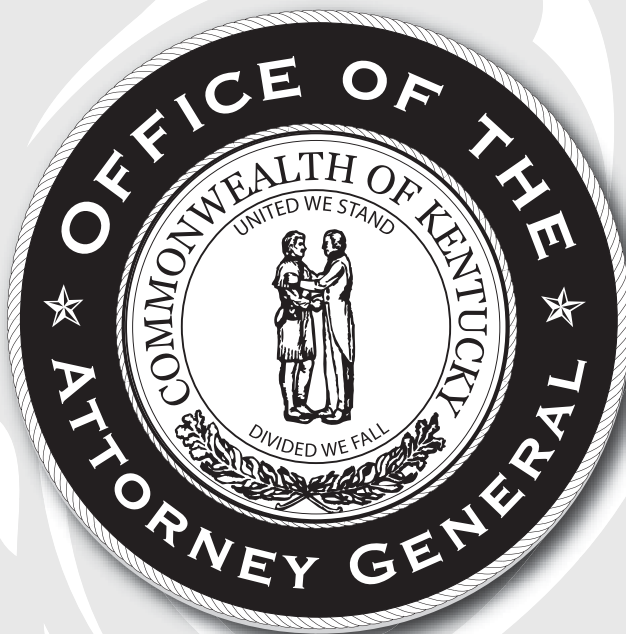


# IDENTITY THEFT

## VICTIM KIT



# IDENTITY THEFT

## KENTUCKY VICTIM KIT

If you are a victim of identity theft, or you suspect that someone is using your name and personal identification information, this kit is designed to help you through the process of resolving your identity theft case and clearing your name. This kit was specifically developed to provide assistance to Kentuckians who are identity theft victims, as well as individuals in other states who had their personal information fraudulently used in the state of Kentucky.

### **What is Identity Theft?**

Identity theft is a crime. It involves acquiring key pieces of someone's identifying information, such as name, address, date of birth, social security number and mother's maiden name, in order to impersonate them. This information enables the thief to commit numerous forms of fraud which include taking over a victim's financial accounts, opening new bank accounts, applying for loans, credit cards and social security benefits, using existing credit accounts to run up charges, writing bad checks, renting apartments, buying cars and establishing services with utility and phone companies. Thieves will ruin their victim's credit. They will also use their victim's name when committing crimes or driving offenses, resulting in warrants being issued in the victim's name.

### **How does identity theft occur?**

Offenders who commit identity theft may or may not know the victim. The offender may obtain personal information, including information related to financial accounts, from trash bins, mailboxes, stolen wallets or purses, using email or the Internet or from dishonest personnel who work at banks, mortgage firms, social or credit agencies, doctor's offices, collection agencies and other businesses where personal or credit information can be accessed.

### **What do I do if I become a victim?**

Navigating through the system as an identity theft victim can be a lengthy and confusing process. As you contact law enforcement, creditors, and financial institutions, it is important that you keep track of the actions you take and maintain a record of your progress. In the back of this kit, you will find a chart to help with your record keeping.

As soon as you become aware that your information has been misused, there are several basic steps you should take that apply to nearly all kinds of identity theft cases. The following are steps that should be taken immediately. When you have completed a step, check it off.

## Obtain a copy of your credit report

Fraud victims are entitled to a free credit report. A person who believes they are the victim of identity theft should obtain a copy of their credit record. Carefully review the entire credit reporting record. Any errors or actions that are suspect or fraudulent should be immediately submitted to ALL of the credit reporting agencies. A list of those agencies is found below.

### **Equifax**

P.O. Box 740241  
Atlanta, GA 30374-0241  
To order your report: 1-800-685-1111  
To report fraud: 1-800-525-6285  
TDD: 800-255-0056

### **TransUnion**

Fraud Victim Assistance  
P.O. Box 6790  
Fullerton, CA 92634-6790  
Email: fvad@transunion.com  
To order your report: 1-800-888-4213  
To report fraud: 1-800-680-7289  
TDD: 877-553-7803

### **Experian** (formerly TRW)

P.O. Box 9532  
Allen, TX 75013  
To order your report: 1-888-EXPERIAN (397-3742)  
To report fraud: 1-888-EXPERIAN (397-3742)  
TDD: 800-972-0322

## Report the incident to law enforcement

A person who believes they are a victim of identity theft is encouraged to promptly report those facts to a law enforcement agency. You should report to the law enforcement agency that has jurisdiction both where the crime occurred and where you live. The address and telephone number for the Commonwealth's Attorney, County Attorney, and the local police department can be found in your local telephone directory. Once a report has been filed, request a copy of the report so that it will be available to send to credit reporting agencies and creditors.

When you file the report, provide as much documentation as possible, including copies of debt collection letters, credit reports, and your notarized ID Theft Affidavit (located at the back of this kit).

Identity theft is a Class D Felony under KRS 514.160. Theft related to credit or debit cards is a Class A Misdemeanor or Class D Felony under KRS 434.550 – 434.730.

## Notify all of the Credit Report Bureaus

- 1) **Report identity theft, and the theft of any credit cards or credit card numbers, to each credit reporting agency. Request that all your accounts be "Flagged with a fraud alert."**  
*Contact information for the agencies is listed on page 2.*

### **Fraud Alerts**

There are two types of fraud alerts: an **initial alert**, and an **extended alert**.

- **An initial alert stays on your credit report for at least 90 days.** You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial alert is appropriate if your wallet has been stolen or if you've been taken in by a "phishing" scam. When you place an initial fraud alert on your credit report, you're entitled to one free credit report from each of the three nationwide consumer reporting companies.
- **An extended alert stays on your credit report for seven years.** You can have an extended alert placed on your credit report if you've been a victim of identity theft and you provide the consumer reporting company with an "identity theft report." When you place an extended alert on your credit report, you're entitled to two free credit reports within twelve months from each of the three nationwide consumer reporting companies. In addition, the consumer reporting companies will remove your name from marketing lists for pre-screened credit offers for five years unless you ask them to put your name back on the list before then.

To place either of these alerts on your credit report, or to have them removed, you will be required to provide appropriate proof of your identity: that may include your SSN, name, address and other personal information requested by the consumer reporting company.

- 2) When a business sees the alert on your credit report, they must verify your identity before issuing you credit. As part of this verification process, the business may try to contact you directly. This may cause some delays if you're trying to obtain credit. To compensate for possible delays, you may wish to include a cell phone number, where you can be reached easily, in your alert. Remember to keep all contact information in your alert current.

### **Active Duty Alerts for Military Personnel**

If you are a member of the military and away from your usual duty station, you may place an active duty alert on your credit reports to help minimize the risk of identity theft while you are deployed. Active duty alerts are in effect on your report for one year. If your deployment lasts longer, you can place another alert on your credit report.

When you place an active duty alert, you'll be removed from the credit reporting companies' marketing list for prescreened credit card offers for two years unless you ask to go back on the list before then.

See **Consumer Reporting Companies** for contact information. The process for getting and removing an alert, and a business's response to your alert, are the same as that for an initial alert. See Fraud Alerts. You may use a personal representative to place or remove an alert.

## Consider putting a Security Freeze on Your Credit Report (effective July 12, 2006)

You may want to put a "security freeze" on your credit report with each credit reporting bureau. A security freeze means that your credit report or credit score cannot be shared with others, such as potential creditors, without your authorization. This can help prevent further identity theft because most businesses will not open credit accounts without first checking your credit report. Additionally, if someone tries to change certain information in a frozen credit report (like your name, address, birth date, or SSN), the credit bureau must send written confirmation of the change to you within 30 days. Each credit bureau may charge you up to \$10 for security freezes, but there is no fee for an identity theft victim who provides a valid police report upon request. (The amount of the fee is subject to a yearly CPI adjustment.)

To put a security freeze on your credit report, send a written request by certified mail to the credit bureaus (see addresses below), with proper identification, and with the required fee. You may want to call each credit bureau, or visit their internet websites, to confirm the amount of the fee and any special information they need with your request. After receiving the request, the credit bureau must place the freeze within 10 business days of receiving your request and send you a password or PIN to use for making changes to the security freeze.

Equifax Security Freeze  
PO Box 105788  
Atlanta, GA 30348  
800-685-1111  
www.equifax.com

Experian Security Freeze  
PO Box 9554  
Allen, TX 75013  
888-397-3742  
www.experian.com

TransUnion Security Freeze  
PO Box 6790  
Fullerton, CA 92834-6790  
888-909-8872  
www.transunion.com

You can allow access to your credit report for a specific period of time after you have placed a security freeze (for obtaining credit, or for a potential employer or lessor, or for any other reason), or you can permanently remove the freeze. To do so, you must contact each credit bureau from which you want to temporarily lift or remove the freeze, and provide proper identification and the fee. Again, you may want to call the credit bureau or visit its website for specific information about temporarily lifting a freeze. Be sure that you make the request ahead of time, because the credit bureau has three business days to comply with your request.

## Contact all credit card companies, creditors, banks and financial institutions

Contact all credit card companies, creditors, banks and financial institutions where you have accounts that may have been affected or where an account may have been created in your name, without your knowledge.

- 1) Request that those accounts be processed as "Account Closed at Consumer's Request."
- 2) Get replacement cards with new account numbers.
- 3) Stop payments on any checks or withdrawal drafts that are suspect.
- 4) Change any passwords and PIN numbers on the accounts, including any Automated Teller Machine (ATM) accounts with banks, savings institutions, other financial service entities, credit cards, online entities and merchants.

- 5) Do not use the old password, mother's maiden name, birth date, any portion of your Social Security number, or other easily obtained passwords. Follow up all telephone contacts with a written confirmation.

## Contact check verification companies

Contact the major check verification companies if you have had checks stolen or bank accounts set up by an identity thief. Inform the verification companies that you are an identity theft victim.

CheckRite 1-800-234-7800  
ChexSystems 1-800-428-9623 (closed checking accounts)  
CrossCheck 1-800-552-1900  
Equifax 1-800-437-5120  
International Check Services 1-800-631-9656  
National Processing Co. (NPC) 1-800-526-5380  
SCAN 1-800-262-7771  
TeleCheck 1-800-710-9898

## Contact utility and service provider companies

Contact utility and service provider companies such as: the local telephone company, long distance telephone company, cable company, Internet service provider, and electric, power, gas or water providers. Alert each company or service provider of the theft of your identity and inform them that attempts may be made to open new service using your identification information. Request that any new request for service be confirmed with you and provide a telephone number and mailing address. Keep a copy of all of these requests.

## Contact your local post office

Notify your local U.S. Postal Inspector if you suspect an identity thief has filed a change of your address with the post office or has used the mail to commit fraud. Find out what your address was changed to. Notify the local Postmaster for that address to forward all mail addressed to you to your correct address. You may also need to talk with the mail carrier on the route where fraudulent mail is being sent. Confirm all telephone conversations in writing. To obtain the telephone number of your local post office, call 800-275-8777.

The phone numbers for U.S. Postal Inspectors and Post Offices can also be obtained through their website: [www.usps.gov/postalinspectors](http://www.usps.gov/postalinspectors)

## Contact the Federal Trade Commission

File a report of an identity theft and obtain assistance in restoring credit by contacting the Federal Trade Commission, Consumer Response Center at:

**Consumer Response Center  
Federal Trade Commission**  
600 Pennsylvania Avenue, NW, Washington, D.C. 20580  
Toll-free telephone: 1-877-438-4338  
Online: [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft)

The FTC also has an Internet website ([www.consumer.gov/idtheft/info.htm](http://www.consumer.gov/idtheft/info.htm)) with useful Internet links to other federal agencies and non-profit organizations that provide assistance to victims of identity theft.

## Contact the Social Security Administration

Report a misuse or possible theft of your Social Security Number to the Office of the Inspector General of the Social Security Administration:

**Social Security Administration, Fraud Hotline**  
**Office of the Inspector General**  
P.O. Box 17768, Baltimore, MD 21235  
Toll-free telephone: 1-800-269-0271  
Fax: 1-410-597-0018  
Online: [www.ssa.gov/oig/hotline/](http://www.ssa.gov/oig/hotline/)  
EMail: [oig.hotline@ssa.gov](mailto:oig.hotline@ssa.gov)

## Obtain a copy of your criminal history record

Request a copy of your own Criminal History Record by contacting the Criminal Records Section of the Kentucky State Police at (502) 227-8713 to obtain a "request for review" form and further instructions.

To request your record by mail, send a letter stating that you are requesting a review of your KY criminal history record; provide a copy of a photo ID, such as a driver's license; and provide a notarized signature. There is also a \$10.00 payment due at the time of request that should be made payable to the "KY State Treasurer." Send your request to:

KSP Criminal Identification and Records Branch  
Criminal Records Section  
1250 Louisville Road  
Frankfort, KY 40601

## Contact the Division of Driver Licensing

At your request, the Department of Transportation's Division of Driver Licensing will place a flag on your driver's license if you are a victim of identity theft (regardless of whether your Kentucky Driver's License has been compromised). Contact the Division of Driver Licensing at:

Kentucky Department of Transportation  
Division of Driver Licensing  
200 Mero Street  
Frankfort, KY 40622  
502-564-6800 x5366

## Contact the FBI for Internet or online fraud

If the theft of an identity is the result of, or otherwise connected to, an Internet or other online fraud, file an online complaint with the Internet Fraud Complaint Center of the Federal Bureau of Investigation at: [www.ifccfbi.gov](http://www.ifccfbi.gov)

## Contact the U.S. State Department

All identity theft victims, whether they have a passport or not, should contact the U.S. State Department. Victims should request the State Department confirm, in writing to the address you have provided, any application for a passport or changes of address, etc.

Internet/On-line Assistance is available at: [www.travel.state.gov/passport/lost/us/us\\_848.html](http://www.travel.state.gov/passport/lost/us/us_848.html)

## Contact other federal agencies as necessary

Numerous federal agencies have jurisdiction over specific aspects of identity theft. If you experience a theft related to any of the following categories, contact the agencies directly for help and information or to initiate an investigation.

### **Bank Fraud**

If you're having trouble getting your financial institution to help you resolve your banking-related identity theft problems, including problems with bank-issued credit cards, contact the agency with the appropriate jurisdiction. If you're not sure which of the agencies listed below has jurisdiction over your institution, call your bank or visit: [www.ffiec.gov/enforcement.htm](http://www.ffiec.gov/enforcement.htm)

Federal Deposit Insurance Corporation (FDIC) at 1-800-934-3342. Online: [www.fdic.gov](http://www.fdic.gov)

Federal Reserve System (Fed) at (202) 452-3693. Online: [www.federalreserve.gov](http://www.federalreserve.gov)

National Credit Union Association (NCUA) at (703) 518-6360. Online: [www.ncua.gov](http://www.ncua.gov)

Office of the Comptroller of Currency (OCC) at 1-800-613-6743. Online: [www.occ.treas.gov](http://www.occ.treas.gov)

Office of Thrift Supervision (OTS) at (202) 906-6000. Online: [www.ots.treas.gov](http://www.ots.treas.gov)

### **Bankruptcy Fraud**

If you believe someone has filed for bankruptcy in your name, write to the U.S. Trustee in the region where the bankruptcy was filed. A list of the offices is available online at: [www.usdoj.gov/ust](http://www.usdoj.gov/ust)

### **Investment Fraud**

If you believe that an identity thief has tampered with your securities investments or a brokerage account, immediately report it to your broker or account manager or the U.S. Securities and Exchange Commission (SEC). You can file a complaint with the SEC online at: [www.sec.gov/complaint.shtml](http://www.sec.gov/complaint.shtml)

### **Cellular and Long Distance Phone Fraud**

If you are having trouble getting fraudulent phone charges removed from your account or getting an unauthorized account closed, contact the Federal Communications Commission (FCC) at 1-888-CALL FCC (1-888-225-5322). File a complaint online at: [www.fcc.gov](http://www.fcc.gov)



## Tax Fraud

If you believe someone has assumed your identity to file Federal Income Tax Returns, or to commit other tax fraud, contact the Internal Revenue Service (IRS) at 1-800-829-0433. Online: [www.treas.gov/irs/ci](http://www.treas.gov/irs/ci)

## Stay alert!

Once resolved, most cases of identity theft stay resolved. But occasionally, some victims have recurring problems. To help stay on top of the situation, continue to monitor your credit reports and read your financial account statements promptly and carefully. You may want to review your credit reports once every three months in the first year of the theft, and once a year thereafter. And stay alert for other signs of identity theft, like:

- failing to receive bills or other mail. Follow up with creditors if your bills don't arrive on time. A missing bill could mean an identity thief has taken over your account and changed your billing address to cover his tracks
- receiving credit cards that you didn't apply for.
- being denied credit, or being offered less favorable credit terms, like a high interest rate, for no apparent reason
- getting calls or letters from debt collectors or businesses about merchandise or services you didn't buy

## Getting your Credit Report

### Free Annual Credit Reports

A recent amendment to the federal Fair Credit Reporting Act requires each of the major nationwide consumer reporting companies to provide you with a free copy of your credit reports, at your request, once every 12 months.

To order your free annual report from one or all of the national consumer reporting companies, visit <http://www.annualcreditreport.com>, call toll-free 877-322-8228, or complete the Annual Credit Report Request Form and mail it to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The form is at the back of this brochure; or you can print it from <http://www.ftc.gov/credit>. Do not contact the three nationwide consumer reporting companies individually. They provide free annual credit reports only through [www.annualcreditreport.com](http://www.annualcreditreport.com), 877-322-8228, and Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For more information, see Your Access to Free Credit Reports, a publication from the FTC.

## Other consumer rights to free reports

Under federal law, you're entitled to a free report if a company takes adverse action against you, such as denying your application for credit, insurance, or employment, and you request your report within 60 days of receiving notice of the action. The notice will give you the name, address, and phone number of the consumer reporting company. You're also entitled to one free report a year if you're unemployed and plan to look for a job within 60 days; you are on welfare; or your report is inaccurate because of fraud. Otherwise, a consumer reporting company may charge you up to \$9.50 for another copy of your report within a 12-month period.

To buy a copy of your report, contact:

Equifax: 800-685-1111 ; [www.equifax.com](http://www.equifax.com)

Experian: 888-EXPERIAN (888-397-3742) ; [www.experian.com](http://www.experian.com)

TransUnion: 800-916-8800; [www.transunion.com](http://www.transunion.com)

# CHART YOUR COURSE OF ACTION

Use this form to record the steps you've taken to report the fraudulent use of your identity . Keep this list in a safe place for reference.

## NATION WIDE CONSUMER REPORTING COMPANY'S —REPORT FRAUD

Consumer Reporting Company	Phone Number	Date Contacted	Contact Person	Comments
Equifax	1.800.525.6285			
Experian	1.888.EXPERIAN (397.3742)			
TransUnion	1.800.680.7289			

## BANKS, CREDIT CARD ISSUERS AND OTHER CREDITORS (Contact each creditor promptly to protect your legal rights.)

Creditor	Address and Phone Number	Date Contacted	Contact Person	Comments

## LAW ENFORCEMENT AUTHORITIES —REPORT IDENTIFY THEFT

Agency / Department	Phone Number	Date Contacted	Contact Person	Report Number	Comments

# 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 or used in your name that you didn't create the debt.

A group of credit grantors, consumer advocates, and attorneys at the Federal Trade Commission (FTC) developed an ID Theft Affidavit to make it easier for fraud victims to report information. 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.

It will be necessary to provide the information in this affidavit anywhere a new account was opened in your name. The information will enable the companies to investigate the fraud and decide the outcome of your claim. If someone made unauthorized charges to an existing account, call the company for instructions.

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 to placing the fraud alert, the three consumer reporting companies will send you free copies of your credit reports, 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 or 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 to file a 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.

**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)
_____	_____
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 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)**

\_\_\_\_\_  
(Date of report)

\_\_\_\_\_  
(Phone number)

\_\_\_\_\_  
(Officer/Agency personnel taking report)

\_\_\_\_\_  
(Report number, if any)

\_\_\_\_\_  
(email address, if any)

\_\_\_\_\_  
**(Agency #2)**

\_\_\_\_\_  
(Date of report)

\_\_\_\_\_  
(Phone number)

\_\_\_\_\_  
(Officer/Agency personnel taking report)

\_\_\_\_\_  
(Report number, if any)

\_\_\_\_\_  
(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

### 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	01/05/2002	\$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



This kit was compiled by the Office of the Kentucky Attorney General with the assistance of materials from other state attorneys general and the federal government.

For more information contact:

Office of the Attorney General  
Consumer Protection Division  
1024 Capital Center Drive, Suite 200  
Frankfort, Kentucky 40601

(502) 696-5389  
Toll Free: 1-888-432-9257  
Online: [www.ag.ky.gov](http://www.ag.ky.gov)

The OAG does not discriminate on the basis of race, color, national origin, sex, religion, age or disability in employment or in the provision of services and provides upon request, reasonable accommodation necessary to afford individuals with disabilities an equal opportunity to participate in all programs and activities.