Identity Theft
Resource Guide

Missouri Attorney General
JOSH HAWLEY

Table of Contents

Introduction

One of the fastest growing crimes in the United States is identity theft. Identity theft is a form of taking, accessing, or using someone's personal information such as their name, social security number, account number, or payment card number, without their permission, pretending to be someone else by assuming another's identity, or creating a fake identity or account.

This identity theft resource guide provides you with detailed information to help you prevent the theft of your identity and outlines the action you should take to repair damage caused by identity theft. I urge you to study the information and share it with family and friends. It can greatly reduce your risk of becoming a victim.

My office will continue to work to safeguard Missourians from identity theft. If you have questions or comments, please do not hesitate to contact us at www.ago.mo.gov or 800-392-8222.

Respectfully,

Joshua D. Hawley
Attorney General

Types of Identity Theft

Identity theft is when someone wrongfully obtains and uses your private identifying information, usually for financial gain. Identity thieves are resourceful: they rummage through your garbage, the trash of businesses, or public dumps. They may work — or pretend to work — for legitimate companies, medical offices, clinics, pharmacies, or government agencies, or convince you to reveal personal information. Some thieves pretend to represent an institution you trust, and try to trick you into revealing personal information by email or phone. Once identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance. An identity thief can file a tax refund in your name and get your refund. In some extreme cases, a thief might even give your name to the police during an arrest.

There are several types of identity theft:

1. Financial Identity Theft

- Financial identity theft occurs when someone uses another's identity to obtain money, credit, goods, or services.
- Someone may actually steal your credit card or debit card, or they may steal your credit card number or bank account number to access your money.

2. Tax Fraud Identity Theft

- Tax fraud occurs when an identity thief uses a taxpayer's stolen identity to file a fraudulent return and claim the identity theft victim's tax refund. The identity thief will use a stolen Social Security number and consumer information to file a forged tax return early in the filing season before the victim does. The scammer then receives the victim's refund before the IRS processes the real filing. To help prevent tax fraud, file your tax returns early and, if you have someone help you with your return, use a reputable tax return preparation company.
- You may be notified when you file your state or federal tax return that a return has already been filed in your name.
- If you receive mail from the Missouri Department of Revenue or the federal Internal Revenue Service and you do not understand it, call our Office at 800-392-8222.

3. Medical Identity Theft

- Medical identity theft occurs when someone uses another's identity to obtain medical care or drugs.
- You may receive an invoice or a collection notice for services you did not obtain.
- Contact the provider of the service and explain it was not you in order to dispute the charge and to correct any inaccuracies in your medical history.

4. Insurance Identity Theft

- Insurance identity theft occurs when someone uses your information to obtain insurance coverage or benefits or to obtain health care services and products. Auto insurance, personal property insurance, and health insurance are all subject to abuse.
- As an example, someone might open an insurance policy using your identification information.
- It is often intertwined with medical identity theft or financial identity theft.
- If someone is using your information, you might be subject to higher premiums or even become unable to obtain insurance for you and your family.

5. Synthetic Identity Theft

- Synthetic identity theft occurs when someone uses various data elements of others in order to create a synthetic, or fake, person.
- When the credit files of unrelated consumers become mixed so that the credit file contains data which should be attributed to one person and not the other, it can be considered "synthetic" identity theft.
- Your credit report may show loans or lines of credit that do not belong to you, and if delinquent, it may negatively impact your ability to get credit or more favorable rates.

6. Driver's License Identity Theft

- Driver's license identity theft occurs when someone obtains a driver's license using your personal information.
- You may lose your license or be unable to renew it if the thief has obtained a license using your information.
- The thief may accumulate traffic violations which will appear on your driving record.
- If you are a victim, obtain a copy of your driving record from your state's Department of Motor Vehicles and correct any errors.
- File a fraud report with the DMV enforcement office in the state you live in and report the bad record to local law enforcement.

7. Criminal Identity Theft

- Criminal identity theft occurs when someone poses as another person when being investigated or apprehended for a crime.
- An imposter may give another person's name and personal information such as a driver's license, date of birth, or Social Security number (SSN) to a law enforcement officer, often that of a friend or relative.
- A warrant may be wrongly issued for your arrest or you may be wrongly accused of a crime. You could be denied a passport or a job.

8. Social Security Identity Theft

- Social Security identity theft occurs when someone uses your Social Security Number (SSN) to start a
  new life.
- There can be as many as 20 different users of one SSN.
- Fill out the Social Security Administration's online complaint form or call them at 1-800-269-0271 to report the activity.

9. Child Identity Theft

- Child identity theft occurs when the child's Social Security number is used to apply for government benefits, open bank and credit card accounts, apply for a loan or utility service, or rent a place to live.
- Request your child's credit report to see if your child's information is being misused.
- With more and more minors online, either playing games or on social networking sites, be sure to talk to your kids about being safe online.

Checklist to Help Prevent Identity Theft

HELP PREVENT ALL TYPES OF IDENTITY THEFT

1. Use a paper shredder to destroy financial documents or other documents with personal information, including receipts, credit applications, and bank statements.

2. Don't carry your Social Security card with you or write it on a check. Place the card in a safe place, and only give your number out when absolutely necessary. Consider asking to use another identifier for accounts.

3. Don't share personal information with anyone you don't trust. Before sharing it with businesses or at the workplace, ask why they need it, how they will safeguard it, and the consequences of not sharing. If you aren't comfortable with their answer, take your business elsewhere.

4. Don't over-share on social networking sites. If you post too much information about your life, identity thieves can piece together enough information to answer "challenge" questions on your accounts, and possibly access your bank accounts or even construct a false identity that mirrors your life. Consider limiting access to your networking page to only a small group of people. Never post information that could identify you, like your Social Security number or even your full name, on websites that the public can access. Don't post the year of your birth if you decide to post your birthday.

5. Change your passwords every 60 days and make them "strong" (more difficult to "crack") by using a combination of upper case, lower case, numbers, and symbols. Avoid using your birth date, mother's maiden name, last four digits of your Social Security number, family names, or other obvious identifying words or numbers.

6. Order a free copy of your credit report from each of the three credit bureaus each year: Experian, Transunion, and Equifax. It contains information about what credit accounts have been opened in your name, as well as where you live and work, how you pay your bills, if you've been sued, arrested, or filed for bankruptcy. You are entitled to one free report each year from each of the three major bureaus, for a total of three free credit reports. Consider spreading these three reports out over the year so that you can review an up-to-date, free credit report once every few months.

7. Watch your billing cycles closely. If a bill is late, check with your creditors to see why it has not arrived, and watch for any unauthorized charges or unexpected account statements.

8. Have your mail sent to a post office box or get a locking mailbox. Also take outgoing mail to the post office. When you travel, have a trusted friend pick up your mail.

9. Only use a secure connection on the Internet when sending credit card numbers or other personal information. The website should begin with "https" instead of just "http," because the "s" means "secure."

10. Use virus protection and a firewall program to prevent your computer from being accessed by others, and keep them up to date. Run your virus scan on a regular basis. Don't download

files or click on links from unknown sources. Instead, type in a web address you know. Also, unplug or close your Internet connection when you're not using it.

11. Keep your personal information in a secure place at home, especially if you have roommates, and employ only trusted outside help if you are having work done at your home.

12. Opt out of pre-approved credit card offers and receive fewer solicitations at home by calling 888-567-8688 or visiting www.optoutprescreen.com.

13. Destroy the labels on prescription bottles before you throw them away. Don't share your health plan information with anyone offering free health services or products.

14. Stay on the lookout for suspicious behavior and occurrences, such as unusual email or impersonators asking for your personal information. If you're not absolutely certain you're speaking with a real employee, do not give out any of your personal information. Instead, hang up and call them directly. These concepts also apply to email. Do not be tricked into sending personal information to a fake business or someone you do not know. Companies you do business with will not ask you for personal information by email. Do not open email from people or companies that you do not recognize.

15. Password protect your cell phone and other devices. It's easy to lose your cell phone. And if a criminal gets it, your cell phone provides an easy way to commit identity theft with the apps and other information it stores.

16. Before you sell or dispose of a computer or mobile device, get rid of all the personal information it stores.For computers, use a wipe utility program to overwrite the entire hard drive. For mobile devices, 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.

17. Read any notices that are sent to you by mail that describe the way your data might have been exposed in a data breach. If you need help understanding the letter or want to confirm that the data is real, you can contact our Office at www.ago.mo.gov or 800-392-8222.

18. Beware of imposter websites and emails that look similar to real sites. If a site or email has poor grammer, typos, or logos that are not quite right, it could be an imposter site or spoof email. Again, be cautious when clicking on links because these could be attempts to trick you.

EXTRA STEPS TO HELP PREVENT MEDICAL IDENTITY THEFT

19. Make sure you've taken all steps above to "Help prevent all types of identity theft."

20. Remember that your medical and insurance information are very valuable to identity thieves, so do not hand it out unnecessarily.

21. Don't share medical or insurance information by phone or email unless you initiated the contact and know who you're dealing with.

22. Be suspicious of people offering "free" health services or products, especially if they ask you to provide your health plan ID number or other insurance information. Medical identity thieves may pretend to work for an insurance company, doctor's office, clinic, or pharmacy to try to trick you into revealing your personal information.

23. Keep paper and electronic copies of your medical and health insurance records in a safe place. Shred outdated health insurance forms, medical statements, receipts, and the labels from prescription bottles before you throw them out.

EXTRA STEPS TO HELP PREVENT TAX FRAUD IDENTITY THEFT

24. Make sure you've taken all steps above to "Help prevent all types of identity theft."

25. File your tax returns as early as possible.

26. Request a Personal Identification Number, or PIN, from the IRS. This can help prevent scammers from filing a federal return in your name. Other PIN numbers help consumers make secure payments on amounts owed to the IRS.

27. Consumers with questions about whether a contact from the IRS is authentic should call the IRS toll-free number (1-800-829-1040) to confirm.

28. Keep copies of all your tax records in a secure location.

29. Check your credit reports and other records for accuracy. Check your banking records daily or weekly.

30. Report the improper use of your Social Security number to the Social Security Administration at their fraud hotline (1-800-269-0271).

Checklist If You Think You're a Victim of Identity Theft

STEPS TO TAKE IF YOU THINK YOU'RE A VICTIM OF ANY TYPE OF IDENTITY THEFT

1. Order a copy of your credit report from one or more of the three credit bureaus. Check for credit accounts that you didn't open, debts you didn't know about, inquiries from companies you don't know, or any other incorrect or suspicious information.
2. Dispute any fraudulent charges or accounts.
    - Sample dispute letter for existing accounts [See Appendix C]
    - Sample dispute letter for new accounts [See Appendix C]
    - Sample Request for Fraudulent Transaction/Account Information [See Appendix C]
3. Place a fraud alert on your credit report with all three of the credit reporting agencies, which tells creditors to follow certain procedures before they can open new accounts in your name or make changes to existing accounts (calling and alerting one bureau will place an alert to all three).
4. Close any accounts that you think have been tampered with or opened fraudulently. If you will continue to use an account, make sure that you are using a new account number.
5. Change all of your passwords, especially if you use the same passwords on multiple websites. When creating new passwords, use a different password for each website, and use passwords that are hard to guess. Be sure that your passwords have a combination of letters, numbers, and special symbols.
6. Call the security or fraud departments of each company where an account was fraudulently opened or changed without your permission; follow up in writing with documents that support your claim.
7. Complete a Victim's Complaint and Affidavit form. [See Appendix A]
8. Keep a log of all your actions, including all telephone calls, letters, other documents, and deadlines that you encounter. Save copies of all letters and other documents. This information may become extremely important for resolving the issue.
    - Credit Bureau and Law Enforcement Worksheet [See Appendix B]
    - Account Statement and Activity Worksheet [See Appendix B]
9. Block any fraudulent information from your credit report. Sample letter to block info [See Appendix C]
10. If you need to fix specific identity theft problems, like stolen checks or passports, phone fraud, tax fraud, falsified change of address, or other problems, see the Attorney General's recommendations and important contact information on page 30 (Appendix F).

11. If you've become a victim of identity theft, file a police report with your local police or sheriff's department.

12. File a complaint with the Attorney General's Office at www.ago.mo.gov.

EXTRA STEPS TO TAKE IF YOU THINK YOU'RE A VICTIM OF MEDICAL IDENTITY THEFT

13. Contact information and other details are available in Appendix F.

14. Obtain copies of your medical bills from your providers to see if there are any services, visits, or prescriptions that do not belong to you. If you identify any you did not request or obtain, ask for a copy of the records pertaining to that visit or procedure. You have a right, under federal law, to know what's in your medical records. Check to see if there are any errors.

15. Get an "accounting of disclosures" by asking each of your health plans and medical providers for a copy of the account of disclosures for your medical records. This will tell you who has received copies of your records. You can receive one free copy from each medical provider every 12 months.

16. Ask that any errors be corrected. Tell your provider if there is any incorrect information, and explain what is incorrect. If you have documents that support your explanation, send copies. Be sure to keep the original copies of everything for yourself, though. If they won't correct your records, ask that they include in your record a statement of your dispute.

17. The Federal Trade Commission website (www.ftc.gov) offers additional resources for dealing with medical identity theft.

EXTRA STEPS TO TAKE IF YOU THINK YOU'RE A VICTIM OF TAX FRAUD IDENTITY THEFT

18. Make sure you've taken steps "1 through 12" above if you think you're a victim of any type of identity theft.

19. Report it to the Internal Revenue Service at 800-908-4490. Consumers will need to complete the form 14039 (www.irs.gov/pub/irs-pdf/f14039.pdf) and return it to the IRS.

20. Missourians should also report the fraud to the Missouri Department of Revenue at 573-751-3505 or by email to idtheft@dor.mo.gov.

21. The Missouri Attorney General's Consumer Protection Hotline is available to assist consumers in reporting identity theft. Missourians can reach the hotline at 800-392-8222 or file a complaint form (www.ago.mo.gov/divisions/consumer/identity-theft-data-security/identity-theft-complaint-form).

CREDIT MONITORING SERVICE

There are a variety of commercial services that, for a fee, will monitor your credit reports for activity and alert you to changes to your accounts. Prices and services vary widely. Many of the services only monitor one of the three major consumer reporting companies. If you're considering signing up for a service, make sure you understand what you're getting before you buy. Also check out the company with the Better Business Bureau and the Consumer Protection Division of the Attorney General's Office to see if any complaints are on file at www.ago.mo.gov.

If you receive a data breach notice, you may be offered free credit monitoring. Details will be in your notice letter.

Appendix A

IDENTITY THEFT VICTIM'S COMPLAINT AND AFFIDAVIT

- Tear out the following Identity Theft Victim's Complaint and Affidavit or fill it out online at www.ftc.gov/idtheft.

- Mail a copy of this form and documents to our Office at P.O. Box 899 Jefferson City, MO 65102 or email to consumer.help@ago.mo.gov.

- Provide copies of this form and documents to: FTC, police department, credit bureaus, and attach to letters disputing fraudulent charges or acts.

- Keep a copy for your records.

Average time to complete: 10 minutes

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.

About 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

Appendix B

Tear out and fill in the following worksheets to keep as a record of actions you've taken.

CREDIT BUREAU & LAW ENFORCEMENT WORKSHEET

Place a fraud alert on your credit file and request a copy of your credit report. Report criminal activity to the appropriate authorities and agencies.

Organization	Report/Reference #	Date Contacted	Contact Name	Notes
Equifax 1-800-525-6285 www.equifax.com				
Experian 1-888-397-3742 www.experian.com				
TransUnion 800-680-7289 www.transunion.com				
Federal Trade Comm. 877-ID-THEFT www.consumer.gov				
Local Police Dept.				
Missouri Attorney General's Office 800-392-8222 www.ago.mo.gov				
Social Security Fraud Hotline 800-269-0271				
Postal Inspection Service www.usps.com				

ACCOUNT STATEMENT & ACTIVITY WORKSHEET

Track when your statements arrive, what transactions occurred and the statement balance. Verify that the account activity is legitimate.

Issuer	Account Type	Date Received	Statement Balance	Suspicious Transactions	Notes

Appendix C

SAMPLE DISPUTE LETTER FOR EXISTING ACCOUNTS

[Date]

[Your Name]
[Your Address]
[Your City, State, Zip Code]
[Your Account Number]

[Name of Creditor]
Billing Inquiries
[Address]
[City, State, Zip Code]

Dear Sir or Madam:

I am writing to dispute a fraudulent [charge/debit] on my account in the amount of $_____. I am a victim of identity theft, and I did not make this [charge/debit]. I am requesting that the [charge be removed/the debit reinstated], that any finance and other charges related to the fraudulent amount be credited, as well, and that I receive an accurate statement.

Enclosed is a copy of my Identity Theft Victim's Complaint supporting my position. In addition, I am enclosing a copy of sections 605B, 615(f) and 623(a)(6) of the Fair Credit Reporting Act (FCRA), which detail your responsibilities as an information furnisher to consumer reporting agencies in response to the Identity Theft Report I am providing. These enclosures also detail your responsibilities that apply in the event you receive from a consumer reporting agency notice under section 605B of the FCRA that information you provided to is the result of identity theft.

Please investigate this matter and correct the fraudulent [charge/debit] as soon as possible.

Sincerely,
[Your Name]

Enclosures:
Identity Theft Victim's Complaint and Affidavit
FCRA Sections 605B, 615(f), 623(a)(6)

SAMPLE BLOCKING LETTER TO CONSUMER REPORTING COMPANY

[Date]

[Your Name]
[Your Address]
[Your City, State, Zip Code]

(Write to one at a time:)

Equifax Information Services, LLC
P.O. Box 105169
Atlanta, GA 30348

-or-

Experian
P.O. Box 9532
Allen, TX 75013

-or-

TransUnion
Fraud Victim Assistance Department
P.O. Box 6790
Fullerton, CA 92834-6790

Dear Sir or Madam:

I am a victim of identity theft. I am writing to request that you block the following fraudulent information from my credit report: [Identify item(s) to be blocked by name of source, such as creditors or tax court, and identify type of item, such as credit account, judgment, etc].

This information does not relate to any transaction that I have made. I have enclosed a copy of my Identity Theft Victim's Complaint. In addition, I have enclosed a copy of section 605B of the Fair Credit Reporting Act, which details your responsibility to block fraudulent information on my credit report resulting from identity theft. Please let me know if you need any other information from me to block this information from my credit report.

Sincerely,
[Your Name]

Enclosures:
Identity Theft Victim's Complaint and Affidavit
FCRA Section 605B

SAMPLE DISPUTE LETTER FOR NEW ACCOUNTS

[Date]

[Your Name]
[Your Address]
[Your City, State, Zip Code]
[Your Account Number (if known)]

[Name of Creditor]
Billing Inquiries
[Address]
[City, State, Zip Code]

Dear Sir or Madam:

I am a victim of identity theft. I have recently learned that my personal information was used to open an account at your company. I did not open this account, and I am requesting that the account be closed and that I be absolved of all charges on the account.

Enclosed is a copy of my Identity Theft Victim's Complaint supporting my position. In addition, I am enclosing a copy of sections 605B, 615(f) and 623(a)(6) of the Fair Credit Reporting Act (FCRA), which detail your responsibilities as an information furnisher to consumer reporting agencies in response to the Identity Theft Report I am providing. These sections also detail your responsibilities that apply in the event you receive from a consumer reporting agency notice under section 605B of the FCRA that information you provided is the result of identity theft.

Please investigate this matter, close the account and absolve me of all charges, take the steps required of you under the FCRA, and send me a letter confirming your findings and actions, as soon as possible.

Sincerely,
[Your Name]

Enclosures:
Identity Theft Victim's Complaint and Affidavit
FCRA Sections 605B, 615(f), 623(a)(6)

Appendix D

ENCLOSURE: FCRA 605B (15 U.S.C. § 1681c-2)

Block of Information Resulting from Identity Theft

(a) Block

Except as otherwise provided in this section, a consumer reporting agency shall block the reporting of any information in the file of a consumer that the consumer identifies as information that resulted from an alleged identity theft, not later than 4 business days after the date of receipt by such agency of--

(1) appropriate proof of the identity of the consumer;

(2) a copy of an identity theft report;

(3) the identification of such information by the consumer; and

(4) a statement by the consumer that the information is not information relating to any transaction by the consumer.

(b) Notification

A consumer reporting agency shall promptly notify the furnisher of information identified by the consumer under subsection (a) of this section--

(1) that the information may be a result of identity theft;

(2) that an identity theft report has been filed;

(3) that a block has been requested under this section; and

(4) of the effective dates of the block.

(c) Authority to decline or rescind

(1) In general

A consumer reporting agency may decline to block, or may rescind any block, of information relating to a consumer under this section, if the consumer reporting agency reasonably determines that--

(A) the information was blocked in error or a block was requested by the consumer in error;

(B) the information was blocked, or a block was requested by the consumer, on the basis of a material misrepresentation of fact by the consumer relevant to the request to block; or

(C) the consumer obtained possession of goods, services, or money as a result of the blocked transaction or transactions.

(2) Notification to consumer

If a block of information is declined or rescinded under this subsection, the affected consumer shall be notified promptly, in the same manner as consumers are notified of the reinsertion of information under section 1681i(a)(5)(B) of this title.

(3) Significance of block

For purposes of this subsection, if a consumer reporting agency rescinds a block, the presence of information in the file of a consumer prior to the blocking of such information is not evidence of whether the consumer knew or should have known that the consumer obtained possession of any goods, services, or money as a result of the block.

(d) Exception for resellers

(1) No reseller file

This section shall not apply to a consumer reporting agency, if the consumer reporting agency--

(A) is a reseller;

(B) is not, at the time of the request of the consumer under subsection (a) of this section, otherwise furnishing or reselling a consumer report concerning the information identified by the consumer; and

(C) informs the consumer, by any means, that the consumer may report the identity theft to the Commission to obtain consumer information regarding identity theft.

(2) Reseller with file

The sole obligation of the consumer reporting agency under this section, with regard to any request of a consumer under this section, shall be to block the consumer report maintained by the consumer reporting agency from any subsequent use, if--

(A) the consumer, in accordance with the provisions of subsection (a) of this section, identifies, to a consumer reporting agency, information in the file of the consumer that resulted from identity theft; and

(B) the consumer reporting agency is a reseller of the identified information.

(3) Notice

In carrying out its obligation under paragraph (2), the reseller shall promptly provide a notice to the consumer of the decision to block the file. Such notice shall contain the name, address, and telephone number of each consumer reporting agency from which the consumer information was obtained for resale.

(e) Exception for verification companies

The provisions of this section do not apply to a check services company, acting as such, which issues authorizations for the purpose of approving or processing negotiable instruments, electronic fund transfers, or similar methods of payments, except that, beginning 4 business days after receipt of information described in paragraphs (1) through (3) of subsection (a) of this section, a check services company shall not report to a national consumer reporting agency described in section 1681a(p) of this title, any information identified in the subject identity theft report as resulting from identity theft.

(f) Access to blocked information by law enforcement agencies

No provision of this section shall be construed as requiring a consumer reporting agency to prevent a Federal, State, or local law enforcement agency from accessing blocked information in a consumer file to which the agency could otherwise obtain access under this subchapter.

ENCLOSURE: FCRA 615(f) (15 U.S.C. § 1681m(f))

Requirements on Users of Consumer Reports – Prohibition on Sale or Transfer of Debt Caused by Identity Theft

(f) Prohibition on sale or transfer of debt caused by identity theft

(1) In general

No person shall sell, transfer for consideration, or place for collection a debt that such person has been notified under section 1681c-2 of this title has resulted from identity theft.

(2) Applicability

The prohibitions of this subsection shall apply to all persons collecting a debt described in paragraph (1) after the date of a notification under paragraph (1).

(3) Rule of construction

Nothing in this subsection shall be construed to prohibit--

(A) the repurchase of a debt in any case in which the assignee of the debt requires such repurchase because the debt has resulted from identity theft;

(B) the securitization of a debt or the pledging of a portfolio of debt as collateral in connection with a borrowing; or

(C) the transfer of debt as a result of a merger, acquisition, purchase and assumption transaction, or transfer of substantially all of the assets of an entity.

ENCLOSURE: FCRA 623(a)(6) (15 U.S.C. § 1681s-2(a)(6))

Responsibilities of Furnishers of Information to Consumer Reporting Agencies – Duties of Furnishers upon Notice of Identity Theft-Related Information

(6) Duties of furnishers upon notice of identity theft-related information

(A) Reasonable procedures

A person that furnishes information to any consumer reporting agency shall have in place reasonable procedures to respond to any notification that it receives from a consumer reporting agency under section 1681c-2 of this title relating to information resulting from identity theft, to prevent that person from refurnishing such blocked information.

(B) Information alleged to result from identity theft

If a consumer submits an identity theft report to a person who furnishes information to a consumer reporting agency at the address specified by that person for receiving such reports stating that information maintained by such person that purports to relate to the consumer resulted from identity theft, the person may not furnish such information that purports to relate to the consumer to any consumer reporting agency, unless the person subsequently knows or is informed by the consumer that the information is correct.

Appendix E

CREDIT REPORTING

There are three major credit reporting companies: Equifax, Experian, and TransUnion. These companies collect and report your data to potential creditors, employers, insurers, and to others for purposes allowed by law.

FREE ANNUAL CREDIT REPORTS

Each of the major nationwide consumer reporting companies are required by the federal Fair Credit Reporting Act to provide you with a free copy of your credit report, at your request, once every 12 months. Consider spreading these three reports out over the year so that you can review an up-to-date, free credit report once every few months. To obtain a free copy of your report:

- Visit www.annualcreditreport.com,
- Call toll-free 877-322-8228, or
- Complete the Annual Credit Report Request Form at www.ftc.gov/credit and mail it to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

You are also 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. You are also entitled to one free report a year if you are 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 around $10.00 for any other copies of your report.

To buy a copy of your report, or to request a fraud alert or security freeze, contact one of the three credit bureaus:

CREDIT BUREAUS		
EQUIFAX P.O. Box 740241 Atlanta, GA 30374 888-766-0008	EXPERIAN P.O. Box 9532 Allen, TX 75013 888-EXPERIAN (397-3742)	TRANSUNION P.O. Box 6790 Fullerton, CA 92834 800-680-7289

Fraud Alert: You can add a fraud alert message to your credit report to help protect your credit information. Fraud alert messages notify potential creditors to verify your identification before extending credit in your name in case someone is using your information without your consent.

Security Freeze: You can initiate a security freeze on your credit report to prevent a credit reporting company from releasing your credit report without your consent. Be aware that a security freeze limiting access to the personal and financial information in your file may delay, interfere with, or prohibit the timely approval of any subsequent request or application you

make regarding a new loan, credit, mortgage, insurance, government services or payments, rental housing, employment, investment, license, cellular telephone, utilities, digital signature, Internet credit card transaction, or other services. Many experts recommend that you place a freeze if you have been a victim of identity theft, or if you have received a data breach notice. If you place a freeze, call to have the freeze lifted before applying for credit. Some charges may apply when lifting the freeze. Additionally, credit reporting agencies may charge you both for initiating the security freeze and for removing the security freeze. The fee is waived if a police report has been filed.

Appendix F

ADDITIONAL CONTACT INFORMATION AND OTHER RESOURCES

Stolen Checks
If an identity thief steals your checks or counterfeits checks from your existing bank account, contact your bank to have them put "stop-payment-orders" on your checks, and close your account.

- Contact major check verification companies to request that they notify retailers who use their databases not to accept your checks:
  - TeleCheck at 1-800-710-9898 or 1-800-927-0188, and
  - Certegy, Inc. (previously Equifax Check Systems) at 1-800-437-5120.
- To find out if the identity thief has been passing bad checks in your name, call SCAN at 1-800-262-7771.

Stolen Passport
If you believe your passport is lost, stolen, or is being used fraudulently, contact the United States Department of State (USDS).

- Report your lost or stolen passport by calling 1-877-487-2778 (TTY: 1-888-874-7793).
- Complete the form at www.travel.state.gov/passport/lost/lost_848.html regarding a lost or stolen passport and submit it to: U.S. Department of State Passport Services, Consular Lost/ Stolen Passport Section, 1111 19th Street, NW, Suite 500, Washington, DC 20036.

Fraudulent Use of Social Security Number (SSN)
To report fraudulent use of a Social Security number, contact the Social Security Administration (SSA) Office of the Inspector General.

- File a complaint with SSA online at www.socialsecurity.gov/oig, call: 1-800-269-0271, fax: 410-597-0118, or write: SSA Fraud Hotline, P.O. Box 17768, Baltimore, MD 21235.
- Request a replacement Social Security number card if yours is lost or stolen, or verify the accuracy of reported earnings, by calling 1-800-772-1213.

Falsified Change of Address
If an identity thief has stolen your mail, has falsified change-of-address forms, or otherwise obtained your personal information via mail fraud, contact your local postal inspector.

- Contact the U.S. Postal Inspection Service (USPIS) district office nearest you by calling your local post office.
- File a complaint with the USPIS online at https://postalinspectors.uspis.gov/.

Tax Fraud
If you believe an identity thief has used your information to commit tax fraud, contact the Internal Revenue Service (IRS).

- Contact the IRS by calling 1-800-829-1040 or visit www.irs.gov.
- Contact Missouri Department of Revenue at 573-751-3505, email idtheft@dor.mo.gov, or by mail to Missouri Department of Revenue Attn: Identity Theft P.O. Box 3366, Jefferson City, MO 65105-3366.

Bankruptcy Fraud
If you believe someone has filed for bankruptcy in your name, report suspected bankruptcy fraud to the U.S. Department of Justice's Trustee Program.

- Prepare a written summary containing the information specified at www.justice.gov/ust/eo/fraud/index.htm and send this information via email to: USTP.Bankruptcy.Fraud@usdoj.gov or by mail to: Executive Office for U.S. Trustees Criminal Enforcement Unit, 20 Massachusetts Ave., NW Ste. 8000, Washington, DC 20530.

Phone Fraud
If an identity thief has established phone service in your name, is making unauthorized calls that are billed to your cellular phone, or is using your calling card and PIN, contact your service provider immediately to cancel the account and/or calling card.

- If you have problems removing the fraudulent phone charges from your account or closing an unauthorized account, contact the Missouri Public Service Commission by calling: 1-800-392-4211. You can file a complaint online at www.psc.mo.gov or by mail to Governor Office Building, 200 Madison Street, P.O. Box 360, Jefferson City, MO 65102-0360.
- For cellular phones and long distance, contact the Federal Communications Commission (FCC) by calling 1-888-CALL-FCC (TTY: 1-888-TELL-FCC).
- File a complaint with the FCC online at www.fcc.gov; write: Federal Communications Commission, Consumer Information Bureau, 445 12th Street, SW, Room 5A863, Washington, DC 20554 or e-mail fccinfo@fcc.gov.

Student Loan Fraud
If an identity thief has used your information to take out a student loan, contact the school or program that opened the student loan to close the loan.

- Report the fraudulent loan to the U.S. Department of Education Inspector General's Hotline by calling 1-800-MIS-USED.
- File a complaint online at www.ed.gov/about/offices/list/oig/hotline.html?src=rt or write: Office of Inspector General, U.S. Department of Education, 400 Maryland Avenue, SW, Washington, DC 20202-1510.

Investment Fraud
If you believe an identity thief has tampered with your securities investments or brokerage account, immediately report it to your broker or account manager.

- File a complaint with the U.S. Securities and Exchange Commission's Complaint Center at www.sec.gov/complaint.shtml, send a fax to 703-813-6965, or write to: SEC Complaint Center, 100 F Street NE, Washington, D.C. 20549-0213.
- Contact the Securities Division of the Missouri Secretary of State's Office, which is responsible for ensuring compliance with state securities laws, at: www.sos.mo.gov/securities/mipc/complaint.asp.

Other Identity Fraud
For other situations involving identity fraud not listed above, visit the FTC website at www.ftc.gov/bcp/edu/microsites/idtheft/.

This information was adapted from the Federal Trade Commission.

OFFICE OF ATTORNEY GENERAL
JOSH HAWLEY
P.O. Box 899
Jefferson City, MO 65102
573-751-3321
ago.mo.gov