

## A Resolution Adopting an Identity Theft Prevention Program

The Nassau County Commission does hereby adopt, pursuant to the General Corporation Law of Florida, the following Resolution:

WHEREAS the Board of County Commissioners finds that identity theft is a serious problem for providers in the county and throughout the country; and

WHEREAS in response to the risks posed by identity theft to consumers and to the financial soundness of businesses, the United States Congress enacted the Fair and Accurate Credit Transactions Act of 2003 (FACT Act); and

WHEREAS The Federal Trade Commission (FTC), along with federal bank regulators, adopted regulations implementing the FACT Act (the Red Flag Rules) that require creditors to adopt a written Identity Theft Prevention Program; and

WHEREAS the Nassau Board of County Commissioners believes it is a creditor subject to the FTC's Red Flag Rules; and;

WHEREAS a written Identity Theft Prevention Program designed to detect, prevent, and mitigate identity theft has been developed.

NOW THEREFOR BE IT RESOLVED THAT:

- (1) The Board of County Commissioners hereby approves the Identity Theft Prevention Program submitted; and
- (2) The Clerk of Court/Chief Financial Officer is delegated responsibility for oversight, ongoing development, implementation, and administration of the program and shall have the responsibility to develop periodic updates to the program to reflect changes in risk to customers and to the safety and soundness of the organization.

Effective Date: May 1, 2009.

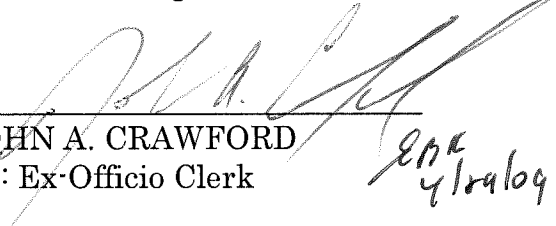
BOARD OF COUNTY COMMISSIONERS  
NASSAU COUNTY, FLORIDA



---

BARRY HOLLOWAY  
Its: Chairman

Attestation: Only to Authenticity as to  
Chairman's Signature



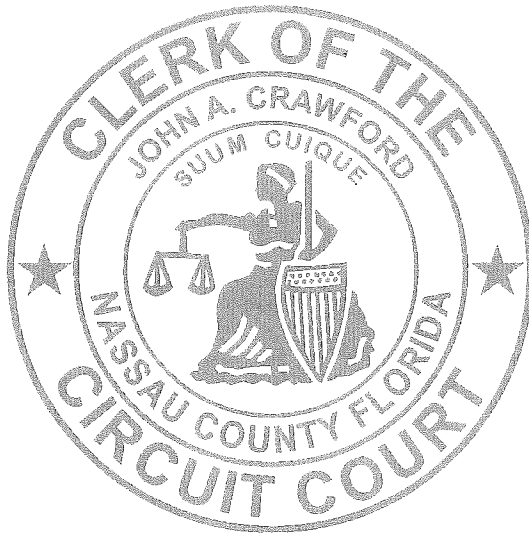
JOHN A. CRAWFORD  
Its: Ex-Officio Clerk

*EMK  
4/19/09*

Approved as to form by the  
Nassau County Attorney:



DAVID A. HALLMAN



---

## Identity Theft Prevention Program

For

Nassau County Clerk of Courts

Billing Office

76347 Veterans Way

Yulee, FL 32097

---

This Program is intended to identify red flags that will alert our employees when new or existing accounts are opened using false information, protect against the establishment of false accounts, provide methods to ensure existing accounts are not opened using false information and measures to respond to such events.

### Contact Information:

The Nassau County Clerk of Courts is responsible for this program;

Name: John A. Crawford

Title: Nassau County Clerk of Courts

Phone number: 904-548-4800/548-4600

---

Revision Date: May 11, 2009

Implementation Date: May 1, 2009

## Risk Assessment:

The Nassau County Clerk of Courts Financial Services Billing Department has conducted an internal risk assessment to evaluate how at risk the current procedures are at allowing customers to create a fraudulent account and evaluate if current (existing) accounts are being manipulated. This risk assessment evaluated how new accounts were opened and the methods used to access the account information. Using this information, the billing department was able to identify red flags that were appropriate to prevent identity theft on the following:

- New accounts opened In Person
  - New accounts opened via Fax
  - New accounts opened via Telephone
  - Account information accessed In Person
  - Account information accessed via Telephone (Person)
  - Account information accessed via Fax
  - Identity theft occurred in the past from someone falsely using a current account or falsely opening a utility account
- 

## Detection (Red Flags):

Nassau County Clerk of Courts Financial Services Billing Department has adopted the following red flags to detect potential fraud. These are not intended to be all-inclusive and other suspicious activity may be investigated as necessary.

- Identification documents appear to be altered
  - Photo and physical description do not match appearance of customer
  - Other information is inconsistent with information provided by customer
  - Other information provided by customer is inconsistent with information on file.
  - Information provided is associated with known fraudulent activity (e.g. address or phone number provided is same as that of a fraudulent application)
  - SS#, address, Drivers License # or telephone # is the same as that of other billing customer
  - Customer fails to provide all information requested
  - Personal information provided is inconsistent with information on file for a customer
  - Customer cannot provide information requested beyond what could commonly be found in a purse or wallet
  - Identity theft is reported or discovered
  - Security Breach
  - Unauthorized access/downloading of a covered account or files
-

## Response:

Any employee that may suspect fraud or detect a red flag will implement the following response as applicable. All detections or suspicious red flags shall be reported to the senior management official.

- Ask applicant for additional documentation
  - Notify supervisor: Any employee who becomes aware of a suspected or actual fraudulent use of a customer or potential customers' identity must notify the Billing Supervisor, Financial Services Director, or Clerk of Courts
  - Notify law enforcement: The Financial Services Director will notify the Nassau County Sherriff at 904-225-0331 of any attempted or actual identity theft.
  - Do not open the account
  - Close the account
  - Do not attempt to collect against the account but notify authorities
- 

## Customer Notification:

If there is a confirmed incident of identity theft or attempted identity theft, Nassau County Clerk of Courts Financial Services billing office will notify the customer after consultation with law enforcement about the timing and the content of such notification (to ensure notification does not impede a law enforcement investigation) via certified mail. See customer notification letter-Appendix A. Victims of identity theft will be encouraged to cooperate with law enforcement in identifying and prosecuting the suspected identity thief, and will be encouraged to complete the FTC Identity Theft Affidavit-See appendix D.

---

## Personal Information Security Procedures:

The Nassau County Clerk of Courts Financial Services Billing Office adopted the following security procedures:

1. ID verification before discussing Account Information. Before discussing any information related to a covered account with any individual, or making a change to any information on a covered account; personnel shall sufficiently ascertain the identity of the individual. Customer or appropriate representative of the customer should be able to verify the date of birth, social security number (or at least last 4 digits) and/or address to whom the account pertains. If the customer or appropriate representative of the customer presents in person, a photo ID in addition to the information above must be provided. If unable to provide the necessary information, the staff shall make a notation of the inquiry on the customer account and alert an appropriate supervisor without providing access or honoring the address change request.
2. Paper documents, files, and electronic media containing secure information will be stored in locked file cabinets after business hours. File cabinets will be stored in a locked area.

3. Only specially identified employees with a legitimate need will have access to the keys to the room and cabinet. Keys are kept in protected location except when locking or unlocking the file cabinet.
4. Files containing personally identifiable information are kept in locked file cabinets except during work hours when an authorized employee is always present.
5. Employees will not leave uncovered sensitive papers out on their desks when they are away from the area of their workstations.
6. Employees store sensitive files in locked file cabinets when leaving their work areas at the end of the day.
7. Employees log off their computers when leaving their work areas.
8. Employees keep access to the finance office area locked at all times.
9. Access to offsite storage facilities is limited with access keys in possession of Nassau County Clerk of Courts staff. Access to the Clerk's storage facility will be strictly enforced.
10. Any sensitive information shipped will be shipped using a shipping service that allows tracking of the delivery of this information.
11. Visitors who must enter areas where sensitive files are kept must be escorted by a Clerk of Courts staff member.
12. No visitor will be given any entry codes/cards or allowed unescorted access to the finance office.
13. Passwords will not be shared or posted near workstations.
14. Sensitive information that is sent to third parties over public networks will be encrypted.
15. When sensitive data is received or transmitted, secure connections will be used.
16. Computer passwords will be required.
17. User names and passwords will be different.
18. Anti-virus and anti-spyware programs will be run on servers daily.

19. The computer network will have a firewall where your network connects to the Internet.
  20. The use of laptops is restricted to those employees who need them to perform their jobs.
  21. Laptops will be stored in secure place. Employees will never leave a laptop visible in a car, hotel luggage stand or packed in checked luggage. If laptop must be left in vehicle, it should be stowed in a safe, secure manner.
  22. Check references or do background checks before hiring employees who will have access to sensitive data.
  23. New employees sign an agreement to follow company confidentiality and security standards for handling sensitive data.
  24. Procedures exist for making sure that workers who leave our employ or transfer to another part of the company no longer have access to sensitive information.
  25. Employees who violate security policy are subject to discipline, up to and including dismissal.
  26. Ensure complete destruction of paper documents containing customer information. Paper records will be shredded before being placed into the trash.
- 

#### Outside Service Providers:

In the event that the county engages a service provider to perform an activity in connection with one or more covered accounts the County Coordinator shall exercise his or her discretion in reviewing such arrangements in order to ensure, to the best of his or her ability, that the service provider's activities are conducted in accordance with policies and procedures, agreed upon by contract, that are designed to detect any red flags that may arise in the performance of the service provider's activities and take appropriate steps to prevent or mitigate identity theft. See appendix B

---

## Identity Theft Prevention Program Review and Approval

This plan has been reviewed and adopted by John A. Crawford, Nassau County Clerk of Courts. Appropriate employees have been trained on the contents and procedures of this Identity Theft Prevention Program.

This plan has been reviewed and adopted by:

Name of: John A. Crawford, Nassau County Clerk of Courts

Signature: \_\_\_\_\_

Date: \_\_\_\_\_

A report will be prepared annually and submitted to the above named senior management or governing body to include matters related to the program, the effectiveness of the policies and procedures, the oversight and effectiveness of any third party billing and account establishment entities, a summary of any identify theft incidents and the response to the incident, and recommendations for substantial changes to the program, if any.

Revision Date: May 11, 2009

Implementation Date: May 1, 2009



CUSTOMER NOTIFICATION LETTER- Appendix A

**THIS SHOULD BE ON LETTERHEAD**

[Date]

**Via Certified Mail Return Receipt Requested**

[Applicant/Patient Name]

[Applicant /Patient Address]

Re: Suspected Identity Theft

Dear: \_\_\_\_\_:

This letter addresses the unauthorized use of your name and other personal information at the Nassau County Clerk of Courts Billing Office on [date]. [Insert: Explain factual situation and describe compromise of information in detail (e.g., how it happened, information disclosed, what actions have been take to remedy situation, etc.)]. We have reported this incident to [name of law enforcement officer] at the Nassau County Sheriffs office, who can be reached at \_\_\_\_\_. We also have placed an alert on your account in an effort to prevent further misuse of your identity.

Identity theft is very serious because it can cause severe financial harm and take a long time to correct. If you believe you are the victim of identity theft, you should, in addition to the measures outlined below, ask to review and make appropriate corrections to your [personal/medical] information.

**[INSERT FOR RESCUE BILLING ONLY-For your health and safety, it is very importation that your medical records do not contain information about another person. We request your assistance in ensuring that our records about you are correct. We recommend that you carefully monitor explanations of benefits (EOBs) or other remittance advice or account statements received from your health insurer to determine if any other person has used your identity to obtain health care. If you receive an EOB or bill for health care services you believe you did not receive, immediately contact your insurer and the health care provider who furnished the services.]**

We also recommend that you place a fraud alert on your credit file. A fraud alert tells creditors to contact you and verify your identity before they open any new accounts or change existing accounts.

Please contact one of the three major credit bureaus. Once a credit bureau confirms your fraud alert, the others are notified to place fraud alerts. The numbers for the credit bureaus are:

- Equifax: 1-800-685-1111
- Experian: 1-888-397-3742
- TransUnion Corp: 1-800-680-7289

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, immediately notify the credit bureaus. If you believe an unauthorized account has been opened in your name, immediately contact the financial institution that holds the account.

You should also file a police report of identity theft. Get a copy of the police report. You may need to give copies of the police report to creditors to clear up your records. Creditors want the information it contains to absolve you of the fraudulent debts. You should also file a complaint with the FTC at [www.ftc.gov/idtheft/](http://www.ftc.gov/idtheft/) or 1-877-ID-THEFT (877-438-4338). Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcers for their investigations.

We encourage you to report any helpful information to \_\_\_\_\_  
[investigating law enforcement officer] at the Nassau County Sheriff Office. We also encourage you to alert other area health care providers that your identifying information is being used in a fraudulent manner.

If there is anything that our office can do to assist you please call our Compliance/Privacy Officer at 904-548-4800

Sincerely

[Name of Compliance/Privacy Officer]

## Business Associate Agreement-Appendix B

### BUSINESS ASSOCIATE AGREEMENT FOR RED FLAG RULES COMPLIANCE

This will serve as a Business Associate Agreement (“BA Agreement”) between [COC/BOCC] and \_\_\_\_\_ (Business Associate). The Parties acknowledge that acceptance of this Amendment by the Business Associate is an essential requisite to providing its contracted services to [COC/BOCC].

1. This Amendment is incorporated into the existing BA Agreement between the parties and is an integral part of that agreement.
2. This Amendment shall be effective as of \_\_\_\_\_ (date) as long as the existing BA Agreement has not been terminated.
3. This Amendment is executed pursuant to the requirements of the Identity Theft Red Flag Rules promulgated under the Fair and Accurate Credit Transactions Act of 2003 (“Red Flag Rules”) found at 16 C.F.R. Part 681.
4. The Business Associate of [COC/BOCC] agrees to assume the following obligations.
  - a) Business Associate agrees to ensure that its activities for [COC/BOCC] are conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft.
  - b) Business Associate agrees to have in place policies and procedures to detect relevant Red Flags that may arise in the performance of services on behalf of [COC/BOCC].
  - c) Business Associate agrees that it has received a copy of [COC/BOCC] Identity Theft Prevention Program and that it will take all steps necessary to comply with the policies and procedures therein.
  - d) Business Associate will ensure that any agent or third party, who performs services on behalf in connection with [COC/BOCC] covered accounts, including a subcontractor, agrees to implement reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft.
  - e) Business Associate agrees to alert [COC/BOCC] of any red flag incident (as defined by the Red Flag Rules) of which it becomes aware, and the steps it has taken to mitigate any potential security compromise that may have occurred, and provide a report to [COC/BOCC] of any threat of identity theft as a result of the incident.
  - f) Business Associate authorizes termination of the BA Agreement if [COC/BOCC] reasonably determines that Business Associate has violated a material term of this Amendment.

Agreed to this \_\_\_\_\_ day of \_\_\_\_\_, 2009

John A. Crawford

[Business Associate]

Nassau County Clerk of Courts

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

Date: \_\_\_\_\_

Date: \_\_\_\_\_

## **Job Description-Appendix C**

### **Language for Job Description of Red Flag Rules Compliance Officer**

NOTE: This information should be added to an existing job description.

The [Job Title of Individual responsible] shall also be responsible for compliance with the Red Flag Rules and shall be responsible for:

1. The implementation of Nassau County Clerk of Courts Financial Services billing office Identity Theft Prevention Program; and
2. Reporting to the [appropriate individual] at least annually on compliance by the Nassau County Clerk of Courts Financial Services billing office with the Program. The report shall address material matters related to the program and evaluate issues such as:
  - a. The effectiveness of the policies and procedures of the Nassau County Clerk of Courts Financial Services billing office in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts;
  - b. Service provider agreements;
  - c. Incidents involving identity theft and management's response; and
  - d. Recommendations for material changes to the program.

## **ID Theft Affidavit-Appendix D**

### **Instructions for Completing the ID Theft Affidavit**

To make certain that you do not become responsible for any debts incurred by an 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:

- Part One — the ID Theft Affidavit — is where you report general information about yourself and the theft.
- Part Two — the 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 (for example, driver's license or 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 access to them.

Complete this affidavit as soon as possible. Many creditors ask that you send it within two weeks. Delays on your part 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.

If you are unable to 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 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](http://www.equifax.com)
- **Experian:** 1-888-EXPERIAN (397-3742); [www.experian.com](http://www.experian.com)
- **TransUnion:** 1-800-680-7289; [www.transunion.com](http://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 accounts. 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 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 also can 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](http://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](http://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**

Revision Date: May 11, 2009

Implementation Date: May 1, 2009



**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)

\_\_\_\_\_  
Address (if known)

\_\_\_\_\_  
Address (if known)

\_\_\_\_\_  
Phone number(s) (if known)

\_\_\_\_\_  
Phone number(s) (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 was 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)

\_\_\_\_\_  
(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**

(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)

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

### Fraudulent Account Statement

**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)

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**