They may have forged a drivers' license or passport in your name and purchased vehicles, other "large ticket" goods or even rented or purchased homes. If arrested, they may have even used your stolen identity to bond out of jail!

Often, your first indications of Identity Theft are calls or letters from collection agencies, bank overdraft notices or being turned down for a loan. In some cases it might be a police officer informing you of a warrant for arrest you know nothing about!

How Much is This Going to Cost Me Financially?

As stated earlier, time is of the essence. The sooner you begin reporting suspicious activity, the more you can reduce the impact. You may already be facing bank fees, credit card charges and other costs associated with your own accounts, as well as having to explain that you weren't responsible for other accounts you knew nothing about. The good news is that there are some limitations on what firms can try to recover from you, so it's essential that you report the fraud and subsequent losses promptly. As time goes by, these limitations can expire.

Here's a list that summarizes the loss potential and how long you have to make your report:

- **Fraudulent Credit Card Charges:**
  You cannot be held liable for more than $50 for fraudulent purchases made with your credit card, as long as you let the credit card company know within 60 days of when the credit card statement with the fraudulent charges was sent to you. Some credit card issuers say cardholders who are victims of fraudulent transactions on their accounts have no liability for them at all.

- **Lost or Stolen ATM/Debit Card:**
  If your ATM or debit card is lost or stolen, you may not be held liable for more than $50 for the misuse of your card, as long as you notify the bank or credit union within two business days after you realize the card is missing. If you do not report the loss of your card promptly, your liability may increase.

- **Fraudulent Electronic Withdrawals:**
  If fraudulent electronic withdrawals are made from your bank or credit union account, and your ATM or debit card has not been lost or stolen, you are not liable, as long as you notify the bank or credit union in writing of the error within 60 days of the date the bank or credit union account statement with the fraudulent withdrawals was sent to you.

- **Fraudulent Checks:**
  Under most state laws, you are liable for just a limited amount for fraudulent checks issued on your bank or credit union account, as long as you notify the bank or credit union promptly. Contact your state banking or consumer protection agency for more information.

- **Fraudulent New Accounts:**
  Under most state laws, you are not liable for any debt incurred on fraudulent accounts opened in your name and without your permission. Contact your state attorney general's office for more information.

What Should I Do First?

You *can* recover your good name and credit, by following these 5 SIMPLE STEPS!

Follow the 5 simple steps in this workbook to record all needed information, notify financial institutions, credit accounts and others of your loss. We've made it as easy as possible to do all of the things necessary to limit your financial losses, while tracking your progress in restoring your good name and credit.

It is important that you keep track of your reporting and follow-up activities.
(Easy to use forms can be found beginning on page 7.)

STEP ONE: Contact All Three Major Credit Bureaus.

There are three main credit bureaus in the United States: Experian, Equifax and TransUnion. You should request that each bureau issue a "fraud alert" on your credit file. Obtain copies of your credit report and review them for errors and fraudulent activity.

For Credit Bureaus: Use Form A to contact the bureaus and track your progress.

STEP TWO: Contact Your Financial Institutions and Credit Vendors.

Report the identity theft to each creditor and financial institution you do business with—even if you do not have any specific knowledge of a loss from some of them. Change any accounts, access codes, pin codes and passwords you need and replace any ATM or other cards.

Remember to change your online account usernames and passwords!

Ask each company if they have a specific ID Theft Affidavit or theft reporting form you should use to file your report. If they do not, use the ID Theft Affidavit Form in this workbook to make your report. (See Instructions, page in this workbook.)

We have made it easy for you to track your progress in contacting these firms.

For Financial Institutions and Creditors: Complete Form B
For Credit Card Accounts: Complete Form C
For Online Accounts (eBay, Pay Pal, etc.) Complete Form D

(NOTE: DO NOT list any passwords on these forms!)

STEP THREE: File a Local Police Report.

It is important that you file a police report in your local area. Obtain a copy of the filed report, as you will need it to verify to credit issuers, your financial institution and credit bureaus that you were a victim of identity theft. Depending on your situation, the local police or sheriff may recommend filing additional reports with other agencies.

You should also file a report with the Federal Trade Commission (FTC). They act as a clearinghouse on Identity Theft in the United States and often forward reports to other agencies investigating similar crimes. This is also important because providing a printed copy of your FTC ID Theft Complaint to the local police department and having it incorporated in their report creates an Identity Theft Report that provides certain protections.

This Identity Theft Report can be used to:

1) Permanently block fraudulent information from appearing on your credit report
2) Ensure that debts do not reappear on your credit report
3) Prevent a company from continuing to collect debts that result from identity theft
4) Place an extended fraud alert on your credit report.

Reporting to Law Enforcement and the FTC: Use Form E

STEP FOUR: Other Agencies You May Need to Contact:

There are several other organizations that you may need to advise of your identity theft.

These include:

Homeowner/Renter Insurance Carrier. Some homeowner and related policies have coverage for theft losses. Contact your agent or claims department to verify coverage. File a loss report if necessary.

Postal Inspection Service. If you suspect your mail has been tampered with, stolen or an unauthorized address change has been made, contact your local Postmaster or Postal Inspector. You can also make a report at www.usps.com.

Department of Motor Vehicles. If you believe someone has obtained or is attempting to obtain your operator license or identification card using your name or information, report it immediately.

Social Security Administration. If you believe your Social Security Number is being used for fraudulent purposes, contact the Social Security Administration's hotline at 1-800-269-0271.

Utility Service. Criminals may open cellular phone or other utility service accounts using your name. You may need to contact those firms and report the fraud.

U.S. Department of State. If your Passport or Passport Information was stolen, you need to notify the U.S. Department of State of your loss and obtain a replacement. This can be done online at http://travel.state.gov/passport or call 1-877-487-2778.

Track your contacts with other agencies and firms using Form F.

STEP FIVE: Keep Track of Your Accounts.
After you report your identity theft, you need to review all of your account statements and transactions regularly. You should report any discrepancies immediately. Be vigilant in checking your credit reports and monitoring your account statements.

Monitor your monthly statements: Use Form G

That's it! You're now on the road to recovering your credit and good name.

To help you prevent future incidents of Identity Theft, follow these ten tips.

Ten Tips to Secure Your Identity:

1. Never give your Social Security Number or other personal information to anyone online.

2. Do not open unsolicited email, open web pages or call phone numbers listed in suspicious emails, even if it appears urgent or demands an immediate response.

3. Make sure you have anti-spyware and anti-virus software on your computer, keep them updated and run scans at least weekly.

4. Use strong passwords, eight characters or more, including numbers. Use a random order instead of words and change passwords frequently.

5. Check your bank and credit card statements when they arrive and verify any charge you don't remember making.

6. Shred any documents containing personal information before you throw it in the trash.

7. Promptly remove mail from your mailbox. If you're gone for more than a day, have mail held at the Post Office until you return.

8. Keep your passwords and access codes secret! Don't leave them in easy to find places on your desk—at work or in your home.

9. Don't provide personal information over the phone to callers demanding confirmation of your identity.

10. Keep your personal papers, Passports and Social Security Cards secured in a lock box or other device and out of view.

Reporting and Monitoring

Heritage Bank
Brilliant banking.™

FORM A

Credit Bureaus

Contact each Credit Bureau to report Identity Theft, determine the steps necessary to resolve inaccuracies and obtain a copy of your credit report from each bureau.

Bureau	Date Contacted	Contact Name	Notes	Follow-up Needed
Equifax:1-888-766-0008 *www.equifax.com*				
Experian: 888-397-3742 *www.experian.com*				
TransUnion: 1-800-680-7289 *www.transunion.com*				
Other Local Credit Bureau:				

Financial Institutions & Other Creditors

Notify any financial institution or credit issuer you currently have an account or relationship with of any fraudulent activity that has occurred and make any reports necessary.

Heritage Bank
Brilliant banking.™

FORM B

Financial Institution/ Credit Issuer	Account Information	Date of Contact	Name of Contact	Phone Number	Notes

Credit Cards

Heritage Bank
Brilliant banking.™

FORM C

Notify all credit card companies of identification theft. Cancel all current cards and have new ones issued.
Don't forget to destroy any old cards in your possession.

Credit Issuer	Account Information	Date of Contact	Name of Contact	Phone Number	Notes

Online Account Usernames and Passwords Changed

FORM D

Ensure account security by changing usernames and passwords on all accounts, such as online shopping firms, (E-Bay, Pay Pal), etc. *Note: Don't make the passwords too simple!*

Account Name	Account Type	Date Changed	Comments (DO NOT LIST PASSWORD HERE)

Law Enforcement

Heritage Bank
Brilliant banking.™

FORM E

Make a local police report of your loss and identification theft. Ask if there are any other recommended agencies you should contact to make additional reports.

Request a copy of the police report for your records.

Name of Department	Phone Number	Reported to: (Name/Badge Number)	File Number	Notes
Local Police Department or Sheriffs Office				
Federal Trade Commission 1-877-438-4338 www.consumer.gov/idtheft				
Other Law Enforcement Agency				
Other Law Enforcement Agency				
Other Law Enforcement Agency				

Other Agencies/ Firms You May Need to Contact

(Check boxes YES or NO, then complete lines for information as needed)

FORM F

Insurance Company

Is there coverage in homeowner/renter or other policy for ID Theft losses? ❑ Yes ❑ No

Company	Policy#	Contact	Phone	Notes

US Postal Service

Has my address been compromised or mail stolen from mailbox? ❑ Yes ❑ No

Local Postmaster or Inspector	Phone#	Notes

Department of Motor Vehicles

Has my drivers license information been compromised? ❑ Yes ❑ No

Local or State DMV	Phone#	Notes

Utilities

Has my utilities or phone information been compromised? ❑ Yes ❑ No

Utilities Department	Phone#	Notes
Gas		
Electrical/Power		
Phone		
Cable		
Internet		

Social Security Administration

Has my Social Security Number been compromised or a duplicate card been issued without my permission? ❑ Yes ❑ No

800-269-0271 or your local SSA Office	Contacted	Date	Notes

U.S. Department of State

Has my Passport or Passport Information been stolen? ❑ Yes ❑ No

U.S. Department of State	Phone#	Notes
http://travel.state.gov/passport	1-877-487-2778	

Monthly Statement Monitoring

Verify that all activity on your monthly statement is correct.

FORM G

Credit Issuer	Account Type	Date Verified	Notes

Instructions for Completing the ID Theft Affidavit

Instructions for Completing the ID Theft Affidavit

NOTE: This form is ONLY to be used to report that a new account has been opened in your name but does not belong to you. In other words, you are reporting that your identity was stolen and someone else used it to fraudulently open an account.

It should NOT be used to file reports with Law Enforcement or other Government Agencies.

Steps to Completing the Affidavit:

The ID Theft Affidavit has two parts—the ID Theft Affidavit form includes general information, while the Fraudulent Account Statement is specific to the fraudulent account found in your name.

- Contact each company that opened a fraudulent account in your name, ask the following questions:

    a. Do they have specific forms needed to report the fraud?
    b. If they do not have a specific form, explain that you are going to send them the FTC ID Theft Affidavit and Fraudulent Account Statement. Do they require that it be notarized?
    c. How long do you have to file the report? (Some companies want reports filed within two weeks.)

- Complete the first part—the "ID Theft Affidavit," where you report general information about yourself and the theft. You will need to make several copies of this form so that you can send a copy to each company. (If a company requires the notarized form, each copy must be notarized separately.)

- Complete the second part—the "Fraudulent Account Statement," where you describe the fraudulent account that was opened in your name. This form should be completed individually for each company you need to inform of a fraudulent account.

- Make sure you keep copies of each affidavit that you send.

- When you send an affidavit, attach copies (NOT ORIGINALS) of any supporting documents they request, such as a copy of your drivers' license or police report.

- Be as accurate and complete as possible in completing the documents. Printing the information clearly will make it easier and faster to receive a response from the company!

- Mail each affidavit "Certified, Return Receipt Requested" to the company so that you can prove it was received.

- If you are unable to complete the affidavit yourself, a legal guardian or someone with power of attorney may complete it for you.

Name _____ Phone Number _____

ID Theft Affidavit

Victim Information

(1) My full name is _____

(2) (If different from above) When the events described in this affidavit took place, I was known as

_____

(First) (Middle) (Last) (Jr., Sr., lll)

(3) My date of birth is_____
(day/month/year)

(4) My Social Security number is_____

(5) My driver's license or identification card state and number are _____

(6) My current address is _____

City_____ State _____ Zip Code_____

(7) I have lived at this address since_____
(month/year)

(8) (If different from above) When the events described in this affidavit took place, my address was

_____

City_____ State _____ Zip Code_____

(9) I lived at the address in Item 8 from _____until_____
(month/year) (month/year)

(10) My daytime telephone number is (_____) _____

My evening telephone number is (_____) _____

DO NOT SEND AFFIDAVIT TO THE FTC OR ANY OTHER GOVERNMENT AGENCY

Name _____ Phone Number _____

How the Fraud Occurred

Check all that apply for items 11-16:

(11) ☐ I did not authorize anyone to use my name or personal information to seek the money, credit, loans, goods or services described in this report

(12) ☐ I did not receive any benefit, money, goods or services as a result of the events described in this report.

(13) ☐ My identification documents (for example, credit cards; birth certificate; driver's license; Social Security card; etc.) were stolen, lost on or about_____(day/month/year)

(14) ☐ To the best of my knowledge and belief, the following person(s) used my information (for example, my name, address, date of birth, existing account numbers, Social Security number, mother's maiden name, etc.) or identification documents to get money, credit, loans, goods or services without my knowledge or authorization:

_____
Name (if known)

_____
Address (if known)

_____
Phone numbers(s) (if known)

_____
Additional information (if known)

_____
Name (if known)

_____
Address (if known)

_____
Phone numbers(s) (if known)

_____
Additional information (if known)

(15) ☐ I do NOT know who used my information or identification documents to get money, credit, loans, goods or services without my knowledge or authorization.

(16) ☐ Additional comments: (For example, description of the fraud, which documents or information were used or how the identity thief gained access to your information.)

_____

_____

_____

_____

_____

(attach additional pages as necessary)

DO NOT SEND AFFIDAVIT TO THE FTC OR ANY OTHER GOVERNMENT AGENCY

Name _____ Phone Number _____

Victim's Law Enforcement Actions

(17) (check one) I ☐ am ☐ am not willing to assist in the prosecution of the person(s) who committed this fraud.

(18) (check one) I ☐ am ☐ am not authorizing the release of this information to law enforcement for the purpose of assisting them in the investigation and prosecution of the person(s) who committed this fraud.

(19) (check all that apply) I ☐ have ☐ have not reported the events described in this affidavit to the police or other law enforcement agency. The police ☐ did ☐ did not write a report. In the event you have contacted the police or other law enforcement agency, please complete the following:

_____ (Agency # 1)

_____ (Officer/Agency personnel taking report)

_____ (Date of report)

_____ (Report number, if any)

_____ (Phone numbers)

_____ (email address, if any)

_____ (Agency #2)

_____ (Officer/Agency personnel taking report)

_____ (Date of report)

_____ (Report number, if any)

_____ (Phone number)

_____ (email address, if any)

Documentation Checklist

Please indicate the supporting documentation you are able to provide to the companies you plan to notify. Attach copies (NOT originals) to the affidavit before sending it to the companies.

(20) ☐ A copy of a valid government-issued photo-identification card (for example, your driver's license, state-issued ID card or your passport). If you are under 16 and don't have a photo-ID, you may submit a copy of your birth certificate or a copy of your official school records showing your enrollment and place of residence.

(21) ☐ Proof of residency during the time the disputed bill occurred, the loan was made or the other event took place (for example, a rental/lease agreement in your name, a copy of a utility bill or a copy of an insurance bill).

DO NOT SEND AFFIDAVIT TO THE FTC OR ANY OTHER GOVERNMENT AGENCY

Name _____ Phone Number _____

(22) ☐ A copy of the report you filed with the police or sheriff's department. If you are unable to obtain a report or report number from the police, please indicate that in Item 19. Some companies only need the report number, not a copy of the report. You may want to check with each company.

Signature

I certify that, to the best of my knowledge and belief, all the information on and attached to this affidavit is true, correct, and complete and made in good faith. I also understand that this affidavit or the information it contains may be made available to federal, state, and/or local law enforcement agencies for such action within their jurisdiction as they deem appropriate. I understand that knowingly making any false or fraudulent statement or representation to the government may constitute a violation of 18 U.S.C. §1001 or other federal, state, or local criminal statutes, and may result in imposition of a fine or imprisonment or both.

_____ _____

(signature) (date signed)

_____

(Notary)

[Check with each company. Creditors sometimes require notarization. If they do not, please have one witness (non-relative) sign below that you completed and signed this affidavit.]

Witness:

_____ _____

(signature) (printed name)

_____ _____

(date) (telephone number)

Name _____ Phone Number _____

Fraudulent Account Statement

Completing this Statement

- Make as many copies of this page as you need. Complete a separate page for each company you're notifying and only send it to that company. Include a copy of your signed affidavit.
- List only the account(s) you're disputing with the company receiving this form. See the example below.
- If a collection agency sent you a statement, letter or notice about the fraudulent account, attach a copy of that document (NOT the original).

I declare (check all that apply):

☐ As a result of the event(s) described in the ID Theft Affidavit, the following account(s) was/were opened at your company in my name without my knowledge, permission or authorization using my personal information or identifying documents:

Creditor Name/Address *(the company that opened the account or provided the goods or services)*	Account Number	Type of unauthorized credit/goods/services provided by creditor *(if known)*	Date issued or opened *(if known)*	Amount/Value provided *(the amount charged or the cost of the goods/services)*
Example *Example National Bank* *22 Main Street* *Columbus, Ohio 22722*	*01234567-89*	*Auto Loan*	*01/05/2007*	*$25,500.00*

☐ During the time of the accounts described above, I had the following account open with your company:

Billing name_____

Billing address_____

Account number_____

DO NOT SEND AFFIDAVIT TO THE FTC OR ANY OTHER GOVERNMENT AGENCY