FIRST HOPE BANK

Identity Theft
Prevention & Resolution Kit

A guide designed to help you protect your identity and to provide solutions if you become a victim.

P.O. Box 296 • Hope, NJ 07844 • (908) 459-4121 • Fax (908) 459-5429
E-Mail: info@firsthope.com • Web Site: www.firsthope.com

FIRST HOPE BANK

Index

Dear Customer:

We are glad you have taken the opportunity to learn more about identity theft – the fastest growing white collar crime in the United States. Some people think it can't happen to them, but it does happen – right here in northwest New Jersey. The best offense is a good defense, so we have compiled some information on how you can help safeguard your identity.

Identity theft is a serious crime. People whose identities have been stolen can spend months or years – and their hard-earned money – cleaning up the mess thieves have made of their good name and credit record. In the meantime, victims may lose job opportunities, be refused loans, education, housing or cars, or even get arrested for crimes they did not commit. If you think or know you have become the victim of identity theft, be assured that we will work with you every step of the way to correct all unauthorized transactions in your First Hope Bank accounts.

Enclosed are additional materials we hope you will find helpful when documenting and resolving this problem with your other service providers:

- Tips to avoid becoming a victim of identity theft and steps to take if you do become a victim.
- A list of organizations, including helpful phone numbers, to which you may report fraudulent activity.
- An identity theft affidavit accompanied by a fraudulent account statement.

We hope you will find these materials useful in managing this process and minimizing further risk and exposure if you have become a victim of identity theft. To read First Hope Bank's privacy policy regarding our customer's sensitive financial and personal information, please visit www.firsthope.com/privacypolicy.htm. Should you have any questions concerning your fraud claim, please contact First Hope Bank at (908) 459-4121, (908) 813-3119, or (973) 729-8333.

Thank you for your business, and we look forward to serving your financial needs.

First Hope Bank

FIRST HOPE BANK

Simple Steps to Safeguard Your Identity

Up to 500,000 individuals are victims each year of identity theft, a fast-growing form of fraud. "Identity theft" or "account takeover fraud" involves criminals stealing a person's personal information. The crooks assume a person's identity, apply for credit in his or her name, run up huge bills, stiff creditors, and generally wreck the victim's credit record. Fortunately, a few simple steps can help you avoid becoming a statistic.

At First Hope Bank, we put a combination of safeguards in place to protect customers, including employee training, rigorous security standards, data encryption and fraud detection. You can take these steps to avoid being a victim:

- Do not give your Social Security or account numbers to anyone over the telephone unless you initiated the call.
- Tear up or shred receipts, old bank statements and unused credit card offers before throwing them away. Crooks can steal information from the trash and use it to get credit in your name.
- Review your bank and credit card statements as soon as you receive them to check for unauthorized transactions.
- Protect your PINs and computer passwords; use a combination of letters and numbers and change them often. Never carry this information with you!
- Order copies of your credit report once a year to ensure accuracy. You can contact one of the three national credit bureaus (TransUnion (800) 888-4213, Equifax (800) 685-1111, and Experian (888) 397-3742) to order a credit report. As of September 1, 2005, consumers from all states can request an annual free credit report as a result of the Fair and Accurate Credit Transactions Act (FACT Act), signed into law in 2003. To obtain your free yearly credit report, visit www.annualcreditreport.com, call (877) 322-8228, or write to: Annual Credit Report Request Service, P.O. Box 105283, Atlanta, GA 30348-5283.
- Report any suspected fraud to your bank and credit card issuers immediately so they can start to close accounts and clear your name right away.

By law, you are only liable for the first $50 of unauthorized charges against a credit card account. Still, restoring your identity can be a tremendous inconvenience. It is worth your while to exercise preventive maintenance to protect yourself against this crime.

For more personal finance tips, visit our web site at www.firsthope.com or visit the American Bankers Association's Consumer Connection at www.aba.com.

A SPECIAL WORD ABOUT SOCIAL SECURITY NUMBERS

Very likely, your employer and financial institution will need your SSN for wage and tax reporting purposes. Other private businesses may ask you for your SSN to do a credit check, such as when you apply for a car loan. Sometimes, however, they simply want your SSN for general record keeping. If someone asks you for your SSN, ask the following questions:

- Why do you need it?
- How will it be used?
- How do you protect it from being stolen?
- What will happen if I don't give it to you?

If you don't provide your SSN, some businesses may not provide you with the service or benefit you want. Getting satisfactory answers to your questions will help you to decide whether you want to share your SSN with the business.

Manage Your Mailbox

- Do not leave bill payment envelopes clipped to your mailbox or inside with the flag up; criminals may steal your mail and change your address.
- Know your billing cycles, and watch for any missing mail. Follow up with creditors if bills or new cards do not arrive on time. An identity thief may have filed a change of address request in your name with the creditor or the post office.
- Carefully review your monthly accounts, credit card statements and utility bills (including cellular telephone bills) for unauthorized charges as soon as you receive them. If you suspect unauthorized use, contact the provider's customer service and fraud departments immediately.
- When you order new checks, ask when you can expect delivery. If your mailbox is not secure, then ask to pick up the checks instead of having them delivered to your home.
- Although many consumers appreciate the convenience and customer service of general direct mail, some prefer not to receive offers of pre-approved financing or credit. To "opt out" of receiving such offers, call (888) 5-OPT-OUT sponsored by the three credit bureaus.
- The Direct Marketing Association offers services to help reduce the number of mail and telephone solicitations. To join their mail preference service, visit their website at **https://www.dmaconsumers.org**, or mail your name, home address and signature, along with a $1 check or money order made payable to DMA (no cash, please) to: Mail Preference Service, P.O. Box 282, Carmel, NY 10512.

Check Your Purse or Wallet

- Never leave your purse or wallet unattended – even for a minute.
- Protect your PINs (don't carry them in your wallet!) and passwords; use a 10-digit combination of letters and numbers for your passwords, and change them periodically.
- Carry only personal identification and credit cards you actually need in your purse or wallet. If your I.D. or credit cards are lost or stolen, notify the creditors immediately, and ask the credit bureaus to place a "fraud alert" in your file.
- Keep a list of all your credit cards and bank accounts along with their account numbers, expiration dates and credit limits, as well as the telephone numbers of customer service and fraud departments. Store this list in a safe place.
- If your state uses your Social Security number as your driver's license number, ask to substitute another number.
- Line up closely the contents of your wallet on a photocopy machine; do both sides of each license, credit card, etc. You will know what you had in your wallet and all of the account numbers and phone numbers to call and cancel. Keep the photocopy in a safe place.

Keep Your Personal Numbers Safe and Secure

- When creating passwords and PINs (personal identification numbers) do not use any part of your Social Security number, birth date, middle name, wife's name, child's name, pet's name, mother's maiden name, address, consecutive numbers, or anything that a thief could easily deduce or discover.
- Ask businesses to substitute alpha-numeric code as a password instead of your mothers maiden name.
- Shield the keypad when using ATMs or when placing calling card calls.
- Memorize your passwords and PINs; never keep them in your wallet, purse, Rolodex or electronic organizer, and never write your PIN on your debit or credit card!

FIRST HOPE BANK

OnGuard Online's Computer News and Notes: Be Safe Online

Reference:
http://ftc.gov/bcp/edu/pubs/articles/naps22.pdf

Being on guard online can help protect your information, your computer – even yourself. Experts say these seven practices can help you be safe while surfing.

1. Protect your personal information. It's valuable. To minimize your risk of identity theft, don't share your personal information unless you know how it will be used and protected. Don't reply to or click on links in any e-mail asking for your personal information.
2. Know who you're dealing with. When shopping online, look for a seller's physical address and a working telephone number. Before downloading free software, read the fine print – some downloads come with spyware.
3. Use antivirus software and a firewall, and update both regularly. Look for antivirus software that recognizes current viruses, as well as older ones; effectively reverses the damage; and updates automatically. If your firewall was shipped in the "off" mode, turn it on, and be sure to set it up properly.
4. Be sure to set up your operating system and Web browser software properly, and update them regularly. Select security settings high enough to reduce your risk of being hacked. Make sure to regularly update your system with the latest patches.
5. Protect your passwords. Keep your passwords in a secure place, and don't share them on the Internet, over e-mail, or on the phone.
6. Back up important files. If you have important files stored on your computer, copy them onto a removable disc and store it in a safe place.
7. Learn who to contact if something goes wrong online. Visit **OnGuardOnline.gov** and click on "File a Complaint" to learn how to respond if problems occur when you're online.

The website also provides practical tips (including the ones above) from the federal government and the technology industry to help you be on guard against Internet fraud, secure your computer, and protect your personal information.

Web Watch

The helpful content at OnGuardOnline.gov includes tips, articles, videos and quizzes. The site shows you how to report spam or scams and how to sign up for periodic computer security alterations while its interactive quizzes are a fun way to help you figure out how savvy you are about computer safety.

ATM Cards, Debit Cards and Electronic Fund Transfers

The Electronic Fund Transfer Act provides consumer protections for transactions involving an ATM or debit card or any other electronic way to debit or credit an account. It also limits your liability for unauthorized electronic fund transfers.

It's important to report lost or stolen ATM and debit cards immediately because the amount you can be held responsible for depends on **how quickly** you report the loss.

- If you report your ATM card lost or stolen within two business days of discovering the loss or theft, your losses are limited to $50.
- If you report your ATM card lost or stolen after the two business days, but within 60 days after a statement showing an unauthorized electronic fund transfer, you can be liable for up to $500 of what a thief withdraws.
- If you wait more than 60 days, you could lose **all** the money that was taken from your account from the end of the 60 days to the time you reported your card missing.

The best way to protect yourself in the event of an error or fraudulent transaction is to call the financial institution and follow up in writing – by certified letter, return receipt requested – so you can prove when the institution received your letter. Keep a copy of the letter you send for your records.

After receiving notification about an error on your statement, the financial institution generally has 10 business days to investigate. The institution must tell you the results of its investigation within three business days after completing it and must correct an error within one business day after determining that the error has occurred. If the institution needs more time, it may take up to 45 days to complete the investigation – but only if the money in dispute is returned to your account and you are notified promptly of the credit. At the end of the investigation, if no error has been found, the institution may take the money back if it sends you a written explanation.

Note: VISA and MasterCard voluntarily have agreed to limit consumers' liability for unauthorized use of their debit cards in most instances to $50 per card, no matter how much time has elapsed since the discovery of the loss or theft of the card.

For more information, see Credit, ATM and Debit Cards: What to Do If They're Lost or Stolen, a consumer publication from the FTC at ***www.consumer.ftc.gov/articles/0213-lost-or-stolen-credit-atm-and-debit-cards***

Where can I obtain more information?

To learn more about Identity Theft, you can visit the websites listed below.

Credit Bureaus

- www.equifax.com
- www.experian.com
- www.transunion.com

ID Theft Links

- www.consumer.gov/idtheft
- www.ftc.gov/credit

Reference: http://www.ftc.gov/bcp/conline/pubs/credit/idcrisis.shtm

"I don't remember opening that credit card account. And I certainly didn't buy those items I'm being billed for."

Maybe you never opened that account, but someone else did… someone who used your name and personal information to commit fraud. When an imposter co-opts your name, your Social Security Number (SSN), your credit card number, or some other piece of your personal information for their use – in short, when someone appropriates your personal information without your knowledge – it's a crime.

The biggest problem? You may not know your identity's been stolen until you notice that something's amiss: you may get bills for a credit card account you never opened; your credit report may include debts you never knew you had; a billing cycle may pass without your receiving a statement; or you may see charges on your bills that you didn't sign for, didn't authorize, and don't know anything about.

First Things First

If you are a victim of identity theft, Consumer Financial Protection Bureau, the nation's consumer protection agency, recommends you take the following steps:

1. **You have the right to ask the nationwide consumer reporting agencies to place "fraud alerts" in your file** to let potential creditors and others know that you may be a victim of identity theft. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you. It also may delay your ability to obtain credit. You may place a fraud alert in your file by calling just one of the three nationwide consumer reporting agencies. As soon as that agency processes your fraud alert, it will notify the other two, which then also must place fraud alerts in your file.
   - Equifax: 1.888.766.0008; PO Box 740241 Atlanta GA 30374
   - Experian: 1.888.EXPERIAN (397.3742); PO Box 2002 Allen TX 75013
   - Trans Union: 1.800.680.7289; PO Box 6790 Fullerton CA 92834

   An initial fraud alert stays in your file for at least 90 days. An extended alert stays in your file for seven years. To place either of these alerts, a consumer reporting agency will require you to provide appropriate proof of your identity, which may include your social security number. If you ask for an extended alert, you will have to provide an identity theft report. An identity theft report includes a copy of a report you have filed with a federal, state or local law enforcement agency, and additional information a consumer reporting agency may require you to submit. For more detailed information about the identity theft report, visit www.consumerfinance.gov.
2. **You have the right to free copies of the information in your file (your "file disclosure").** An initial fraud alert entitles you to a copy of all information in your file at each of the three nationwide agencies, and an extended alert entitles you to two free file disclosures in a 12 month period following the placing of the alert. These additional

disclosures may help you detect signs of fraud, for example, whether fraudulent accounts have been opened in your name or whether someone has reported a change of address. Once a year, you also have the right to a free copy of the information in your file.

3. **You have the right to obtain documents relating to fraudulent transactions made or accounts opened using your personal information.** A creditor or other business must give you copies of applications and other business records relating to transactions and accounts that resulted from the theft of your identity, if you ask for them in writing. A business may ask you for proof of your identity, a police report, and an affidavit before giving you the documents. It also may specify an address for you to send your request. Under certain circumstance, a business can refuse to provide you with these documents. See www.consumer.gov/idtheft.
4. **You have the right to obtain information from a debt collector.** If you ask, a debt collector must provide you with certain information about the debt you believe was incurred in your name by an identity theft- like the name of the creditor and the amount of the debt.
5. **If you believe information in your file results from identity theft, you have the right to ask that a consumer reporting agency block that information from your file.** An identity thief may run up bills in your name and not pay them. Information about the unpaid bills may appear on your consumer report. Should you decide to ask a consumer reporting agency to block the reporting of this information, you must identify the information to block, and provide the consumer reporting agency with proof of your identity and a copy of your *identity theft report.* The consumer reporting agency can refuse or cancel your request for a block if, for example, you don't provide the necessary documentation, or where the block results from an error or a material misrepresentation of fact made by you. If the agency declines or rescinds the block, it must notify you. Once a debt resulting from identity theft has been blocked, a person or business with notice of the block may not sell, transfer or place the debt for collection.
6. **You also may prevent businesses from reporting information about you to consumer reporting agencies if you believe the information is a result of identity theft.** To do so, you must send your request to the address specified by the business that reports the information to the consumer reporting agency. The business will expect you to identify what information you do not want reported and to provide an *identity theft report.*

To learn more about identity theft and how to deal with its consequences, visit www.consumer.gov/idtheft or write to the FTC. You may have additional rights under state law. For more information, contact your local consumer protection agency or your state attorney general.

In addition to the new rights and procedures to help consumers deal with the effects of identity theft, the FCRA has many other important consumer protections. They are described in more detail at www.ftc.gov/credit.

SAMPLE DISPUTE 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 writing to dispute the following information in my file. The items I dispute also 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.)

I am a victim of identity theft, and did not make the charge(s). I am requesting that the item be blocked to correct my credit report.

Enclosed are copies of (use this sentence if applicable and describe any enclosed documentation) supporting my position. Please investigate this (these) matter(s) and block the disputed item(s) as soon as possible.

Sincerely,

Your name

Enclosures: (List what you are enclosing.)

To make certain you do not become responsible for the debts incurred by the identity thief, you must prove to each of the companies where accounts were opened in your name that you didn't create the debt. The ID Theft Affidavit was developed by a group of credit grantors, consumer advocates, and attorneys at the Federal Trade Commission (FTC) for this purpose. Importantly, this affidavit is only for use where a new account was opened in your name. If someone made unauthorized charges to an existing account, call the company for instructions.

While many companies accept this affidavit, others require that you submit more or different forms. Before you send the affidavit, contact each company to find out if they accept it. If they do not accept the ID Theft Affidavit, ask them what information and/or documentation they require.

You may not need the ID Theft Affidavit to absolve you of debt resulting from identity theft if you obtain an Identity Theft Report. We suggest you consider obtaining an Identity Theft Report where a new account was opened in your name. An 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 reports; (3) prevent a company from continuing to collect debts or selling the debt to others for collection; and (4) obtain an extended fraud alert.

The ID Theft Affidavit may be required by a company in order for you to obtain applications or other transaction records related to the theft of your identity. These records may help you prove that you are a victim. For example, you may be able to show that the signature on an application is not yours. These documents also may contain information about the identity thief that is valuable to law enforcement.

This affidavit has two parts:

- **ID Theft Affidavit** – is where you report general information about yourself and the theft.
- **Fraudulent Account Statement** – is where you describe the fraudulent account(s) opened in your name. Use a separate Fraudulent Account Statement for each company you need to write to.

When you send the affidavit to the companies, attach copies (**NOT** originals) of any supporting documents you have (e.g., driver's license, police report). Before submitting your affidavit, review the disputed account(s) with family members or friends who may have information about the account(s) or have access to them.

Complete this affidavit as soon as possible. Many creditors ask that you send it within two weeks. Delaying could slow the investigation.

Be as accurate and complete as possible. You *may* choose not to provide some of the information requested. However, incorrect or incomplete information will slow the process of investigating your claim and absolving the debt. Print clearly.

When you have finished completing the affidavit, mail a copy to each creditor, bank, or company that provided the thief with the unauthorized credit, goods, or services you describe. Attach a copy of the Fraudulent Account Statement with information only on accounts opened at the institution to which you are sending the packet, as well as any other supporting documentation you are able to provide.

Send the appropriate documents to each company by certified mail, return receipt requested, so you can prove that it was received. The companies will review your claim and send you a written response telling you the outcome of their investigation. **Keep a copy of everything you submit.**

Documents concerning accounts at First Hope Bank should be mailed to:

First Hope Bank
P.O. Box 296
Hope, NJ 07844
Attention: Compliance Officer

If you cannot complete the affidavit, a legal guardian or someone with power of attorney may complete it for you. Except as noted, the information you provide will be used only by the company to process your affidavit, investigate the events you report, and help stop further fraud. If this affidavit is requested in a lawsuit, the company might have to provide it to the requesting party. Completing this affidavit does not guarantee that the identity thief will be prosecuted or that the debt will be cleared.

If you haven't already done so, report the fraud to the following organizations:

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

- **Equifax:** 1-800-525-6285; **www.equifax.com**
- **Experian:** 1-888-EXPERIAN (397-3742); **www.experian.com**
- **TransUnion:** 1-800-680-7289; **www.transunion.com**

In addition, once you have placed a fraud alert, you're entitled to order one free credit report from each of the three consumer reporting companies, and, if you ask, they will display only the last four digits of your Social Security Number on your credit reports.

2. The security or fraud department of each company where you know, or believe, accounts have been tampered with or opened fraudulently. Close the account. 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 Personal Identification Numbers (PINs) and passwords. Avoid using easily available information like your mother's maiden name, your birth date, the last four digits of your Social Security Number, your phone number, or a series of consecutive numbers.

3. Your local police department or the police in the community where the identity theft took place. Provide a copy of your ID Theft Complaint filed with the FTC (see below), to be incorporated into the police report. Get a copy of the police report or, at the very least, the number of the report. It can help you deal with creditors who need proof of the crime. If the police are reluctant to take your report, ask to file a "Miscellaneous Incidents" report, or try another jurisdiction, like your state police. You can also check with your state Attorney General's office to find out if state law requires the police to take reports for identity theft. Check the Blue Pages of your telephone directory for the phone number or check **www.naag.org** for a list of state Attorneys General.

4. The Federal Trade Commission. By sharing your identity theft complaint with the FTC, you will provide important information that can help law enforcement officials across the nation track down identity thieves and stop them. The FTC also can refer victims' complaints to other government agencies and companies for further action, as well as investigate companies for violations of laws that the FTC enforces.

You can file a complaint online at **www.consumer.gov/idtheft**. If you don't have Internet access, call the FTC's Identity Theft Hotline, toll-free: 1-877-IDTHEFT (438-4338); TTY: 1-866-653-4261; or write: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580. When you file an ID Theft Complaint with the FTC online, you will be given the option to print a copy of your ID Theft Complaint. You should bring a copy of the printed ID Theft Complaint with you to the police to be incorporated into your police report. The ID Theft Complaint, in conjunction with the police report, can create an Identity Theft Report that will help you recover more quickly. The ID Theft Complaint provides the supporting details necessary for an Identity Theft Report, which go beyond the details of a typical police report.

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

ID Theft Affidavit

Victim Information

(1) My full legal name is _____
(First) (Middle) (Last) (Jr., Sr., III)

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

_____
(First) (Middle) (Last) (Jr., Sr., III)

(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

How the Fraud Occurred

Check all that apply for items 11 – 17:

(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)	Name (if known)
_____	_____
Phone number(s) (if known)	Phone number(s) (if known)
_____	_____
Name (if known)	Name (if known)
_____	_____
Additional information (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

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 number) (E-mail address, if any)

_____ _____

(Agency #2) (Officer/Agency personnel taking report)

_____ _____

(Date of report) (Report number, if any)

_____ _____

(Phone number) (E-mail 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).

(22) ❒ A copy of the report you filed with the police or other law enforcement agency. 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)

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

Fraudulent Account Statement

Name _____ Phone number _____

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 (*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, OH 22722	01234567-89	Auto Loan	01/05/2002	$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

FIRST HOPE BANK

Contact Worksheet

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

Other Important Numbers	Phone Number	Contact Date	Contact Person	Comments
FTC ID Theft Hotline	(877) ID-THEFT			
Local Police Department				
ChexSystems	(888) 478-6536			
Social Security Fraud Hotline	(800) 269-0271			
Internal Revenue Service	(800) 829-0433			
New Jersey Motor Vehicle Commission	(609) 292-6500			
Pennsylvania Dept. of Transportation	(800) 932-4600			

Financial Institutions	Phone Number	Contact Date	Contact Person	Comments
First Hope Bank	(908) 459-4121			

Creditors	Phone Number	Contact Date	Contact Person	Comments