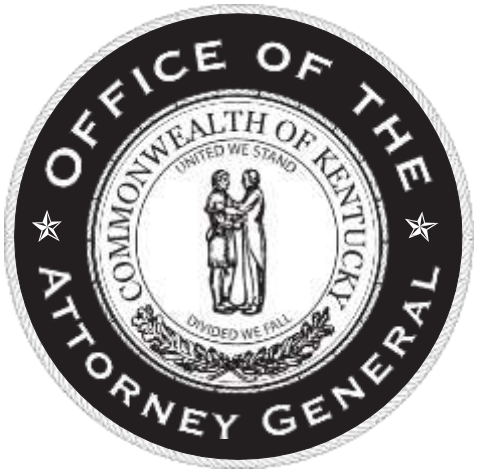
IDENTITY THEFT

KENTUCKY 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. Some of the information and forms in this kit are from or based on information in the Federal Trade Commission's "*Taking Charge – What To Do If Your Identity Is Stolen*", available online at www.ftc.gov/idtheft – please consult that publication for additional forms and sample letters that consumers may use .

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.

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.

☐ Place an Initial Fraud Alert

Contact one of the credit reporting bureaus and ask them to place a fraud alert on your credit file. **Placing a fraud alert is free. Confirm that the credit reporting bureau you call will contact the other two.**

Equifax: 1-800-525-6285 Experian: 1-888-397-3742 TransUnion: 1-800-680-7289

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 provided personal information in a phishing or telephone 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.

When a business sees the alert on your credit report, they should verify your identity before issuing you credit. As part of this verification process, the business may try to contact you directly. 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.

☐ Order your credit reports

After you place an initial fraud alert, you 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 the credit reporting agencies.

Equifax, http://www.equifax.com
To order your report: 1-800-525-6285

Experian, http://www.transunion.com
To order your report: 1-888-397-3742

TransUnion, http://www.transunion.com
To order your report: 1-800-680-7289

☐ Review your credit reports and dispute errors with credit reporting bureaus and companies where you have existing accounts or unauthorized accounts

Closely review your credit reports. If you notice errors in the reports or about your existing accounts, or notice accounts you did not authorize, contact the credit reporting bureaus and the fraud department of each credit card company, creditor, bank and financial institution where you have an account that may have been affected or where an account may have been created in your name, without your knowledge. Send them letters explaining the errors, and keep copies for your files.

After the business gets notice from the credit reporting bureau, it has 30 days to investigate and respond to the credit reporting bureau. If the business finds an error, it must notify the credit reporting bureau so your credit file can be corrected, and if this changes your credit file the credit reporting bureau must send you a letter. The credit reporting bureau can't add the disputed information back into your file unless the business says the information is correct, and if the information is added back in your file the credit reporting bureau must send you a letter.

Credit reporting bureaus must block identity theft-related information from appearing on your credit report within 4 business days after accepting your Identity Theft Report, and tell the business that sent the fraudulent information about the block. If the credit reporting bureaus does not accept your Identity Theft Report, it can ask you for more proof and must notify if it accepts the additional information or will not block the identity theft-related information.

After a business has been notified about a block of fraudulent information, it must stop reporting that information to the credit reporting bureaus and not sell or transfer a debt for collection.

Some sample letters are available from the FTC's website and *Taking Charge* publication, www.ftc.gov/idtheft.

☐ Create an Identity Theft Report

An Identity Theft Report helps you deal with credit reporting companies, debt collectors, and businesses that opened accounts in your name. You can use the Report to:

- get fraudulent information removed from your credit report
- stop a company from collecting debts that result from identity theft, or from selling the debt to another company for collection
- place an extended fraud alert on your credit report
- get information from companies about accounts the identity thief opened or misused

To create an Identity Theft Report:

1. Use the affidavit form located in the back of this kit, or submit a complaint about the theft to the FTC online at www.ftc.gov/complaint and be sure to print a copy for yourself as your FTC Identity Theft Affidavit. Or call the FTC at 1-877-438-4338 [1-866-653-4261 TTY]. You can use the Affidavit when to file a police report (next step).
2. File a police report about the identity theft with your local law enforcement agency, and get a copy of the police report or the report number.
3. Attach your FTC Identity Theft Affidavit to your police report to make an Identity Theft Report.

Information about your rights as an identity theft victim, and an FTC memo that you can share with your law enforcement agency about identity theft reports, is available online at www.ftc.gov/idtheft.

Some companies want more information than the Identity Theft Report includes, or want different information. The information you need to provide depends on the policies of the credit reporting company and the business that sent the information about you to the credit reporting company.
When you file the report, provide as much documentation as possible, including copies of debt collection letters, credit reports, and your notarized Identity Theft Affidavit.

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.

☐ Consider Putting a Security Freeze on Your Credit Reports

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	Experian	TransUnion
1-800-525-6285	1-888-397-3742	1-888-909-8872
www.equifax.com	www.experian.com	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 utility and service provider companies

Contact utility and service provider companies such as your telephone service provider, 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 1-877-876-2455.

The phone numbers for U.S. Postal Inspectors and Post Offices can also be obtained through their website, https://postalinspectors.uspis.gov/.

☐ 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, or visit your local Social Security Administration office.

Social Security Administration, Fraud Hotline
Office of the Inspector General
P.O. Box 17785, Baltimore, MD 21235
Toll-free telephone: 1-800-269-0271
Fax: 1-410-597-0118
TTY: 1-866-501-2101 for the deaf or hard of hearing
Online: https://www.socialsecurity.gov/fraudreport/oig/public_fraud_reporting/form.htm

☐ Tax Fraud

If someone gets a job by using your Social Security number, the earnings will be reported to the tax authorities in your name but you will be unaware of them. When you file your tax returns, you won't include those earnings, and the tax authority may contact you for not reporting those earnings. Also, if someone uses your Social Security number to file a tax return in your name before you file they may get your refund, which will affect your ability to get a refund in the time you expect. Respond quickly to notices from the Internal Revenue Service (IRS) and the Kentucky Department of Revenue.

If you believe someone has assumed your identity to file income tax returns or to commit other tax fraud, contact the IRS and the Kentucky Department of Revenue.

Internal Revenue Service
1-800-908-4490
www.irs.gov/identitytheft

Kentucky Department of Revenue
502-564-4581
http://revenue.ky.gov/

☐ Student Loan Fraud

An identity thief may use your personal or financial information to get a student loan. Contact the U.S. Department of Education Office of the Inspector General, lender, school or program that opened the loan to report the fraud and ask them how to clear the loan from your name.

U.S. Department of Education Office of the Inspector General
1-800-647-8733
www.ed.gov/about/offices/list/oig/hotline.html

☐ Criminal and Traffic Violations

If an identity thief uses your personal information to commit a crime or during an investigation or arrest, the information may be added to a national or local law enforcement criminal database or court records. If this happens to you, contact the local law enforcement agency or prosecutor involved in the case to obtain information on how to clear your record and to declare your innocence. You will likely be asked for identifying information like fingerprints, photograph, and identifying documents. Ask the law enforcement agency or prosecutor if they can issue a "clearance letter" or "certificate of release".

To ask the Kentucky Transportation Cabinet's Division of Driver Licensing to place a flag on your driver's license (if you are a victim of identity theft or not) so no one else can get a license or ID in your name, or to check your driver history or learn how to challenge incorrect information on it, contact them at 502-564-1257, or visit their website at http://transportation.ky.gov/driver-licensing/Pages/default.aspx.

☐ Medical Identity Theft

If an identity thief gets medical treatment in your name, their medical information, like test results or illnesses, can become part of your medical, health insurance, and payment records. Review your Explanation of Benefits forms and medical bills. If you suspect an identity thief has used your medical information, contact your medical insurer, doctors, pharmacies, labs, or other health care providers to report it, get a copy of your medical records, and ask about correcting your records.

If a provider denies your request, you have a right to appeal. Contact the person listed in the provider's Notice of Privacy Practices and explain the situation. If the provider still refuses to provide your records within 30 days of your written request, you may complain to the U.S. Department of Health and Human Services' Office for Civil Rights at www.hhs.gov/ocr.

The health care provider that created the information must correct the information in your files, and should also tell anyone else with whom they shared the incorrect information. If an investigation doesn't resolve your dispute, ask that a statement of the dispute be included in your record.

☐ Child Identity Theft

Child identity theft happens when someone uses a child's personal information to commit fraud, get a job or government benefits, or obtain medical care, utilities, or loans. The child's identity may be used for many years before the crime is discovered.

A parent or guardian can check whether a minor child has a credit report if they think the child's information is at risk. To get a minor child's credit report, a parent or guardian must contact the credit reporting companies and provide proof of identity and other documents.

Equifax	Experian	TransUnion
1-800-525-6285	1-888-397-3742	1-800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

If you suspect your child is an identity theft victim, then follow the other steps in this kit to help them recover from the identity theft.

☐ Contact other 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.

- **FBI**
  If the identity theft is the result of or connected to an Internet or other online fraud, file an online complaint with the FBI's Internet Crime Complaint Center, www.ic3.gov.
- **U.S. State Department**
  You may contact the U.S. State Department to report fraudulent passports or ask about the effect of identity theft on your current passport, www.travel.state.gov.
- **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 for information.
  - Federal Deposit Insurance Corporation, 877-275-3342, www.fdic.gov.
  - Federal Reserve System, 888-851-1920, www.federalreserve.gov.
  - Office of the Comptroller of Currency, 800-613-6743, www.occ.gov.
  - National Credit Union Association, 800-755-1030, www.ncua.gov.
  - Kentucky Department of Financial Institutions, 800-223-2579, www.kfi.ky.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, or call 202-307-1391.

☐ Stay alert!

Continue to monitor your credit reports, and read your bills and financial account statements promptly and carefully. Look for changes or charges you did not make. 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 or do not expect.
- Denial of 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 Free Annual Credit Report

Federal law requires each of the major nationwide consumer reporting bureau to provide you with a free copy of your credit report, 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 at the back of this kit and mail it to the address shown on the form.

Do not contact the nationwide consumer reporting bureaus individually, because they only provide the free annual credit report through this website or form.

Protect Your Personal Information

Keep your important papers secure

- **Lock them up.** Lock your financial documents and records in a safe place at home, and lock your wallet or purse in a safe place at work. Keep your information secure from roommates or workers who come into your home.

- **Limit what you carry.** When you go out, take only the identification, credit, and debit cards you need. Leave your Social Security and Medicare cards at home or in a secure place.

- **Pick up your new checks at the bank.** When you order new checks, don't have them mailed to your home, unless you have a secure mailbox with a lock.

- **Be careful with your mail.** Take outgoing mail to post office collection boxes or the post office. Promptly remove mail that arrives in your mailbox. If you will be away from home for several days, request a vacation hold on your mail:

  - go to your local post office,
  - visit www.usps.com/holdmail, or
  - call the U.S. Postal Service at 1-800-275-8777

- **Shred sensitive documents.** Shred receipts, credit offers, credit applications, insurance forms, physician statements, checks, bank statements, expired charge cards, and similar documents before you put them in your trash.

- **Consider opting out of prescreened offers of credit** and insurance by mail. You can opt out for 5 years or permanently. To opt out for 5 years, call 1-888-567-8688 or go to www.optoutprescreen.com. The 3 nationwide credit reporting companies operate the phone number and website.

- **Protect your medical information.** Destroy the labels on prescription bottles before you throw them out.
Don't share your health plan information with anyone who offers free health services or products.

- **Exercise your curiosity**. Before you share information at your workplace, a business, your child's school, or a doctor's office, ask who will have access to your information, how it will be handled, and how it will be disposed of.

Secure your Social Security Number

- **Protect it.** Share your Social Security number, and your child's, only when necessary. Ask if you can use a different kind of identification.

- **If someone asks you to share** your Social Security number or your child's, ask:

  - why they need it
  - how it will be used
  - how they will protect it
  - what happens if you don't share the number

The decision to share is yours. A business may not provide you with a service or benefit if you don't provide your number.

- **Sometimes you must share your number**. Your employer and financial institutions need your Social Security number for wage and tax reporting purposes. A business may ask for your Social Security number so they can check your credit when you apply for a loan, rent an apartment, or sign up for utility service.

Be alert to impersonators online

- **Be sure you know who is getting your personal or financial information online.** If a company that claims to have an account with you sends email asking for personal information, don't click on links in the email. Instead, type the company name into your web browser, go to their site, and contact them through customer service. Or, call the customer service number listed on your account statement. Ask whether the company really sent a request.

Protect your computer and mobile device

- **Use anti-virus software, anti-spyware software, and a firewall.** Set your preference to update these protections often. Protect against intrusions and infections that can compromise your computer files or passwords by installing security patches for your operating system and other software programs.

- **Don't open files, click on links, or download programs sent by strangers.** Opening a file from someone you don't know could expose your system to a computer virus or spyware that captures your passwords or other information you type.

- **Safely dispose of personal information**.

  - Before you dispose of a computer, get rid of all the personal information it stores. Use a wipe utility program to overwrite the entire hard drive.

- Before you dispose of a mobile device:

  - Check your owner's manual, the service provider's website, or the device manufacturer's website for information on how to delete information permanently, and how to save or transfer information to a new device.

  - Remove the memory or subscriber identity module (SIM) card from a mobile device. Remove the phone book, lists of calls made and received, voicemails, messages sent and received, organizer folders, web search history, and photos.

Protect your data and personal information

- **Encrypt your data.** Keep your browser secure. To guard your online transactions, use encryption software that scrambles information you send over the internet. A "lock" icon on the status bar of your internet browser means your information will be safe when it's transmitted. Look for the lock before you send personal or financial information online.

- **Be wise about Wi-Fi.** Before you send personal information over your laptop or smartphone on a public wireless network in a coffee shop, library, airport, hotel, or other public place, see if your information will be protected. If you use an encrypted website, it protects only the information you send to and from that site. If you use a secure wireless network, all the information you send on that network is protected.

- **Keep passwords private.** Use strong passwords with your laptop, credit, bank and other accounts. The longer the password, the harder it is to crack. Create passwords that mix letters, numbers, and special characters. Don't use the same password for many accounts. If it's stolen from you – or from one of the companies with which you do business – it can be used to take over all your accounts.

- **Don't overshare on social networking sites.** If you post too much information about yourself, an identity thief can find information about your life, use it to answer 'challenge' questions on your accounts, and get access to your money and personal information. Consider limiting access to your networking page to a small group of people. Never post your full name, Social Security number, address, phone number, or account numbers in publicly accessible sites.

- **Lock up your laptop**. Keep financial information on your laptop only when necessary. Don't use an automatic login feature that saves your user name and password, and always log off when you're finished. That way, if your laptop is stolen, it will be harder for a thief to get at your personal information.

- **Read privacy policies.** Yes, they can be long and complex, but they tell you how the site maintains accuracy, access, security, and control of the personal information it collects; how it uses the information, and whether it provides information to third parties. If you don't see or understand a site's privacy policy, consider doing business elsewhere.

EQUIFAX experian TransUnion

Annual Credit Report Request Form

You have the right to get a free copy of your credit file disclosure, commonly called a credit report, once every 12 months, from each of the nationwide consumer credit reporting companies - Equifax, Experian and TransUnion.

For instant access to your free credit report, visit www.annualcreditreport.com.

For more information on obtaining your free credit report, visit www.annualcreditreport.com or call 877-322-8228.

Use this form if you prefer to write to request your credit report from any, or all, of the nationwide consumer credit reporting companies. The following information is required to process your request. **Omission of any information may delay your request.**

Once complete, fold (do not staple or tape), place into a #10 envelope, affix required postage and mail to:
Annual Credit Report Request Service P.O. Box 105281 Atlanta, GA 30348-5281.

Please use a Black or Blue Pen and write your responses in PRINTED CAPITAL LETTERS without touching the sides of the boxes like the examples listed below:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z 0 1 2 3 4 5 6 7 8 9

Social Security Number: ___ - ___ - ____

Date of Birth: ___ / ___ / ____
Month / Day / Year

Fold Here ..... Fold Here

First Name _____ **M.I.** _

Last Name _____ **JR, SR, III, etc.** ___

Current Mailing Address:

House Number _____ **Street Name** _____

Apartment Number / Private Mailbox _____ **For Puerto Rico Only: Print Urbanization Name** _____

City _____ **State** __ **ZipCode** _____

Previous Mailing Address (complete only if at current mailing address for less than two years):

House Number _____ **Street Name** _____

Fold Here ..... Fold Here

Apartment Number / Private Mailbox _____ **For Puerto Rico Only: Print Urbanization Name** _____

City _____ **State** __ **ZipCode** _____

Shade Circle Like This → ●

Not Like This → ⊗ ✓

I want a credit report from (shade each that you would like to receive):

- ◯ **Equifax**
- ◯ **Experian**
- ◯ **TransUnion**

◯ **Shade here if, for security reasons, you want your credit report to include no more than the last four digits of your Social Security Number.**

31238

If additional information is needed to process your request, the consumer credit reporting company will contact you by mail.

Your request will be processed within 15 days of receipt and then mailed to you.

Average time to complete: 10 minutes

(From FTC's "Taking Charge – What To Do If Your Identity Is Stolen", http://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf)

Identity Theft Victim's Complaint and Affidavit

A voluntary form for filing a report with law enforcement, and disputes with credit reporting agencies and creditors about identity theft-related problems. Visit ftc.gov/idtheft to use a secure online version that you can print for your records.

Before completing this form:
1. Place a fraud alert on your credit reports, and review the reports for signs of fraud.
2. Close the accounts that you know, or believe, have been tampered with or opened fraudulently.

About You (the victim)

Now

(1) My full legal name: _____
First Middle Last Suffix

(2) My date of birth: _____
mm/dd/yyyy

(3) My Social Security number: _____-_____-_____

(4) My driver's license: _____ _____
State Number

(5) My current street address:

_____
Number & Street Name Apartment, Suite, etc.

_____
City State Zip Code Country

(6) I have lived at this address since _____
mm/yyyy

(7) My daytime phone: (_____)_____
My evening phone: (_____)_____
My email: _____

Leave (3) blank until you provide this form to someone with a legitimate business need, like when you are filing your report at the police station or sending the form to a credit reporting agency to correct your credit report.

At the Time of the Fraud

(8) My full legal name was: _____
First Middle Last Suffix

(9) My address was: _____
Number & Street Name Apartment, Suite, etc.

_____
City State Zip Code Country

(10) My daytime phone: (_____)_____ My evening phone: (____)_____
My email: _____

Skip (8) - (10) if your information has not changed since the fraud.

The Paperwork Reduction Act requires the FTC to display a valid control number (in this case, OMB control #3084-0047) before we can collect – or sponsor the collection of – your information, or require you to provide it.

About You (the victim) (Continued)

Declarations

(11) I ☐ did OR ☐ did not authorize anyone to use my name or personal information to obtain money, credit, loans, goods, or services — or for any other purpose — as described in this report.

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

(13) I ☐ am OR ☐ am not willing to work with law enforcement if charges are brought against the person(s) who committed the fraud.

(14) I believe the following person used my information or identification documents to open new accounts, use my existing accounts, or commit other fraud.

(14): Enter what you know about anyone you believe was involved (even if you don't have complete information).

Name: _____
First Middle Last Suffix

Address: _____
Number & Street Name Apartment, Suite, etc.

_____
City State Zip Code Country

Phone Numbers: (____)_____ (____)_____

Additional information about this person: _____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

(15) Additional information about the crime (for example, how the identity thief gained access to your information or which documents or information were used):

(14) and (15): Attach additional sheets as needed.

_____

_____

_____

_____

_____

_____

_____

Documentation

(16) I can verify my identity with these documents:

(16): Reminder: Attach copies of your identity documents when sending this form to creditors and credit reporting agencies.

☐ A valid government-issued photo identification card (for example, my driver's license, state-issued ID card, or my passport).
If you are under 16 and don't have a photo-ID, a copy of your birth certificate or a copy of your official school record showing your enrollment and legal address is acceptable.

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

About the Information or Accounts

(17) The following personal information (like my name, address, Social Security number, or date of birth) in my credit report is inaccurate as a result of this identity theft:

(A) _____

(B) _____

(C) _____

(18) Credit inquiries from these companies appear on my credit report as a result of this identity theft:

Company Name: _____

Company Name: _____

Company Name: _____

(19) Below are details about the different frauds committed using my personal information.

Name of Institution | Contact Person | Phone | Extension

Account Number | Routing Number | Affected Check Number(s)

Account Type: ☐ Credit ☐ Bank ☐ Phone/Utilities ☐ Loan
☐ Government Benefits ☐ Internet or Email ☐ Other

Select ONE:
☐ This account was opened fraudulently.
☐ This was an existing account that someone tampered with.

Date Opened or Misused (mm/yyyy) | Date Discovered (mm/yyyy) | Total Amount Obtained ($)

Name of Institution | Contact Person | Phone | Extension

Account Number | Routing Number | Affected Check Number(s)

Account Type: ☐ Credit ☐ Bank ☐ Phone/Utilities ☐ Loan
☐ Government Benefits ☐ Internet or Email ☐ Other

Select ONE:
☐ This account was opened fraudulently.
☐ This was an existing account that someone tampered with.

Date Opened or Misused (mm/yyyy) | Date Discovered (mm/yyyy) | Total Amount Obtained ($)

Name of Institution | Contact Person | Phone | Extension

Account Number | Routing Number | Affected Check Number(s)

Account Type: ☐ Credit ☐ Bank ☐ Phone/Utilities ☐ Loan
☐ Government Benefits ☐ Internet or Email ☐ Other

Select ONE:
☐ This account was opened fraudulently.
☐ This was an existing account that someone tampered with.

Date Opened or Misused (mm/yyyy) | Date Discovered (mm/yyyy) | Total Amount Obtained ($)

(19):
If there were more than three frauds, copy this page blank, and attach as many additional copies as necessary.

Enter any applicable information that you have, even if it is incomplete or an estimate.

If the thief committed two types of fraud at one company, list the company twice, giving the information about the two frauds separately.

Contact Person: Someone you dealt with, whom an investigator can call about this fraud.

Account Number: The number of the credit or debit card, bank account, loan, or other account that was misused.

Dates: Indicate when the thief began to misuse your information and when you discovered the problem.

Amount Obtained: For instance, the total amount purchased with the card or withdrawn from the account.

Your Law Enforcement Report

(20) One way to get a credit reporting agency to quickly block identity theft-related information from appearing on your credit report is to submit a detailed law enforcement report ("Identity Theft Report"). You can obtain an Identity Theft Report by taking this form to your local law enforcement office, along with your supporting documentation. Ask an officer to witness your signature and complete the rest of the information in this section. It's important to get your report number, whether or not you are able to file in person or get a copy of the official law enforcement report. Attach a copy of any confirmation letter or official law enforcement report you receive when sending this form to credit reporting agencies.

Select ONE:

- ☐ I have not filed a law enforcement report.
- ☐ I was unable to file any law enforcement report.
- ☐ I filed an automated report with the law enforcement agency listed below.
- ☐ I filed my report in person with the law enforcement officer and agency listed below.

(20):
Check "I have not..." if you have not yet filed a report with law enforcement or you have chosen not to. Check "I was unable..." if you tried to file a report but law enforcement refused to take it.

Automated report: A law enforcement report filed through an automated system, for example, by telephone, mail, or the Internet, instead of a face-to-face interview with a law enforcement officer.

_____
Law Enforcement Department State

_____ _____
Report Number Filing Date (mm/dd/yyyy)

_____
Officer's Name (please print) Officer's Signature

_____ (____) _____
Badge Number Phone Number

Did the victim receive a copy of the report from the law enforcement officer? ☐ Yes OR ☐ No

Victim's FTC complaint number (if available): _____

Signature

As applicable, sign and date IN THE PRESENCE OF a law enforcement officer, a notary, or a witness.

(21) I certify that, to the best of my knowledge and belief, all of the information on and attached to this complaint is true, correct, and complete and made in good faith. I understand that this complaint 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 violate federal, state, or local criminal statutes, and may result in a fine, imprisonment, or both.

_____ _____

Signature Date Signed (mm/dd/yyyy)

Your Affidavit

(22) If you do not choose to file a report with law enforcement, you may use this form as an Identity Theft Affidavit to prove to each of the companies where the thief misused your information that you are not responsible for the fraud. While many companies accept this affidavit, others require that you submit different forms. Check with each company to see if it accepts this form. You should also check to see if it requires notarization. If so, sign in the presence of a notary. If it does not, please have one witness (non-relative) sign that you completed and signed this Affidavit.

_____

Notary

Witness:

_____ _____

Signature Printed Name

_____ _____

Date Telephone Number

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
Office of Consumer Protection
1024 Capital Center Drive, Suite 200
Frankfort, Kentucky 40601

502-696-5389
Identity Theft Hotline: 800-804-7556
www.ag.ky.gov