New York
Finger Lakes
Identity Theft Coalition

Identity Theft Kit

for Victims of Identity Theft

Lifespan
take it on!

Identity Theft Kit for Victims of Identity Theft Contents

Introduction 1

Identity Theft Kit: Eight Easy Steps to Help Remedy ID Theft 4

Sample Dispute Letter for Existing Accounts 17

Sample Dispute Letter for New Accounts 19

Request for Fraudulent Transaction/Account Information 21

Sample Dispute Letter to Credit Reporting Company 26

Identity Theft Victim's Complaint and Affidavit 32

Resources and Contact Information 39

New York
Finger Lakes
Identity Theft Coalition

Identity Theft Kit
for Victims of Identity Theft

Introduction

I. FINGER LAKES ID THEFT COALITION

In October 2011, **Lifespan of Greater Rochester, New York** was selected by the **Maryland Crime Victims' Resource Center, Inc.** (**MCVRC**) as one of ten subgrantees to participate in the **National Identity Theft Victims Assistance Networks Project Grant**. The goal of this project is to expand and improve the outreach and capacity of victim service programs to better address the rights and needs of victims of identity theft nationwide. The project is funded by the **U.S. Department of Justice, Office for Victims of Crime** (**OVC**), through the Crime Victims Fund. This unique fund is financed by fines and penalties paid by convicted federal offenders, not from tax dollars.

Lifespan of Greater Rochester is a not-for-profit social agency in western New York State dedicated to helping older adults and their caregivers take on both the challenges and opportunities of longer life. Since 1971 the agency has provided programs, education and advocacy around aging issues to improve the quality of life for older adults and to help them remain independent in the community for as long as possible. The grant from the Maryland Crime Victims' Resource Center enabled Lifespan to form the Finger Lakes Identity Theft Coalition, a group of professionals from aging services, adult protective services, law enforcement, banking, criminal justice and other institutions to work together to combat identity theft. The Coalition covers eight counties in western

New York: Cayuga, Livingston, Monroe, Ontario, Schuyler, Seneca, Wayne and Yates. The purpose of the Coalition is to offer education to older adults and their caregivers about ways to prevent identity theft and to offer assistance and support to individuals who have become victims of identity theft (also known as **"ID theft"**).

Reporting ID theft to the proper authorities and correcting the damage done by ID theft criminals can be a time consuming and frustrating task. The purpose of this ID Theft Kit is to simplify the task by guiding victims, step by step, through the process they should follow to report the theft of personal information in order to minimize losses, recover lost funds when possible and repair the damage done to credit ratings.

II. ID THEFT IS THE FASTEST GROWING CRIME IN THE USA

What is ID theft? ID theft is the theft or misuse of personal identifying information in order to gain something of value or facilitate other criminal activity. Identity theft is the fastest growing financial crime in the United States. Each year ID thieves prosper from nearly ten million unknowing victims, including a significant number of older adults. Discovering that you have become a victim of ID theft can be devastating; the theft can place an undue financial hardship on victims and their families. The harm caused to victims can be extensive and long lasting. Most victims are unaware of the immediate steps that they should take to stop the victimization, and prevent further harm to their finances and credit rating.

According to the **Federal Trade Commission** (**FTC**) around 12 million or five percent of Americans over the age of 16 became victims of identity theft in the two year period ending in June 2008. Financial identity theft is only part of the overall picture. ID theft can take other forms besides fraudulent use of personal information for financial gain. Thousands of victims also experienced other types of identity theft, including criminal, medical and identity theft by family members. Identities can be stolen to avoid criminal prosecution (for example, claiming another person's identity when arrested); to obtain medical care using another person's identity and health insurance (medical ID theft) or using the identity of another person in a family to get credit cards, or to set up a utility or telephone account. Other common forms of ID theft are using another person's information for employment purposes or to claim a fraudulent tax refund from the IRS.

Identity theft can have more than just financial consequences. Many victims feel moderate to severe distress from the identity theft, according to a recent report from the Bureau of Justice Statistics. Recovering victims also spend an average of $1,870 in out-of-pocket costs. Over three

million experienced issues such as having utilities cut off, being arrested, finding erroneous claims on their health records, having child support garnished for children they never had or being harassed by collection agencies.

ID theft victims do not have to struggle with the consequences of ID theft alone. There are many resources available to help individuals know how to prevent becoming a victim and to help victims cope with the aftermath of having personal information misused or stolen. This guide is designed to be a useful resource for victims. The members of the Finger Lakes Identity Theft Coalition are also ready to assist victims in western New York to respond to incidents of ID theft. Information about available resources can be found at the end of this guide.

Identity Theft Kit:
Eight Easy Steps to Help Remedy ID Theft

The purpose of this Identity Theft Kit for Victims of Identity Theft (**the " ID Theft Kit"**) is to provide victims with a **self-help, step-by-step guide** to what ID theft victims need to do to preserve their financial security, protect themselves from further damage by ID theft and to remedy the harm (**financial, emotional, psychological, etc.**) directly caused by this terrible crime. This ID Theft Kit attempts to provide immediate assistance to victims on how to navigate through the various credit reporting agencies, creditors, federal and state bureaucracies, law enforcement and other governmental and non-governmental agencies. Last, the ID Theft Kit provides victims with a simple **"TO DO LIST" and SAMPLE TRANSMITTAL LETTERS AND FORMS.**

The ID Theft Kit will cover the **FOUR IMMEDIATE STEPS** plus the **FOUR FOLLOW-UP STEPS** that an ID Theft Victim should take in order to attempt to recover and seek full remedy from this terrible crime. The **EIGHT STEPS** are outlined as follows:

STEP 1. **Immediately place an Initial Fraud Alert on your credit reports.**

STEP 2. **Obtain a copy of your credit report from each of the three major credit reporting agencies at www.annualcreditreport.com**

STEP 3. **Contact your local Law Enforcement Agency and file a Police Report which specifically states that you are a victim of ID theft.**

STEP 4. **File with the Federal Trade Commission ("FTC") an ID THEFT COMPLAINT AND AFFIDAVIT ("FTC Complaint") at www.ftc.gov**

STEP 5: **Review copies of your credit reports to determine if there any unauthorized accounts or charges.**

STEP 6: **Block erroneous information from appearing in your credit reports.**

STEP 7: **Consider requesting an extended fraud alert or credit freeze, which is called a "Security Freeze" in New York State.**

STEP 8: **Review and monitor all your financial accounts and statements on a regular basis.**

STEP NUMBER ONE:

Place an Initial Fraud Alert with One of the Credit Reporting Agencies:

Contact ONE of the following credit reporting agencies ("CRA"):

- ➤ **EQUIFAX-1-800-525-6285, or**
- ➤ **EXPERIAN-1-888-397-3742, or**
- ➤ **TRANSUNION-1-800-680-7289**

  - **• Report that you are an Identity Theft Victim.**
  - **• Request that your credit file be placed on a 90 Day Temporary Fraud Alert ("TFA"), also called an Initial Fraud Alert.**

Contacting one CRA will automatically cause the other two CRAs to place the same TFA on your credit file. The TFA will require potential creditors and the CRAs to verify the true identity of any person who applies for a new credit account and/or seeks to purchase goods on existing accounts owned by the victim. Placing a TFA on your credit file will require creditors to verify the identity of the individual seeking credit before issuing credit in the victim's name.

- • Confirm in writing that the CRA you call will contact the other two companies to make the same request.
- • There is no charge to place a TFA on your credit files.
- • Mark your calendar. The TFA stays on your CRA for 90 days. You can renew it after 90 days. You may also request an Extended Fraud Alert, which stays on your credit report for seven (7) years.

STEP NUMBER TWO:

Order Copies of Your Credit Reports by:

TELEPHONE:

- ➤ **EQUIFAX-1-800-525-6285**
- ➤ **EXPERIAN-1-888-397-3742**
- ➤ **TRANSUNION-1-800-680-7289.**

  - **• Explain that you already requested and placed a TRA (90 day-Initial Fraud Alert) on your credit files.**
  - **• Record the date that you called the CRAs and follow up with the request in writing.**

OR BY:

INTERNET:

- ➤ Download the Request Form at: **www.AnnualCreditReport.com** and mail it to the address provided in the form.

- ➤ **Obtaining copies of your credit report is the only sure way of determining whether you have, in fact, fallen victim to ID Theft.** You can also request copies of your credit report via the Internet site listed above (free of charge) but you will have to disclose your Social Security number over the unsecured Internet. (**A copy of the CRA Mail-in Request Form is provided in this kit .**)

- ➤ **Ask each CRA to show only the last four (4) digits of you Social Security number on your credit report.**

STEP NUMBER THREE:

File and Obtain a Police Report from Victim's Local Law Enforcement Agency

- ➤ **File a police report about the identity theft, and get a copy of the police report or the report number.**

- ➤ **A police report is critical to get rid of fraudulent debts and clear up bad credit reports.**

- ➤ **REQUEST A FACE-TO-FACE MEETING WITH A LAW ENFORCEMENT OFFICER.**

  - Furnish as much documentation as you can to prove your case. Debt collection letters, credit reports, a copy of your printed ID Theft Complaint, and other evidence of fraudulent activity can help demonstrate the legitimacy of your case.

  - Be persistent if local authorities tell you that they can't take a report. Stress the importance of a police report; many creditors require one to resolve your dispute. Remind them that under federal law consumer reporting companies will automatically block the fraudulent accounts and bad debts from appearing on your credit report, but only if you can give them a copy of the police report. In addition, a police report may be needed to obtain the fraudulent application and other records the company has.

- If you can't get the local police to take a report, try your county sheriff's department. If that doesn't work, try the state police.
    - — In New York State, a law enforcement agency is required to take reports from ID theft victims. If the law enforcement agency you contact in New York refuses to take a report, refer them to:
        - NYS Executive Law: §646 – **Mandatory Police Reports for ID Theft Victims:** The law enforcement agency must take a police report of the matter and provide the complainant with a copy of the report at no charge.
- See sample Law Enforcement Report on page 31.

STEP NUMBER FOUR:

File an FTC Complaint/Affidavit with the FTC:

The FTC Complaint/Affidavit plus the Police Report Form What is Referred to as an "ID Theft Report."

Filing an ID Theft Complaint/ Affidavit (**"FTC Complaint"**) with the Federal Trade Commission (FTC) is important for several reasons. First, the information that you enter in the complaint can be used as part of the Identity Theft Report that you prepare, which is an important tool in recovering from identity theft. **The ID Theft Report is a simple but important document which consists of a copy of the FTC Complaint/ Affidavit and a copy of the Police Report.**

I. PREPARING AND FILING AN FTC COMPLAINT:

➤ When you file an FTC Complaint, you can help law enforcers catch identity thieves. Your complaint is entered into the FTC's Identity Theft Data Clearinghouse, which law enforcement officers can search as part of their criminal investigations. (The FTC, however, does not bring criminal cases.) Law enforcement officers who are members of the Clearinghouse may contact you if your case becomes part of their investigation. But it's also a good idea to stay in touch with your local police department about their investigation, or about any recent developments in your case.

A sample of the FTC Complaint is contained in this Identity Theft Kit beginning on page 32.

➤ The FTC Complaints which are received from victims are made available to other federal, state and local law enforcement officials nationwide. The printed FTC Complaint can be used in

conjunction with a police report to create an Identity Theft Report that will help you recover more quickly.

II. COMPLETING THE IDENTITY THEFT REPORT:

- The **Identity Theft Report** is a detailed report that gives enough information about the crime for the credit reporting companies and the businesses involved to verify that you've been a victim of ID theft. When you file your Identity Theft Report with the credit reporting companies or creditors, you get several important legal protections that will help you recover from ID theft. The ID Theft Report will help you deal with credit reporting companies, debt collectors, and businesses that opened accounts in your name.

- You can use the ID Theft Report to remove fraudulent information 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. It can also be used to place an Extended Fraud Alert on your credit report and to obtain information from companies about accounts the identity thief opened or misused.

- You can file a complaint with the FTC using the online ID Theft Complaint Form at www.ftc.gov; you can call the FTC's Identity Theft Hotline, toll-free: 1-877-ID-THEFT (438-4338); TTY: 1-866-653-4261; or you can write to the Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580. A printed version of your complaint is available only if you file your complaint online.

- Please do not send the FTC your printed ID Theft Complaint Form, ID Theft Affidavit, police report, credit reports, financial information, or any other documents relating to your case. The FTC does not keep these materials on file or forward them to law enforcement agencies. If a law enforcement agency decides to open an investigation of your case, they will contact you directly and let you know what documents they need.

ADDITIONAL NOTES ON THE FTC COMPLAINT/ID THEFT REPORT:

(a) If you know that your personal information has been misused, you should immediately file the FTC Complaint, and provide a copy to local law enforcement right away. The faster you act, the less chance the ID thief has to do more damage to your credit.

(b) If your personal information has been lost or otherwise compromised, you may want to file an FTC Complaint even if your information has not yet been misused. Reporting the incident

now may help if your information is misused in the future and you need to prove the date or circumstances of the compromise. Filing an FTC Complaint can also be useful when your information has been released in a data breach (that is, an intentional theft or mistaken release of personal data about customers from a bank, credit card company, health insurance company, etc.). An FTC Complaint in such cases can assist the FTC in finding out about such breaches.

STEP NUMBER FIVE:

Review Entries Contained in Your Credit Reports to Discover Any Fraudulent Activity:

I. REVIEW CREDIT REPORTS:

➤ **UPON RECEIPT OF COPIES OF YOUR CREDIT REPORTS FROM THE CRAs (EXPERIAN, EQUIFAX AND TRANSUNION), YOU SHOULD IMMEDIATELY DO THE FOLLOWING:**

- Review your credit reports to determine if there has been any unauthorized or fraudulent activity.

- Monitor and review all of your monthly credit card statements and bills. If you discover any unauthorized accounts, federal law requires the Furnisher (i.e., credit card company, a business where an ID theft made unauthorized purchases, etc.) and the credit reporting agency (CRA) to investigate and delete the erroneous account information.

II. DISPUTE ERRORS WITH CREDIT REPORTING AGENCIES (CRAs)

➤ **If you find inaccurate information when you review your credit reports, send letters (see Sample Letters beginning on page 17) explaining the errors to:**

- **Experian, Equifax and TransUnion**
- **the Fraud Department of each business that reported a fraudulent transaction on your existing accounts**
- **the Fraud Department of each business that reported a new account opened in your name by an identity thief.**

➤ **The CRA must investigate the items you report, and forward that information to the business or organization that reported the information to the credit reporting agency.**

- **If your credit file changes because of the business's investigation, the CRA must send you a letter with the results.**

- **If the credit reporting company puts the information back into your file, it must send you a letter explaining what it did.**

- **After a business gets notice from the CRA, it has 30 days to investigate and respond to the credit reporting company. If the business finds an error, it must notify the CRA so that your credit file can be corrected. If your credit file changes because of the business's investigation, the CRA must send you a letter with the results. The CRA can't add the disputed information back into your file unless the business says the information is correct. If the CRA puts the information back into your file, it must send you a letter telling you that.**

- **If the errors result from identity theft and you have an Identity Theft Report, ask the CRAs and businesses to block the disputed information from appearing on your credit reports. The CRA must block transactions and accounts if you are an identity theft victim.**

- **If you discover errors in your existing credit accounts, send a letter to the business explaining the error. (See Sample Letters contained in this ID Theft Kit). The business must review your letter, investigate your complaint, and tell you the results of their investigation. If the information is incorrect, the business must report its findings to the CRAs.**

- **If you discover that new accounts were fraudulently opened in your name, contact the Fraud Department of each business where an account was opened. Explain that you are an identity theft victim. Close the account.**

- **Ask if the business will accept your Identity Theft Report or if it uses special dispute forms. If you must use the business's forms, ask for blank forms.**

- **Ask the business to send you a letter confirming that:**
  - **the fraudulent account isn't yours and that you aren't liable for it.**
  - **it was removed from your credit report. Keep the letter and use it if you see this account on your credit report in the future.**

- **If the CRA's investigation does not resolve your claim, you can ask that a statement of the dispute be included in your file.**

- **Update your files. Record the dates you made calls or sent letters. Keep copies of letters in your files.**

STEP 6:

Blocking Erroneous Information from Appearing on Your Credit Reports:

Federal law requires that CRAs block identity theft-related information from appearing on a victim's credit report. They must block unauthorized transactions, accounts, and inquiries. To get unauthorized information blocked, you must take the following steps.

I. SIMPLE STEPS TO REQUEST CRAs TO BLOCK ERRONEOUS INFORMATION FROM APPEARING ON VICTIM'S CREDIT REPORT:

A. BLOCKING ERRORS CONTAINED IN YOUR CRA CREDIT REPORTS

1. **Write to each CRA (Experian, Equifax & TransUnion). See Sample Dispute Letter to CRAs on page 26.**
2. **Send a copy of your Identity Theft Report to the CRAs.**
3. **Include proof of your identity including your name, address, and Social Security number.**
4. **Explain which information on your report resulted from identity theft and that the information did not come from a transaction you made or approved.**
5. **Ask the company to block the fraudulent information.**
6. **Update your files. Record the dates you made calls or sent letters.**
7. **Keep copies of letters in your files.**
8. **If the CRA accepts your Identity Theft Report, it must block the fraudulent information from your credit report within four (4) business days after accepting your report, and inform the business that sent the fraudulent information about the block.**
9. **If the CRA rejects your Identity Theft Report, it can take five (5) days to ask you for more proof of the identity theft. It has 15 more days to work with you to get the information, and five (5) days to review information you sent. It may reject any information you send after 15 days. It must tell you if it won't block information. You can re-submit the report.**
10. **After a business has been notified about a block of information, it must:**
    • stop reporting that information to all the credit reporting companies.
    • not sell or transfer a debt for collection.

B. BLOCKING ERRORS IN BUSINESS ACCOUNTS

1. **Contact the business that sent the inaccurate information that appears on your credit report.**
2. **Send a copy of your Identity Theft Report and a letter explaining what is inaccurate.**
3. **After the business gets your report, it must stop reporting the inaccurate information to the three nationwide credit reporting companies. However, the business still can try to collect a debt, and sell or transfer the debt to a collection company.**
4. **To prevent a business from collecting, selling or transferring a debt to a collection agency, you must contact the credit reporting companies and ask them to block the fraudulent information.**
5. **Record the blocking request dates and responses received.**

Ask each company for the email or postal mail address for sending dispute or blocking requests.

STEP 7:
Requesting an Extended Fraud Alert or Security Freeze

I. EXTENDED FRAUD ALERT:

➤ **An extended fraud 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**. An automated Identity Theft Report, such as the printed ID Theft Complaint available from the Federal Trade Commission website (www.ftc.gov/idtheft/) should be sufficient to obtain an extended fraud alert. A copy of the Identity Theft Report is also included in this ID Theft Victim Kit. With an extended fraud alert, potential creditors must actually contact you, or meet with you in person, before they issue you credit. When you place an extended fraud 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 an Initial or Extended Fraud Alert on your credit report, or to have one removed, you will be required to provide appropriate proof of your identity. That may include your Social Security number, name, address and other personal information requested by the consumer reporting company.

Depending on the type of fraud alert you place, potential creditors must either contact you or take reasonable steps to verify your identity. 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.

➤ With a fraud alert in place, businesses may still check your credit report. Depending on whether you place an initial 90-day fraud alert or an extended fraud alert, potential creditors must either contact you or use what the law refers to as "reasonable policies and procedures" to verify your identity before issuing credit in your name. However, the steps potential creditors take to verify your identity may not always alert them that the applicant is not you.

➤ While a **Fraud Alert** (**Initial or Extended**) can help keep an identity thief from opening new accounts in your name, it's not a solution to all types of identity theft. It will not protect you from an identity thief using your existing credit cards or other accounts. It also will not protect you from an identity thief opening new accounts in your name that do not require a credit check — such as a telephone, wireless, or bank account. And, if there's identity theft already going on when you place the fraud alert, the fraud alert alone won't stop it. A fraud alert, however, can be extremely useful in stopping identity theft that involves opening a new line of credit.

II. CREDIT FREEZE/SECURITY FREEZE:

➤ Many states have laws that let consumers "freeze" their credit — in other words, letting a consumer restrict access to his or her credit report. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. This means that it's unlikely that an identity thief would be able to open a new account in your name. Placing a credit freeze does not affect your credit score — nor does it keep you from getting your free annual credit report, or from buying your credit report or score.

➤ Credit freeze laws vary from state to state. In New York State, a "credit freeze" is called a **"security freeze."** There is no charge for New York State residents to place a security freeze on their credit report if they are the victim of identity theft or are making this request for the first time. For second or subsequent requests for a security freeze, you may be charged up to $5.

➤ Any consumer in New York may place a security freeze on his or her credit report by requesting one in writing by certified mail or overnight mail to the consumer reporting agencies. Effective in 2010, a consumer may also place or lift a freeze via telephone or secure electronic means. The consumer reporting agencies are not allowed to charge a fee to ID theft victims for placing, temporarily removing , or permanently removing a security freeze on a credit report. To prove you are a victim, you must send a valid copy of a police report or a signed Federal Trade Commission Identity Theft Victim Affidavit.

A security freeze prohibits, with certain exceptions, the CRAs from releasing the consumer's credit report or any information from it without the express authorization of the consumer.

➤ If you place a security freeze, you will continue to have access to your free annual credit report. You'll also be able to buy your credit report and credit score even after placing a credit freeze. Companies that you do business with will still have access to your credit report — for example, your mortgage, credit card, or cell phone company — as would collection agencies that are working for one of those companies. Companies will also still be able to offer you prescreened credit. Those are the credit offers you receive in the mail that you have not applied for. Additionally, in some states, potential employers, insurance companies, landlords, and other non-creditors can still get access to your credit report with a credit freeze in place.

➤ If you want to apply for a loan or credit card, or otherwise need to give someone access to your credit report and that person is not covered by an exception to the security freeze law, you would need to temporarily lift the security freeze. You would do that by using a PIN that each credit reporting agency will send once you have placed the security freeze. In most states, you would have to pay a fee to lift the security freeze (unless you can show that you are a victim of ID theft). Most states currently give the credit reporting agencies three days to lift the security freeze. This might keep you from getting "instant" credit, which may be something to weigh when considering placing a security freeze on your credit files.

➤ While a security freeze can help keep an identity thief from opening most new accounts in your name, it's not a solution to all types of identity theft. It will not protect you, for example, from an identity thief who uses your existing credit cards or other accounts. There are also new accounts, such as telephone, wireless, and bank accounts, which an ID thief could open without a credit check. In addition, some creditors might open an account without first getting your credit report. And, if there's identity theft already going on when you place the security freeze, the freeze itself won't be able to stop it. While a security freeze may not protect

you in these kinds of cases, it can protect you from the vast majority of identity theft that involves opening a new line of credit.

➤ A security freeze will prevent potential creditors and other third parties from accessing your credit report at all, unless you lift the freeze or already have a relationship with the company. Some New York consumers use security freezes rather than a fraud alert described in the previous section because they feel security freezes give more protection. As with security freezes, fraud alerts are mainly effective against new credit accounts being opened in your name, but will likely not stop thieves from using your existing accounts, or opening new accounts such as new telephone or wireless accounts, where credit is often not checked. Also, only people who've had their ID stolen — or who suspect it may have been stolen — may place fraud alerts. In some states, anyone can place a credit freeze. (In New York any consumer can place a security freeze.)

FINAL STEP NUMBER 8:

Review, Monitor and Chart all the Steps Taken to Report the Fraudulent Use of Your Identity

CHART YOUR COURSE OF ACTION

Accurate and complete records will help you resolve your ID theft case more quickly. 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. Also, keep copies of all correspondence or forms you send.

NATIONWIDE CONSUMER REPORTING COMPANIES — 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 IDENTITY THEFT

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

Sample Dispute Letter for Existing Accounts

Use this sample letter to dispute charges on an existing account that are the result of identity theft.

[Date]

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

[Name of Company]
[Fraud Department or Billing Inquiries]
[Address]
[City, State, Zip Code]

[RE: Your Account Number (if known)]

Dear Sir or Madam:

I am writing to dispute [a] fraudulent charge[s] on my account in the amount[s] of $_____, and posted on [dates]. I am a victim of identity theft, and I did not make [this/these] charge[s]. I request that you remove the fraudulent charge[s] and any related finance charge and other charges from my account, send me an updated and accurate statement, and close the account (if applicable). I also request that you stop reporting this inaccurate information and report the correct information to all of the nationwide credit reporting companies (CRCs) to which you provided it.

Enclosed is a copy of my Identity Theft Report, credit report, and account statement showing the fraudulent items related to your company that are the result of identity theft. Also enclosed is a copy of the Notice to Furnishers of Information issued by the Federal Trade Commission, which details your responsibilities under the Fair Credit Reporting Act as an information furnisher to CRCs.

Please investigate this matter and send me a written explanation of your findings and actions.

Sincerely,
[Your Name]

Enclosures:
• Identity Theft Report
• Proof of Identity
• FTC Notice to Furnishers of Information
• Copy of account statement showing fraudulent items
• Credit report of [Your Name] identifying information to be corrected

NOTICES TO FURNISHERS OF INFORMATION: OBLIGATIONS OF FURNISHERS UNDER THE FCRA

The federal Fair Credit Reporting Act ("FCRA"), as amended, imposes responsibilities on all persons who furnish information to consumer reporting agencies ("CRAs"). These responsibilities are found in Section 623 of the FCRA. State law may impose additional requirements. All furnishers of information to CRAs should become familiar with the law and may want to consult with their counsel to ensure that they are in compliance. The FCRA, 15 U.S.C. §§ 1681-1681u, is set forth in full at the Federal Trade Commission's Internet web site *(http://www.ftc.gov)*. Section 623 imposes the following duties:

General Prohibition on Reporting Inaccurate Information:

The FCRA prohibits information furnishers from providing information to a consumer reporting agency ("CRA") that they know (or consciously avoid knowing) is inaccurate. However, the furnisher is not subject to this general prohibition if it clearly and conspicuously specifies an address to which consumers may write to notify the furnisher that certain information is inaccurate. *Sections 623(a)(1)(A) and (a)(1)(C)*

Duty to Correct and Update Information:

If at any time a person who regularly and in the ordinary course of business furnishes information to one or more CRAs determines that the information provided is not complete or accurate, the furnisher must provide complete and accurate information to the CRA. In addition, the furnisher must notify all CRAs that received the information of any corrections, and must thereafter report only the complete and accurate information. *Section 623(a)(2)*

Duties After Notice of Dispute from Consumer:

If a consumer notifies a furnisher, at an address specified by the furnisher for such notices, that specific information is inaccurate, and the information is in fact inaccurate, the furnisher must thereafter report the correct information to CRAs. *Section 623(a)(1)(B)*

If a consumer notifies a furnisher that the consumer disputes the completeness or accuracy of any information reported by the furnisher, the furnisher may not subsequently report that information to a CRA without providing notice of the dispute. *Section 623(a)(3)*

Duties After Notice of Dispute from Consumer Reporting Agency:

If a CRA notifies a furnisher that a consumer disputes the completeness or accuracy of information provided by the furnisher, the furnisher has a duty to follow certain procedures. The furnisher must:

- Conduct an investigation and review all relevant information provided by the CRA, including information given to the CRA by the consumer. *Sections 623(b)(1)(A) and (b)(1)(B)*
- Report the results to the CRA, and, if the investigation establishes that the information was, in fact, incomplete or inaccurate, report the results to all CRAs to which the furnisher provided the information that compile and maintain files on a nationwide basis. *Sections 623(b)(1)(C) and (b)(1)(D)*
- Complete the above within 30 days from the date the CRA receives the dispute (or 45 days, if the consumer later provides relevant additional information to the CRA). *Section 623(b)(2)*

Duty to Report Voluntary Closing of Credit Accounts:

If a consumer voluntarily closes a credit account, any person who regularly and in the ordinary course of business furnishes information to one or more CRAs must report this fact when it provides information to CRAs for the time period in which the account was closed. *Section 623(a)(4)*

Duty to Report Dates of Delinquencies:

If a furnisher reports information concerning a delinquent account placed for collection, charged to profit or loss, or subject to any similar action, the furnisher must, within 90 days after reporting the information, provide the CRA with the month and the year of the commencement of the delinquency that immediately preceded the action, so that the agency will know how long to keep the information in the consumer's file. *Section 623(a)(5)*

Sample Dispute Letter for New Accounts

Use this sample letter to dispute charges on an account opened in your name by an identity thief.

[Date]

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

[Name of Company]
[Fraud Department or Billing Inquiries]
[Address]
[City, State, Zip Code]

[RE: Your Account Number (if known)]

Dear Sir or Madam:

I am a victim of identity theft. I recently learned that my personal information was used to open an account at your company. I did not open or authorize this account, and I therefore request that it be closed immediately. I also request that [Company Name] absolve me of all charges on the account, and that you take all appropriate steps to remove information about this account from my credit files.

Enclosed is a copy of my Identity Theft Report, and a copy of my credit report showing the fraudulent items related to your company that are the result of identity theft. Also enclosed is a copy of the Federal Trade Commission Notice to Furnishers of Information, which details your responsibilities as an information furnisher to credit reporting companies (CRCs). As a furnisher, upon receipt of a consumer's written request that encloses an Identity Theft Report, you are required to cease furnishing the information resulting from identity theft to any credit reporting company.

The Notice also specifies your responsibilities when you receive notice from a CRC, under section 605B of the Fair Credit Reporting Act, that information you provided to the CRC may be the result of identity theft. Those responsibilities include ceasing to provide the inaccurate information to any CRC and ensuring that you do not attempt to sell or transfer the fraudulent debts to another party for collection.

Please investigate this matter, close the account and absolve me of all charges, take the steps required under the Fair Credit Reporting Act, and send me a letter explaining your findings and actions.

Sincerely,
[Your Name]

Enclosures:

- Identity Theft Report
- FTC Notice to Furnishers of Information
- Credit report of [Your Name] identifying information to be corrected

(Enclose "Notice to Furnishers of Information" — see page 18 in previous section on Sample Dispute Letter for Existing Accounts.)

Request for Fraudulent Transaction/Account Information

You can use this sample letter to request information from businesses the identity thief dealt with.

Request for Fraudulent Transaction/Account Information
Made pursuant to Section 609(e) of the Fair Credit Reporting Act
(15 U.S.C. § 1681(g))

To:
Account Number:
Description of fraudulent transaction/account:

From: [Name]
[Address]
[Telephone Number]

As we discussed on the phone, I am a victim of identity theft. The thief made a fraudulent transaction or opened a fraudulent account with your company. Pursuant to federal law, I am requesting that you provide me, at no charge, copies of application and business records in your control relating to the fraudulent transaction. A copy of the relevant federal law is enclosed.

Pursuant to the law, I am providing you with the following documentation, so that you can verify my identity:

(A) A copy of my driver's license or other government-issued identification card; and
(B) A copy of the police report about the identity theft; and
(C) A copy of the identity theft affidavit, on the form made available by the Federal Trade Commission.

Please provide all information relating to the fraudulent transaction, including:

- Application records or screen prints of Internet/phone applications
- Statements
- Payment/charge slips
- Investigator's summary
- Delivery addresses

- All records of phone numbers used to activate the account or used to access the account
- Any other documents associated with the account.

Please send the information to me at the above address. In addition, I am designating a law enforcement officer to receive the information from you. This officer is investigating my case. The law enforcement officer's name, address and telephone number is: [insert]. Please also send all documents and information to this officer.

Sincerely,
[Your name]

Enclosure: Section 609(e) of the Fair Credit Reporting Act (15 U.S.C. § 1681(g))

ENCLOSURE:
FCRA 609(e) (15 U.S.C. § 1681g(e)) Disclosures to Consumers –
Information Available to Victims

(e) Information available to victims

(1) In general

For the purpose of documenting fraudulent transactions resulting from identity theft, not later than 30 days after the date of receipt of a request from a victim in accordance with paragraph (3), and subject to verification of the identity of the victim and the claim of identity theft in accordance with paragraph (2), a business entity that has provided credit to, provided for consideration products, goods, or services to, accepted payment from, or otherwise entered into a commercial transaction for consideration with, a person who has allegedly made unauthorized use of the means of identification of the victim, shall provide a copy of application and business transaction records in the control of the business entity, whether maintained by the business entity or by another person on behalf of the business entity, evidencing any transaction alleged to be a result of identity theft to—

(A) the victim;
(B) any Federal, State, or local government law enforcement agency or officer specified by the victim in such a request; or
(C) any law enforcement agency investigating the identity theft and authorized by the victim to take receipt of records provided under this subsection.

(2) Verification of identity and claim

Before a business entity provides any information under paragraph (1), unless the business entity, at its discretion, otherwise has a high degree of confidence that it knows the identity of the victim making a request under paragraph (1), the victim shall provide to the business entity—

(A) as proof of positive identification of the victim, at the election of the business entity—
(i) the presentation of a government-issued identification card;
(ii) personally identifying information of the same type as was provided to the business entity by the unauthorized person; or
(iii) personally identifying information that the business entity typically requests from new applicants or for new transactions, at the time of the victim's request for information, including any documentation described in clauses (i) and (ii); and

(B) as proof of a claim of identity theft, at the election of the business entity—
(i) a copy of a police report evidencing the claim of the victim of identity theft; and
(ii) a properly completed—
(I) copy of a standardized affidavit of identity theft developed and made available by the Commission; or
(II) an [FN1] affidavit of fact that is acceptable to the business entity for that purpose.

(3) Procedures

The request of a victim under paragraph (1) shall—

(A) be in writing;
(B) be mailed to an address specified by the business entity, if any; and
(C) if asked by the business entity, include relevant information about any transaction alleged to be a result of identity theft to facilitate compliance with this section including—
(i) if known by the victim (or if readily obtainable by the victim), the date of the application or transaction; and
(ii) if known by the victim (or if readily obtainable by the victim), any other identifying information such as an account or transaction number.

(4) No charge to victim

Information required to be provided under paragraph (1) shall be so provided without charge.

(5) Authority to decline to provide information

A business entity may decline to provide information under paragraph (1) if, in the exercise of good faith, the business entity determines that—

(A) this subsection does not require disclosure of the information;
(B) after reviewing the information provided pursuant to paragraph (2), the business entity does not have a high degree of confidence in knowing the true identity of the individual requesting the information;
(C) the request for the information is based on a misrepresentation of fact by the individual requesting the information relevant to the request for information; or
(D) the information requested is Internet navigational data or similar information about a person's visit to a website or online service.

(6) Limitation on liability

Except as provided in section 1681s of this title, sections 1681n and 1681o of this title do not apply to any violation of this subsection.

(7) Limitation on civil liability

No business entity may be held civilly liable under any provision of Federal, State, or other law for disclosure, made in good faith pursuant to this subsection.

(8) No new recordkeeping obligation

Nothing in this subsection creates an obligation on the part of a business entity to obtain, retain, or maintain information or records that are not otherwise required to be obtained, retained, or maintained in the ordinary course of its business or under other applicable law.

(9) Rule of construction

(A) In general
No provision of subtitle A of title V of Public Law 106-102, prohibiting the disclosure of financial information by a business entity to third parties shall be used to deny disclosure of information to the victim under this subsection.

(B) Limitation

Except as provided in subparagraph (A), nothing in this subsection permits a business entity to disclose information, including information to law enforcement under subparagraphs (B) and (C) of paragraph (1), that the business entity is otherwise prohibited from disclosing under any other applicable provision of Federal or State law.

(10) Affirmative defense

In any civil action brought to enforce this subsection, it is an affirmative defense (which the defendant must establish by a preponderance of the evidence) for a business entity to file an affidavit or answer stating that—

(A) the business entity has made a reasonably diligent search of its available business records; and

(B) the records requested under this subsection do not exist or are not reasonably available.

(11) Definition of victim

For purposes of this subsection, the term "victim" means a consumer whose means of identification or financial information has been used or transferred (or has been alleged to have been used or transferred) without the authority of that consumer, with the intent to commit, or to aid or abet, an identity theft or a similar crime.

(12) Effective date

This subsection shall become effective 180 days after December 4, 2003.

(13) Effectiveness study

Not later than 18 months after December 4, 2003, the Comptroller General of the United States shall submit a report to Congress assessing the effectiveness of this provision.

Sample Dispute Letter to Credit Reporting Company

Use this sample letter to request that the consumer reporting companies block fraudulent information from appearing on your credit report.

[Date]

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

(Write to one at a time:)

Equifax Information Services, LLC
PO Box 105169
Atlanta, GA 30348

-or-

Experian
P.O. Box 9554
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 Report. 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 Report
FCRA Section 605B

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 title.

For on-line help in completing letters for ID theft victims:

- ➤ Go to: lawhelp.org/NY/
- ➤ Click on: Consumer
- ➤ Then, click on: Identity Theft

INCIDENT

1. Agency: LIVINGSTON CO SHERIFF'S OFFICE
2. Division/Precinct: GENESEO FD

New York State INCIDENT REPORT

3. ORI: NY 0250000
4. ☐ Orig ☒ Supp
5. Case No.: 201200014754
6. Incident No.: 201200014754

7. Report Day: Wed | 8. Date: 08 22 12 | 9. Report Time: 1141 | Occurred On/From: 10. Day: Mon | 11. Date: 07 16 12 | 12. Time: 1200 | Occurred To: 13. Day: Mon | 14. Date: 07 16 12 | 15. Time: 1300

16. Incident Type: IMPERSONATION
17. Business Name:
18. Weapon(s):

19. Incident Address (Street No., Street Name, Bldg. No., Apt. No.): 4 COURT ST
20. City, State, Zip (☐ C ☐ T ☐ V): GENESEO - VILLAGE OF
21. Location Code: 2622

22. OFF. NO	LAW	SECTION	SUB	CL	CAT	DEG	ATT	NAME OF OFFENSE	CTS
1	PL	190.79		E	F	2	C	IDENTITY THEFT 2-ASSUME ANOTHER'S IDENTITY TO DEFR	1
2									
3									

23. No. of Victims: 1
24. No. of Suspects: 1

A.
B.
C.
D. 01
E. 09
F.
G.
H. I
I. 4
J.
K. 7
L. 30
M. 0
N. 77

ASSOCIATED PERSONS

25. Person Type: CO = Complainant OT = Other PI = Person Interviewed PR = Person Reporting WI = Witness NI = Not Interviewed VI = Victim
26. Victim also complainant ☐ Y ☒ N

TYPE/NO	NAME (LAST, FIRST, MIDDLE, TITLE)	Date of Birth	STREET NO., STREET NAME, BLDG. NO., APT. NO., CITY, STATE, ZIP	TELEPHONE NO.
				BUSINESS / RESIDENCE
				BUSINESS / RESIDENCE
				BUSINESS / RESIDENCE
V1	SAMPLE, SUE Z	01/01/55	456 SAMPLE ST GENESEO, NY 14454-	BUSINESS (555)555-1111

VICTIM

27. Date of Birth: 01 01 55
28. Age: 57
29. Sex: ☐ M ☒ F ☐ U
30. Race: ☒ White ☐ Black ☐ Other ☐ Indian ☐ Asian ☐ Unk.
31. Ethnic: ☐ Hispanic ☐ Unk. ☒ Non-Hispanic
32. Handicap: ☐ Yes ☐ No
33. Residence Status: ☒ Resident ☐ Commuter ☐ Tourist ☐ Military ☐ Temp. Res.- Foreign Nat ☐ Student ☐ Homeless ☐ Other ☐ Unk.
34. Victim DID receive information on Victim's Rights and Services pursuant to New York State Law ☐ YES ☒ NO

SUSPECT MISSING/ARRESTED PERSON

35. Type/No.: S1
36. Name (Last, First, Middle): SMITH, JOHN A
37. Alias/Nickname/Maiden Name (Last, First, Middle):
38. Apparent Condition: ☐ Impaired Drugs ☐ Impaired Alco ☐ Mental Dis ☐ Inj / Ill ☐ Unk. ☒ App Norm
39. Address (Street No., Street Name, Bldg. No., Apt. No., City, State, Zip)): 123 ANY ST GENESEO, NY 14454-
40. Phone No.: (585)555-5555 ☒ Home ☐ Work
41. Social Security No.
42. Date of Birth: 05 05 55
43. Age: 57
44. Sex: ☒ M ☐ F ☐ U
45. Race: ☒ White ☐ Black ☐ Other ☐ Indian ☐ Asian ☐ Unk.
46. Ethnic: ☐ Hispanic ☐ Unk. ☒ Non-Hispanic
47. Skin: ☐ Light ☐ Dark ☐ Unk ☐ Medium ☐ Other
48. Occupation:
49. Height: ft. in.
50. Weight
51. Hair
52. Eyes
53. Glasses: ☐ Yes ☐ Contacts ☐ No
54. Build: ☐ Small ☐ Large ☐ Medium
55. Employer/School
56. Address
57. Scars/Marks/Tattoos (Describe)
58. Misc.

PROPERTY

59. Victim or Suspect No.	Property Status	Property Type	Quantity/ Measure	Make or Drug Type	Model	Serial No.	Description	Value
	07	49					IDENTITY OF SUE Z. SAMPLE	1.00
S1	07	49	1				CAPITAL ONE CREDIT CARD	
							TOTAL	1.00

VEHICLE

60. Vehicle Status
61. License Plate No. Full ☐ Partial ☐
62. State
63. Exp. Yr.
64. Plate Type
65. Value
66. Veh. Yr.
67. Make
68. Model
69. Style
70. VIN
71. Color(s)
72. Towed By: To:
73. Vehicle Notes

NARRATIVE

74. CASE NARRATIVE 8/23/2012 2:55 PM
8/23/2012 1400 hrs Deputy Officer
IDENTITY THEFT CR#2012-14754
Responding Officer met with (V) Sue Z. Sample who received a phone call from Capital One Fraud Department advising that someone had possibly attempted to open an account under her name. Sue stated that a few years ago she had problems with an ex-boyfriend, (S) John A. Smith, doing this same thing. Sue stated that her ex-boyfriend is living on Any Street in Geneseo. Sue stated that it was reported to her that they did give an address for Any Street for where the account was being opened. Responding Officer will follow up on this report.

TOTAL
B use cover sheet

ADMINISTRATIVE

75. Inquiries (Check all that apply): ☐ DMV ☐ Crim. History ☐ Want/Warrant ☐ Stolen Property ☐ Scofflaw ☐ Other
76. NYSPIN Message No.
77. Complainant Signature
78. Reporting Officer Signature (Include Rank): APPLIN, PHYLLIS A DEP ROAD
79. ID No.: 135
80. Supervisor's Signature (Include Rank)
81. ID No.
82. Status ☐ Open ☒ Closed (if Closed, check box below) ☐ Unfounded ☐ Victim Refused to Coop. ☐ Arrest ☐ Pros Declined ☐ Warrant Advised ☐ CBI ☐ Juv. - No Custody ☐ Arrest - Juv ☐ Offender Dead ☐ Extrad. Declin ☐ Unk
83. Status Date: 08 23 12
84. Notified/TOT
85. 1 Page 1 Pages

DCJS-3205 (11/06) *FALSE STATEMENTS ARE PUNISHABLE AS A CRIME, PURSUANT TO THE NEW YORK STATE PENAL LAW

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:

☐ 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).

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

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

EQUIFAX Experian A world of insight 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.**

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

31238

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

Resources and Contact Information

Credit Reporting Companies

Equifax
www.equifax.com
1-800-525-6285

Experian
www.experian.com
1-888-397-3742

TransUnion
www.transunion.com
1-800-680-7289

Federal Communications Commission
For help with telephone service:
www.fcc.gov/cgb
1-888-225-5322
1-888-835-5322 (TTY)

Federal Government

Federal Financial Institutions Examination Council
To locate the agency that regulates
a bank or credit union:
www.ffiec.gov/consumercenter

Federal Trade Commission
To report identity theft:
www.ftc.gov/complaint
1-877-438-4338
1-866-653-4261 (TTY)

Internal Revenue Service
Identity Protection Specialized Unit
To report identity theft:
www.irs.gov/identitytheft
1-800-908-4490

Legal Services Programs
To locate a legal services provider:
www.lsc.gov/local-programs/
program-profiles

Social Security Administration
To report fraud:
go to www.socialsecurity.gov and type "Fraud" in the Search box.
1-800-269-0271
1-866-501-2101 (TTY)

U.S. Department of Education
To report fraud:
www.ed.gov/about/offices/list/oig/hotline.html
Or go to www.ed.gov and type
"OIG Hotline" in the Search box.
1-800-647-8733

U.S. Department of Justice, Office for Victims of Crime

Identity Theft Resources
http://www.ojp.usdoj.gov/programs/identitytheft.htm

Identity Theft Victim Assistance Online Training
https://www.ovcttac.gov/views/TrainingMaterials/dspOnline_IdentityTheft.cfm

To report suspected bankruptcy fraud:
www.justice.gov/ust/eo/fraud
or send email to
USTP.Bankruptcy.Fraud@usdoj.gov

U.S. Postal Inspection Service
To file a complaint:
https://postalinspectors.uspis.gov/contactUs/filecomplaint.aspx
1-877-876-2455

U.S. Postal Service
To place a hold on mail:
www.usps.com/holdmail
To locate a post office:
www.usps.com
1-800-275-8777

U.S. Securities and Exchange Commission
To report fraud:
www.sec.gov/complaint/
tipscomplaint.shtml
1-800-732-0330

U.S. Department of State
To report a lost or stolen passport:
www.travel.state.gov/passport
1-877-487-2778
1-888-874-7793 (TDD/TTY)

U.S. Senate Special Committee on Aging Anti-Fraud Hotline
Older adults can report suspected fraud and receive assistance from a team of committee investigators weekdays from 9 am to 5 pm EST.
www.aging.senate.gov/fraud-hotline
1-855-303-9470

New York State

NYS Division of Consumer Protection
NYS Department of State
ID Theft Mitigation
Consumer Assistance Unit
1-518-474-8583
1-800-697-1220

NYS Attorney General's Office
http://www.ag.ny.gov/consumer-frauds-bureau/identity-theft
LawHelp NY
www.lawhelp.org/NY/

NYS Coalition on Elder Abuse
www.nyselderabuse.org

Other Resources

American Bar Association
To locate state and local bar associations:
www.americanbar.org/groups/bar_services/resources/state_local_bar_associations.html

Free Annual Credit Reports
To order a free annual credit report:
www.annualcreditreport.com
1-877-322-8228

Certegy
To ask about a declined check:
www.askcertegy.com
1-800-437-5120

ChexSystems, Inc.
To report checking accounts opened in your name:
www.consumerdebit.com
1-800-428-9623

National Association of Regulatory Utility Commissioners
To get contact information for a state utility commission:
www.naruc.org/commissions
1-202-898-2200 *(Not a toll-free number)*

Opt Out
To opt out of prescreened offers of credit or insurance:
www.optoutprescreen.com
1-888-567-8688

TeleCheck Services, Inc.
To report check fraud:
www.firstdata.com/telecheck
1-800-710-9898

Identity Theft Resource Center
http://www.idtheftcenter.org\

Privacy Rights Clearinghouse
www.privacyrights.org

To contact the Finger Lakes ID Theft Coalition,
call Lifespan at 1-585-244-8400
or send e-mail to info@lifespan-roch.org

Finger Lakes Identity Theft Coalition
Lifespan of Greater Rochester Inc.
1900 South Clinton Avenue
Rochester, New York 14618
(585) 244-8400
www.lifespan-roch.org