Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>WELCOME</td>
<td>1</td>
</tr>
<tr>
<td>INTRODUCTION</td>
<td>2</td>
</tr>
<tr>
<td>IDENTITY THEFT</td>
<td></td>
</tr>
<tr>
<td>PREVENTION AND DETECTION</td>
<td>3</td>
</tr>
<tr>
<td>Prevention and Detection Tools</td>
<td>3</td>
</tr>
<tr>
<td>Prevention and Detection Tips</td>
<td>4</td>
</tr>
<tr>
<td>Social Security Number</td>
<td>4</td>
</tr>
<tr>
<td>Credit Report</td>
<td>4</td>
</tr>
<tr>
<td>Credit Cards</td>
<td>4</td>
</tr>
<tr>
<td>Bank Statements &amp; Checks</td>
<td>5</td>
</tr>
<tr>
<td>Mail</td>
<td>5</td>
</tr>
<tr>
<td>Automobile</td>
<td>6</td>
</tr>
<tr>
<td>Cell Phone</td>
<td>6</td>
</tr>
<tr>
<td>Computer</td>
<td>6</td>
</tr>
<tr>
<td>Passwords</td>
<td>6</td>
</tr>
<tr>
<td>Medical Records and Health Insurance</td>
<td>6</td>
</tr>
<tr>
<td>Home</td>
<td>7</td>
</tr>
<tr>
<td>Workplace</td>
<td>7</td>
</tr>
<tr>
<td>Traveling</td>
<td>7</td>
</tr>
<tr>
<td>Social Media</td>
<td>8</td>
</tr>
<tr>
<td>IDENTITY THEFT RESOLUTION</td>
<td>9</td>
</tr>
<tr>
<td>Your Primary Goals</td>
<td>9</td>
</tr>
<tr>
<td>Collecting Information</td>
<td>9</td>
</tr>
<tr>
<td>Resolution Tools</td>
<td>10</td>
</tr>
<tr>
<td>RESOLVING VARIOUS FORMS OF IDENTITY THEFT</td>
<td>11</td>
</tr>
<tr>
<td>Lost or Stolen Social Security Card</td>
<td>12</td>
</tr>
<tr>
<td>Lost or Stolen Driver’s License</td>
<td>12</td>
</tr>
<tr>
<td>Lost or Stolen Passport</td>
<td>12</td>
</tr>
<tr>
<td>Credit Card Identity Theft</td>
<td>13</td>
</tr>
<tr>
<td>Check Fraud</td>
<td>13</td>
</tr>
<tr>
<td>Bankruptcy Fraud</td>
<td>14</td>
</tr>
<tr>
<td>Student Loan Fraud</td>
<td>14</td>
</tr>
<tr>
<td>Tax Fraud</td>
<td>14</td>
</tr>
<tr>
<td>Lost or Stolen Medicare Card</td>
<td>14</td>
</tr>
<tr>
<td>Medical Identity Theft</td>
<td>15</td>
</tr>
<tr>
<td>Employment Fraud</td>
<td>16</td>
</tr>
<tr>
<td>Child Identity Theft</td>
<td>16</td>
</tr>
<tr>
<td>Mail Fraud</td>
<td>17</td>
</tr>
<tr>
<td>Telephone Fraud</td>
<td>17</td>
</tr>
<tr>
<td>Online Identity Theft</td>
<td>17</td>
</tr>
<tr>
<td>Synthetic Identity Theft</td>
<td>18</td>
</tr>
<tr>
<td>Automobile Identity Theft</td>
<td>18</td>
</tr>
<tr>
<td>THE FTC’S IDENTITY THEFT AFFIDAVIT</td>
<td>19</td>
</tr>
<tr>
<td>Instructions for Completing the Identity Theft Affidavit</td>
<td>19</td>
</tr>
<tr>
<td>Sample Letter for Dispute of Fraudulent Charges</td>
<td>20</td>
</tr>
<tr>
<td>Sample FTC Identity Theft Affidavit</td>
<td>26</td>
</tr>
</tbody>
</table>
Dear GEICO Insurance Agency Customer,

We are delighted to welcome you to the GEICO Portfolio ID Theft Protection Program, provided by Europ Assistance USA. With EA USA, you get an identity theft protection program specially designed for GEICO Insurance Agency customers. Our program puts equal emphasis on prevention, detection and resolution, providing you peace of mind and a trusted advocate who will work on your behalf should you experience identity theft.

If you have any questions, please do not hesitate to contact EA USA at the toll-free number above 24 hours a day, 7 days a week.

Welcome and thank you for choosing the GEICO Portfolio ID Theft Protection Program, with service provided by EA USA.

Sincerely,
John Zinno
President
GEICO Insurance Agency, Inc.

Secured Through:
GEICO Insurance Agency, Inc.
One GEICO Blvd.
Fredericksburg, VA 24122

Provided by:
4330 East West Hwy. Ste. 1000
Bethesda MD, 20814
1-800-206-4065
An estimated 3.5% of Americans fell victim to theft and fraud last year with the total cost of this crime to consumers and businesses being more than $36 billion.

— Javelin Strategy & Research, Identity Fraud Survey, 2/2011
# Identity Theft

## Prevention And Detection

Identity theft can be inconspicuous. Often times, you may not realize your identity has been compromised until it’s too late. Taking advantage of these tips is not only a quick way to make yourself less of a target, but will ultimately help safeguard your financial security, credit and privacy.

## Prevention and Detection Tools

<table>
<thead>
<tr>
<th>Identity Theft Prevention Tools</th>
</tr>
</thead>
<tbody>
<tr>
<td>3 Bureau Credit Monitoring: 3 bureau credit monitoring is a credit monitoring service that tracks any changes in all three credit bureaus (Experian, Equifax and TransUnion). The use of 3 bureau credit monitoring is to determine if any inaccuracies have been reported by information providers and/or if fraudulent activity has occurred. Credit monitoring includes:</td>
</tr>
<tr>
<td>• Daily or weekly checks for credit report changes</td>
</tr>
<tr>
<td>• Details of all loans opened in the subscriber’s name</td>
</tr>
<tr>
<td>• Details of all credit cards opened in the subscriber’s name</td>
</tr>
<tr>
<td>• A complete payment history breakdown</td>
</tr>
<tr>
<td>• Information regarding all credit report viewings</td>
</tr>
<tr>
<td>• Line-by-line comparisons of reports from the three national credit bureaus</td>
</tr>
<tr>
<td>• Immediate alert of any changes by email or other communication options</td>
</tr>
<tr>
<td>Identity Monitoring: Identity monitoring or tracking is another detection tool to alert you if your personal information is being used. Identity monitoring services typically track use of your personal information in non-credit data sources such as public records, 3rd party databases, court records and Internet sites to detect exposure of your personal information. Identity monitoring adds another layer of protection outside of credit data and can alert you if your personal information is used to file bankruptcy, in the course of an arrest or is being sold in black market trading sites.</td>
</tr>
<tr>
<td>Anti-Phishing &amp; Anti-Keylogging Software: This software prevents your online data from being obtained without your consent by criminals. Software such as Europ Assistance’s Online Data Protection Suite can help protect you from keylogging software that records every keystroke you make or takes pictures of your screen to steal data. It can also help protect you from inadvertently navigating to fraudulent websites that appear to come from brands you trust and are designed to obtain your personal information.</td>
</tr>
<tr>
<td>Suppressing Credit Reports: Suppressing your credit report means granting creditors no access at all to your credit report. However, you will still be able to access your own credit report.</td>
</tr>
<tr>
<td>Consumer Statements: A consumer statement is placed on a minor’s credit report that notifies creditors that the information used is that of a minor and therefore stops the transaction from being completed.</td>
</tr>
<tr>
<td>Military Active Duty Statement: If you are a member of the military and away from your usual duty station, you may place an active duty alert on your credit report to help minimize the risk of identity theft while you are deployed.</td>
</tr>
</tbody>
</table>
PREVENTION AND DETECTION TIPS

Your Social Security Number:

Memorize your Social Security number. Do not carry your Social Security card in your wallet.

Ask if the information is required. Before providing identifying information, especially your Social Security number, ask to use other types of identifiers or if you can provide the last four digits instead.

Remove your Social Security number from any identification you carry, such as checks, a driver’s license or your health insurance card. Both your health insurance company and the Department of Motor Vehicles will give you a substitute number if you request it.

Your Credit Report:

Check your free credit reports at least once a year at each credit bureau to ensure that fraudulent accounts have not been opened in your name. (Requests can be staggered to provide a report once every four months.) Carefully review your credit reports and address any inaccuracies. To order your free annual report from one or all three credit bureaus:

- Visit www.annualcreditreport.com or call toll-free 877-322-8228.
- Hearing impaired consumers can access TDD service at 1-877-730-4104.
- Do not contact the three credit bureaus individually as they provide free annual credit reports only through the channels detailed above.

Attempt to obtain a credit report for your child on his/her 16th birthday. Ideally, there won’t be one but if there is and it contains inaccurate information, this may be an indication of fraud which gives you ample time to resolve the problem before your child applies for college financial aid or his/her first loan.

Your Credit Cards:

Don’t disclose credit card or other financial account numbers on a web site unless the site offers a secure transaction.

Call the financial institution, if the credit card you applied for has not arrived when expected.

Cancel all unused credit card accounts. Even though you do not use them, their account numbers are recorded on your credit report.

Avoid paying by credit card if you suspect the business does not use adequate safeguards to help protect your personal information.

Keep copies of all your cards and identification in a secure location. Copy both the front and the back of the card so you will be able to access the copies and easily call the issuer to cancel the card if your wallet is lost or stolen.

Enroll in electronic statement delivery and bill pay if you feel comfortable doing so. Electronic statements are harder to steal than paper ones.
Your Bank Statements & Checks:

**Review your transactions.** Check your bank and credit card statements monthly for signs of suspicious activity. Alternatively, you can spot abnormal transactions right away by regularly tracking account activity through online banking and also by using customizable e-mail or SMS/text alerts. Mobile banking is another channel through which you can keep watch over your accounts, allowing for on-the-go monitoring with access right at your fingertips.

**Call if statements are late.** If your statement is late by more than a couple of days, call your credit card company or bank to confirm your billing address and account balances.

**Request to receive bank and credit card statements via e-mail or online** when possible. Electronic statements are harder to steal than paper ones.

**Safeguard your paper checks.** Paper checks are risky because they have your checking account and bank routing number on them. When ordering new checks, pick them up from the bank instead of having them mailed to your home.

Your Mail:

**Deposit your outgoing mail in post office collection boxes** or at your local post office, rather than in an unsecured mailbox. If you do not have one, consider purchasing a mailbox that locks. This can deter someone from stealing your mail.

**Request a vacation hold.** If you’re planning to be away from home and can’t pick up your mail, call the U.S. Postal Service at 1-800-275-8777 to request a vacation hold. The Postal Service will hold your mail at your local post office until you can pick it up or are home to receive it. In some areas you can also request a mail hold online at [https://dunsapp.usps.gov/HoldMail.jsp](https://dunsapp.usps.gov/HoldMail.jsp).

**Opt Out.** Opt out of receiving offers of credit in the mail by calling: 1-888-5-OPT-OUT (1-888-567-8688) or through [www.optoutprescreen.com](http://www.optoutprescreen.com). The three credit bureaus let consumers choose not to receive credit offers based on their credit histories. You can also reduce the amount of direct marketing material you receive by registering for the Direct Marketing Association’s Mail Preference Service (MPS). To register, visit the DMA’s web site at [https://www.dmaconsumers.org/cgi/offmailing](https://www.dmaconsumers.org/cgi/offmailing). There is a small fee to register.

**Beware of mail or telephone solicitations that offer prizes or awards,** especially if they ask personal information or financial account numbers. Identity thieves may create phony promotional offers to obtain your personal information.
**Your Automobile:**

Do not leave any personal information in your car.

Review seller’s information before purchasing a car. When buying a car from an individual, make sure the title and registration match the name and address of the person selling the car. In addition, confirm that the Vehicle Identification Number (VIN) on the title matches the VIN of the car. The VIN is usually located on the left side of the dashboard and is visible through the windshield. Additionally, be cautious of a seller with no fixed address, place of employment or phone number.

**Your Cell Phone:**

Place your cell phone number on the Do Not Call Registry. Federal Law prohibits telemarketers from using automated dialers to call cell phones. You may do so by contacting the National Do Not Call Registry either by phone at 1-888-382-1222 or online at www.donotcall.gov. Registration is free of charge and does not expire.

Use digital signals. If you use analog cellular or cordless phones, consider replacing them with digital models. Digital signals are more difficult to eavesdrop on than analog signals.

**Your Computer:**

Always use a secure Internet connection and document encryption.

Install anti-virus and anti-malware software on your computer and keep it updated along with applications, browsers and operating systems. Install security patches and software updates as soon as they are released by verified sources.

Don’t keep computers online when not in use. Either shut them off or physically disconnect them from your Internet connection.

Be cautious about opening any attachment or downloading any files from e-mails you receive, regardless of who sent them. These files can contain viruses or other software that can weaken your computer’s security.

Beware of e-mails that address you as: “Dear cardholder, Dear customer, etc.” E-mails from banks or companies with whom you do business will address you by name.

**Your Passwords:**

Do not use passwords based on other personal information, such as the last four digits of your Social Security number, your date of birth, your mother’s maiden name, your phone number or a series of consecutive numbers.

Memorize your passwords and don’t record them on anything you carry.

Vary the characters. Using random capitalization, numbers and symbols often prevent password detection software from discovering your password.

**Your Medical Records and Health Insurance:**

Keep copies of your medical and insurance records secure, whether they’re on paper in a desk drawer or electronic in an online file. Be on guard when you use the Internet, especially to access accounts or records related to your medical care or insurance.

Ask to see your medical files from your healthcare provider on a regular basis. If a healthcare provider will not allow you to see your own medical records, you can file a complaint with the Office of Civil Rights at Health and Human Services.

Monitor and review medical and insurance bills for services, medicine and equipment to ensure you are only being billed for services you received. Request from your health insurance company an annual list of benefits that have been provided and review it for any fraudulent activity.

To obtain a free copy of your annual medical report, U.S. residents can call the MIB Group’s toll-free number for disclosure at 866-692-6901 (TTY 866-346-3642 for hearing impaired) or by going online to www.annualmedicalreport.com
Be sure to use only reputable tax preparers as that person will have access to your personal financial records.

Check your annual income statement from the Social Security Administration for any discrepancies between the income reported and the wages you received. An identity thief can steal your Social Security number and use it to get a job. In addition, be aware that the IRS may then think you have not reported all of your income on your tax return.

Invest in a shredder. Shred your charge receipts, copies of credit applications, insurance forms, physician statements, checks and bank statements, expired charge cards that you’re discarding and credit offers you get in the mail. Preferably use a crosscut shredder, which cuts paper into confetti-like pieces instead of strips.

Secure personal information, including tax documents. Consider investing in a document safe to store your sensitive personal information.

Secure personal information in your workplace. Keep your purse or wallet in a safe place at work. Do the same with copies of administrative forms that have your sensitive personal information such as your paycheck.

Ask about information security procedures in your workplace and at businesses, doctor’s offices or other institutions that collect your personally-identifying information.

Find out who has access to your personal information and verify that records are kept in a secure location.

Keep the software for your devices (smart phones, laptop, etc.) up to date as updates frequently contain security patches.

Back up your devices before traveling and remove personal information not critical to your travel in case your device is lost or stolen.

Use a hard wired connection (DSL or cable) whenever possible, rather than public wi-fi unless you are carrying your own wi-fi hotspot. The wired connection in your hotel room is generally more secure than any free wi-fi network.

Beware of public computers. Malware that can memorize your keystrokes could be lurking inside. Unless you know that the public computer at a library, youth hostel, hotel, etc. is safe, don’t use it for anything more personal than directions to a restaurant or movie listings, etc.

The average identity theft victim spent 33 hours resolving the crime.

— Javelin Strategy & Research, Identity Fraud Survey, 2/2011
Using Social Media:

**Make sure your social media sites are also secure connections.** Look for the lock icon in the lower right hand corner of the browser and https:// (not just http://) in the URL of sites like Facebook and Twitter. If you don’t see the lock there, change your settings on the social media site to the more secure https:// connection.

**Reduce the amount of personal information on your profile.** While any one piece of information may be harmless, the combination of a few key pieces of information about you makes it easy for a criminal to do damage (e.g. your name, date of birth, hometown, age, phone number, etc.)

**Don’t accept the default privacy settings on social networks.** Their objective is to grow usage and traffic so they often have default settings that allow a lot of your information to be seen outside of your network and appear in online searches. Take the time to learn the ins and outs of the site’s privacy settings and how to adjust yours to protect yourself.

**Post sparingly.** Even if you delete the information from a site, older versions exist on other people’s computers. Post with the thought that it will live on forever and ask yourself if you are willing to have this information available to potentially anyone forever. If not, don’t post it.

**Verify friend requests.** Be cautious when accepting requests from people you don’t know. Social media identity theft is growing, with criminals posing as others to gain access to that person’s network and information. When you get a request from a “real” friend, check the profile information to make sure it matches what you know about the person. Be suspicious of profiles from friends that are “bare-bones” with basic information.
If you have become a victim of identity theft, you are probably feeling violated and anxious about the impact this may have on your family, business and your overall future. This kit will assist you through the process of resolving your identity theft case and clearing your name.

YOUR PRIMARY GOALS

No matter what type of identity theft victim you are, your primary goals are to:

1. Close fraudulent accounts.
2. Clear yourself of responsibility for any debts or other criminal activities the thief has perpetrated in your name.
3. Ensure that the information on your credit report is accurate.

This kit will help you develop a plan of action to accomplish these goals. Make a list of the documents you’ll need and a list of companies from which you’ll need to get those documents.

COLLECTING INFORMATION

When contacting a company, don’t assume that the person you talk to will give you the information you need. Determine in advance what information or result you want and develop a list of questions or a strategy to achieve your goal. For example, the company you call may first say they weren’t the ones that extended the credit to the thief. But if you ask, they may be able to tell you which company did. Listen carefully and take notes. Don’t end the call until you’re sure you understand everything you’ve been told. If you don’t feel you’re getting the help you need, ask to speak to a supervisor.

Tips to help keep your case organized

- Follow up in writing with all contacts you’ve made on the phone or in person. Use certified mail, return receipt requested.
- Keep copies of all correspondence or forms you send.
- Keep a list of anyone you talk to, what you were told and the date of the conversation.

Keep originals of supporting documentation, like police reports and letters to and from creditors. Share copies only.

Keep old files even if you think your case is closed. Once resolved, most cases stay resolved. However, some cases can crop up again. Should this happen, these files will help you quickly resolve the case.
**RESOLUTION TOOLS**

**Fraud Alert:**

A fraud alert is an announcement that major credit bureaus place on your credit report in order to prevent transactions from occurring without your consent. This announcement makes lenders aware that if a new account is being opened under your name, they should contact you to confirm that you really wish to open it. A fraud alert does not force lenders to call you, but it does encourage them to do so for your own safety.

To place a fraud alert on your credit report, contact one of the three credit bureaus. Once the fraud alert is placed by the bureau contacted, then the other two credit bureaus will automatically place a fraud alert on your credit report.

- Equifax: 1-800-525-6285  [www.equifax.com](http://www.equifax.com)
- Experian: 1-888-397-3742  [www.experian.com](http://www.experian.com)
- TransUnion: 1-800-680-7289  [www.transunion.com](http://www.transunion.com)

Request a 7 year fraud alert. Typically, perpetrators are aware that the initial fraud alert lasts for only 90 days and might make an attempt once the alert has expired. Also, with placing a 7 year fraud alert, a police report is required, which demonstrates the validity of the identity theft incident and can be used for disputing purposes. In addition, when a 90 day fraud alert is placed, the consumer is entitled to one free credit report from each bureau. For a 7 year alert, the consumer is entitled to two free credit reports from each bureau.

Removing a fraud alert: To remove a fraud alert, you should contact the three credit bureaus in writing, stating that you would like the fraud alert removed. You should include: your name, Social Security number, current address, telephone number and date of birth.

- TransUnion Fraud Division, P.O. Box 6790, Fullerton, CA 92834
- Experian Fraud Division, P.O. Box 9532, Allen, TX 75013
- Equifax Consumer Fraud Division, P.O. Box 740256, Atlanta, GA 30374

**Credit Freeze:**

A credit freeze will lock your credit report and prevent any information from being released to any institutions, including merchants and financial institutions. To place a credit freeze on your credit report you need to process the freeze through all three credit bureaus. The cost to process a credit freeze may vary by state, but often you pay $10 for each bureau freeze and then an additional $10 to lift it. Identity theft victims may have these charges waived. Due to the complexity of placing the freeze and having it removed, we seldom recommend the credit freeze. In most states, if an actual identity theft has not occurred, there is a minimal charge.

Lifting a credit freeze: 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 credit freeze law, you will need to temporarily lift the credit freeze. You can do this by using a PIN that each credit bureau provides with placement of the credit freeze. In most states, you must pay a fee to lift the credit freeze. Most states currently give the credit bureaus three days to lift the credit freeze. This might keep you from getting “instant” credit, which may be something to weigh when considering a credit freeze. For more information on the rules for your state, visit [http://www.consumersunion.org/campaigns/learn_more/003484indiv.html](http://www.consumersunion.org/campaigns/learn_more/003484indiv.html)
## Resolving Various Forms Of Identity Theft

<table>
<thead>
<tr>
<th>Type of Identity Theft</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lost or Stolen Social Security Card</td>
</tr>
<tr>
<td>Credit Card Identity Theft</td>
</tr>
<tr>
<td>Student Loan Fraud</td>
</tr>
<tr>
<td>Medical Identity Theft</td>
</tr>
<tr>
<td>Mail Fraud</td>
</tr>
<tr>
<td>Synthetic Identity Theft</td>
</tr>
<tr>
<td>Lost or Stolen Driver’s License</td>
</tr>
<tr>
<td>Check Fraud</td>
</tr>
<tr>
<td>Tax Fraud</td>
</tr>
<tr>
<td>Employment Fraud</td>
</tr>
<tr>
<td>Telephone Fraud</td>
</tr>
<tr>
<td>Automobile Identity Theft</td>
</tr>
<tr>
<td>Lost or Stolen Passport</td>
</tr>
<tr>
<td>Bankruptcy Fraud</td>
</tr>
<tr>
<td>Lost or Stolen Medicare Card</td>
</tr>
<tr>
<td>Child Identity Theft</td>
</tr>
<tr>
<td>Online Identity Theft</td>
</tr>
</tbody>
</table>
LOST OR STOLEN SOCIAL SECURITY CARD

Steps to Resolve Lost or Stolen Social Security Card:

1. If your Social Security card has been lost or stolen, you need to request a replacement. You can send an application for a Social Security card by mail, but only if you wish to send the original documents to your local Social Security Administration (SSA) office. The SSA does not accept photocopies of documents.

   If you prefer not to send the original documents, you have to go to a SSA office in person. Locate the nearest Social Security office at [http://www.ssa.gov/locator/](http://www.ssa.gov/locator/).

2. You will need to have with you the Form SS-5, which you can download at [www.ssa.gov](http://www.ssa.gov). Please note that in addition to completing the form you will need to present one identifying document to the local Social Security office. Some documents that SSA can accept as proof of identity are:
   - Driver’s license
   - Marriage or divorce record
   - Military records
   - Employer ID card
   - Adoption record
   - Insurance policy
   - Passport
   - Health insurance card (not a Medicare card)
   - School ID card

If you were born outside of the United States, you must show proof of US citizenship or lawful alien status.

Please also note that SSA takes no special action when the card gets lost. Therefore, your replacement card will have the same number as your old card. Only after you have done all you can to fix the problem and someone is still using your Social Security number, under certain circumstances, SSA may assign a new number. A new Social Security number will NOT be assigned if you:
   - Intend to avoid the law or your legal responsibility
   - Commit fraud or a criminal action
   - Intend to avoid disclosing a poor credit or criminal record
   - Have filed for bankruptcy or
   - Have either lost your Social Security card or it has been stolen, but there is no evidence that someone else is using your Social Security number or that you are being disadvantaged by that use.

3. If you suspect fraud from Social Security personnel, you should contact the Social Security Fraud Hotline at 1-800-269-0271, fax (410) 597-0118 or e-mail at oig.hotline@ssa.gov to report allegations of fraud, waste and abuse within Social Security programs and operations only. Or you can fill out the online Fraud Reporting Form at [www.ssa.gov](http://www.ssa.gov).

LOST OR STOLEN DRIVER’S LICENSE

If your driver’s license has been lost or stolen, please contact your local DMV office.

LOST OR STOLEN PASSPORT

Steps to Resolve Lost or Stolen Passport:

1. Contact the US Department of State to report it by providing form DS-64: Statement Regarding Lost or Stolen Passport. You can download the application form at [www.travel.state.gov](http://www.travel.state.gov). Once completed and signed, send it to the following address:

   US Department of State
   Passport Services
   Consular Lost/Stolen Passport Section
   1111 19th Street, NW, Suite 500
   Washington, DC 20036

2. In the event of an emergency, you can call the US Department of State at (202) 955-0430 during business hours to report the loss. Once the submitted information is introduced in the Consular Lost/Stolen Passport System:
   - Passports reported lost or stolen are invalidated and can no longer be used for travel.
   - If you recover the passport after reporting it lost or stolen, you have to mail it to the address listed above. When submitted, if requested, they will cancel it and return it to you. If not requested, it will be destroyed.

4. Once a passport is reported lost or stolen, it cannot be re-validated.

5. You will then need to obtain a new passport. You can download a passport application (DS-11: Application for Passport) at [www.travel.state.gov](http://www.travel.state.gov) and follow the instructions on the application to obtain a new one.
CREDIT CARD IDENTITY THEFT

Steps to Resolve Credit Card Identity Theft:

1. If your credit card has been lost or stolen, contact your credit card issuer immediately. The financial institution’s representative will request the following information, which will facilitate the cancellation of your card:
   - **Full account number** of the card that is missing. If you are a secondary cardholder, you will also need to provide the primary cardholder’s identity verification details.
   - **Exact cardholder name** as printed on the card.
   - **Billing address** where the credit card statement is sent each month.
   - **Your home phone number.**
   - **Circumstances** of the loss or theft.
   - **Identity verification information:** Social Security number or similar, date of birth and mother’s maiden name.

2. After the card has been cancelled, request a free copy of your credit report and place a fraud alert on your credit reports. Fraud alerts can help prevent an identity thief from opening any more accounts in your name.

3. You may also want to consider additional protection with a credit freeze. A credit freeze will lock your credit report and prevent any information from being released to any institutions, including merchants and financial institutions.

CHECK FRAUD

Check fraud occurs when an identity thief steals or counterfeits checks. Criminals can easily create checks with just a checking account number and the bank routing number. Therefore, checking account numbers are just as valuable to criminals as credit card numbers and should be treated with similar care.

Demand drafts, also known as “remotely created checks,” are a system for cashing checks and have become an attractive target for criminals. They were designed to accommodate legitimate telemarketers who receive authorization from consumers to take money out of their checking accounts. They look just like checks, but indicate “signature not required” or a similar message in the authorized signature area. They require no action from the account holder.

In most states, consumers who complain about a bad demand draft within a reasonable amount of time are entitled to a refund from their bank. The liability for accepting a bad check falls to the account holder’s bank, called the paying bank. But the rules only give the bank 24 hours after receiving the check from the institution that cashed it to make a fraud determination. That makes the work of thieves easier since banks often don’t detect fraudulent demand drafts until a consumer complains, well after the 24-hour period.

Steps to Resolve Check Fraud or Lost Checks:

1. Contact your bank and ask to issue a “stop payment” on the checks as well as close the account. Your bank should notify the check verification service with which it does business. By doing this, retailers will be advised to reject those checks. Please note that you may be held responsible for the forgery if you fail to notify the bank in a timely manner that a check has been lost or stolen. For more information, please check the state banking regulations or the consumer protection agency. Most states hold the bank responsible for losses from such transactions. However, most states also require individuals to take reasonable care of their accounts.

2. Contact the major check verification companies to request that they notify retailers who use their databases not to accept your lost or stolen checks. Contact:
   - TeleCheck at 1-800-710-9898 or 1-800-927-0188
   - Certegy, Inc. (previously Equifax Check Systems) at 1-800-437-5120

3. If you wish to find out if the identity thief has been passing bad checks in your name, call SCAN (Shared Check Authorization Network) at 1-800-262-7771. SCAN can describe any negative check information that has been reported to the SCAN database for the member’s bank accounts and identification numbers.

4. As a precaution, obtain a check consumer report (one order per year is free of charge) by contacting either:
   - SCAN at 1-800-262-7771. The consumer report from SCAN will show a list of checks with the amount of each check, the check date, the name of the merchant and the contact information of that merchant. The report may also be ordered by fax or by mail.
   - Experian (formerly Chex Systems) at 1-800-428-9623 or fax at 602-659-2197. This report shows the details of each check transaction, the reason for denial, etc.
   - Certegy, Inc. at 1-800-437-5120 or by mail

5. Contact the merchant. If a merchant rejects your checks, it may be because an identity thief is using the Magnetic Information Character Recognition (MICR) code (the numbers at the bottom of checks), your driver’s license number or another identification number. The merchant who rejects the check should give you its check verification company contact information so you can find out what information the thief is using. If you find out that the thief is using your MICR code, ask your bank to close your checking account and open a new one. If you discover that the thief is using your driver’s license number or some other identification number, you need to work with your DMV or other identification-issuing agency to get new identification with new numbers.
BANKRUPTCY FRAUD

Steps to Resolve Bankruptcy Fraud:

1. Request a copy of your credit records to review for inaccuracies and confirmation of fraudulent bankruptcy.
2. File a police report.
3. Report the fraudulent bankruptcy filing to all three credit bureaus and place a fraud alert on your credit reports. Send the police report to the three credit bureaus, along with a letter detailing the situation. These bureaus are required to send the police report and the letter to any company requesting your credit information.
4. Write a letter with the problem to the U.S. Trustee in the region where the bankruptcy was filed. A listing of the U.S. Trustee Program's Regions can be found at www.usdoj.gov. The letter should describe the situation and provide proof of your identity. Provide as much information as possible including the affidavit and all information and documentation you may have on who is stealing your identity.

STUDENT LOAN FRAUD

Steps to Resolve Student Loan Fraud:

1. Contact the school or program that opened the student loan to close it.
2. Report the fraudulent loan to the U.S. Department of Education using one of the following sources:
   - Call the Inspector General's Hotline toll-free at 1-800-MIS-USED.
   - Write to the Office of Inspector General
     U.S. Department of Education
     400 Maryland Avenue SW
     Washington, DC 20202-1510

TAX FRAUD

An identity thief may file a tax return using your Social Security number to receive a refund. If the thief already filed a return using your Social Security number, the IRS will believe that you have already filed and received your refund, and the return you submit later is a second copy or duplicate.

Be alert to possible identity theft if the notice or letter states that more than one tax return for you was filed or that IRS records indicate you received wages from an employer unknown to you. Additionally, the IRS does not request personal taxpayer information through e-mail. If you receive this type of request, it may be an attempt from identity thieves to get your private tax information.

Steps to Resolve Tax Fraud:

1. If you receive a notice from the IRS that leads you to believe someone may have used your Social Security number fraudulently, notify the IRS immediately by responding to the name and number printed on the notice or letter.
2. If you have unresolved issues related to identity theft, or have suffered a significant hardship as a result of the administration of the tax laws, visit the IRS Taxpayer Advocate Service web site www.irs.gov/advocate/ or to call toll-free: 1-877-777-4778. IRS tax examiners will work with you and other agencies, such as the Social Security Administration, to help resolve the problem.

LOST OR STOLEN MEDICARE CARD

Steps to Take for Lost Medicare Card:

1. If the card that you need is issued by your state, please contact the Medicare office in your state of residence. You can locate the nearest Medicare office at www.cms.hhs.gov.
2. If not, you can request a replacement Medicare card online by visiting the Medicare Card Replacement section of the Social Security Administration’s Web site: www.ssa.gov. To make an online request, you will need the following information:
   - Your last (exact) payment amount or the month and year you last received a payment if you have received benefits in the last 12 months
   - Name as it appears on your most recent Social Security card
   - Your Social Security number
   - Your date of birth
   - Your phone number in case they need to contact you about the request
   - Your e-mail address (optional)
   - Your place of birth
   - Your mother’s maiden name (to help identify you)

The card will be mailed to the address that Social Security has on record within 30 days.

If you need proof immediately for your doctor or for a prescription, you can request a Medicare card in person at

The average consumer’s out-of-pocket cost due to identity fraud was $631 per incident in 2010.

— Javelin Strategy & Research, Identity Fraud Survey, 2/2011
You can request a replacement Medicare card over the phone by providing the same information required for the online procedure. To contact Social Security please call their toll-free number at 1-800-772-1213 (TTY option: 1-800-325-0778). Working hours are Monday through Friday from 7AM to 7PM.

3. Check your Medicare Summary Notices regularly to verify that you have received the services for which Medicare has paid. If you do not recognize a particular service, it does not necessarily mean that fraud has been committed. For example, it is possible that you have received the service, but the provider name or service description is unfamiliar. If you identify an erroneous charge on your Medicare Summary Notice, please call the number listed in the Customer Service Box in order to speak with the Medicare-contracted insurance company that processed the claim. A representative will be able to access your records via computer, and may be able to determine immediately whether the service charge represents a billing error, a misunderstanding on your part, or a potential instance of fraud. If you are unable to reach the Medicare contractor, you may also report the charge to the Inspector General’s Hotline at 1-800-HHS-TIPS (1-800-447-8477).

MEDICAL IDENTITY THEFT

Medical identity theft occurs when someone uses personal identifying information, without legal authority or consent to obtain medical services or goods, or to make false claims for medical services or goods. Medical identity theft frequently results in erroneous entries being put into existing medical records and can involve the creation of fictitious medical records in the victim’s name.

Medical identity thieves may change your medical and health insurance records. Every time a thief uses your identity to get care, a record is created with the imposter’s medical information that could be mistaken for your medical information – for example, a different blood type, an inaccurate history of drug or alcohol abuse, test results that aren’t yours, or a diagnosis of an illness, allergy or condition you don’t have. Any of these could lead to improper treatment, which in turn, could lead to injury, illness or worse.

You may be a victim of medical identity theft if:
- You have received medical, insurance or a collection bill for services, medicine and equipment you didn’t receive.
- You have received a description of medical benefits from the health insurance company or provider for services for medicine or equipment you didn’t receive.

- You have visited one of the medical providers and discovered that there is fraudulent information on your medical records.
- You have reviewed your credit records and found fraudulent collection notices for medical treatment you never received.

Unlike credit reports, there is no central source for your medical records. You need to contact each provider with whom you do business – including doctors, clinics, hospitals, pharmacies, laboratories and health plans – that is relevant to your experience.

Steps to Resolve Medical Identity Theft:

1. If you suspect you may be a victim of medical identity theft, contact your insurance company and ask for their fraud resolution department.
2. You also have rights under federal law that can assist you in correcting inaccurate medical records. These rights are described in greater detail at www.hhs.gov/ocr/hipaa including:
   - The right to request copies of your current medical files from each health care provider.
   - The right to have your medical records amended to remove inaccurate or incomplete information.
   - The right to an accounting of disclosures – a record of who has been given access to your medical records – from your health care providers and health insurers. This is very important in tracking down where inaccurate information may have been sent.
   - The right to file a complaint with the Office of Civil Rights at the federal Department of Health
EMPLOYMENT FRAUD

There are different types of employment fraud. The most common are immigrant identity theft and offers of fraudulent bonus for non-existent jobs.

Undocumented workers or other individuals may use someone else’s Social Security number to get a job. That person’s employer would report W-2 wages earned using the victim’s information to the IRS creating the appearance that the victim did not report all of his or her income on his or her tax return.

The Social Security Administration and the IRS are not required to notify you that something unusual is happening with your Social Security number. Most people only discover the situation when their impostors secure credit using the stolen number. And even then, the victims may not be told unless the impostor misses a loan payment.

Another employment-related scam is an “online job application” fraud scheme. Individuals have applied for and accepted jobs through an online job search service advertising “signing bonuses” for new hires. Each prospective employee receives a check ranging from $19,000 to $50,000 by mail from the prospective employer with instructions to deposit the check, preferably at an ATM. The recipient is further instructed to keep $2,000 to $4,000, depending upon the amount of the signing bonus, and return the balance of the money by wire. The checks are fraudulent; therefore, the depositor is ultimately responsible for any amounts charged back to his or her account by the bank resulting from the dishonor of the checks.

For more information, please see the Federal Deposit Insurance Corporation’s (FDIC) Special Alert at: http://www.fdic.gov/consumers/consumer/alerts.

Steps to Resolve Employment Fraud:

1. Notify the IRS by calling 1-800-829-3676 to order the IRS Affidavit (Form 14039) or online at http://www.irs.gov/pub/irs-pdf/f14039sp.pdf. The Form 14039 or a police report should be submitted to the IRS along with a copy of a state-issued identification card.

2. Request a Social Security earnings record to see if there are any indications that someone else may be using your Social Security number. You can get a copy of the earnings record by calling 1-800-772-1213 or by completing a Request for Social Security Statement (Form 7004) online at http://www.ssa.gov/online/ssa-7004.html.

3. If you suspect that someone else has claimed unemployment benefits using your Social Security number, then call the Social Security Fraud Hotline at 1-800-269-0271 to report it.

4. For more information, please see the following publications from the SSA:

   • Guidelines for reporting fraud: http://www.ssa.gov/oig/guidelin.htm
   • Your Social Security number and your card: http://www.ssa.gov/pubs/10002.html
   • Identity Theft and your Social Security number: http://www.ssa.gov/pubs/10064.html

CHILD IDENTITY THEFT

Child identity theft occurs when an impostor uses a child’s identity for personal gain. The perpetrator may be a family member, someone known by the family or a stranger. In some cases, a child’s relative finds out about the crime. In other cases, adults find out that their identity was stolen as a child. There are some cases that appear to be identity theft but are not. For example, if a parent opened a college fund for his or her child, he or she may receive some pre-approved credit card offers in the child’s name.

Signs of potential child identity theft include offers for credit for the child or other offers mailed to the home, or trouble opening bank accounts for the child. Also, strange identity-related questions when applying for schools or outside activities could be a tipoff. A bank or school might find that there are other identities linked to your child’s Social Security number during a routine check. It is important to note that a child is a minor and by law cannot enter into a contract.

Steps to Resolve Child Identity Theft:

1. TransUnion has the most parent-friendly process, with the only online application specifically for child inquiries, so this credit bureau is the best place to start. If TransUnion says
there is no report, odds are good that your child is in the clear, but if there is a report – or you have a specific reason to believe your child is a victim – you’ll want to follow up with the other two major credit bureaus – Experian and Equifax – and get a report from them as well.

2. Review the child’s credit report. If there is no credit report, then it may not be a case of financial identity theft. However, the fraudulent accounts may appear at a later time, so make sure to review your child’s credit report at least one more time. It’s important to note, however, that both the FTC and the Identity Theft Resource Center say parents should not check their kids’ credit reports on an annual basis.

3. For children between 14 to 18 years old, the process is different. If they have a report, it would be possible to get a credit report through http://www.annualcreditreport.com

4. If there are fraudulent accounts, then you need to obtain a copy of your child’s birth certificate to submit to creditors along with the *Identity Theft Affidavit Form* found in this kit.

5. If applicable, a fraud alert should be placed on child’s credit report. This will alert the other credit reporting agencies.

6. File a police report to create a history of this case.

7. The child’s Social Security earnings statement should be requested to check if the thief has used the child’s Social Security number to gain employment.


**MAIL FRAUD**

Sometimes thieves steal mail from someone’s mailbox or submit a false change-of-address order. When a change of address request is filed, post offices send a “Move Validation Letter” to both the old and new address. The letter requests the resident to call an 800 number if he or she did not file the change.

**Steps to Resolve Mail Fraud:**

File a mail fraud report with the U.S. Postal Inspection Service as follows:

- By mail at: Criminal Investigations Service Center
  ATTN: Mail Fraud
  222 S. Riverside Plaza Ste 1250
  Chicago IL 60606-6100

- Call your local Postal Inspector’s office. To find the nearest postal inspection station, visit www.usps.com.

- Submit a Mail Fraud Report online at www.usps.com.

If you suspect mail fraud by postal employees, you should send a complaint form to the U.S. Postal Inspection Service. Please follow instructions online at www.usps.com.

**TELEPHONE FRAUD**

Identity thieves may:

- Establish phone service in your name.
- Make unauthorized calls that are billed to your cellular phone.
- Use your calling card and PIN.

**Steps to Resolve Telephone Fraud:**

Contact your service provider immediately to cancel the account and/or calling card. You will need to open new accounts and choose new PINs. If you are having trouble getting fraudulent phone charges removed from your account or getting an unauthorized account closed, contact the appropriate agency from the list below:

For local service, contact your state Public Utility Commission, listed in the government section of your telephone directory or find them online: http://transition.fcc.gov/wcb/iad/stage_puc.html.

For cellular phones and long distance, contact the Federal Communications Commission (FCC) - www.fcc.gov. The FCC regulates interstate and international communications by radio, television, wire, satellite and cable. Call: 1-888-CALL-FCC; TTY: 1-888-TELL-FCC; or write to: Federal Communications Commission Consumer Information Bureau 445 12th Street, SW, Room S1063 Washington, DC 20554

You can also file complaints via the online complaint form at: www.fcc.gov or e-mail questions to fccinfo@fcc.gov

**ONLINE IDENTITY THEFT**

If you suspect fraudulent activity with your online accounts (eBay®, PayPal®, etc.) or with online purchases, verify which card or account was used for those activities and then follow the steps indicated in the Lost or Stolen Credit Card section.

**Steps to Resolve Unauthorized Access of Online Account(s):**

1. First, confirm with family members and others who may use your account that they did not make any changes.

2. Immediately notify the affected online account that there has been unauthorized use of your account.

3. Next, change the password to your personal e-mail account in case that has been compromised. The password should be alphanumeric and different from any other password.

4. Immediately after, request a new password for the affected online account and make sure you change the Secret Question and Answer on the affected online account.

5. Verify all personal contact information registered on the
affected online account and change any incorrect data.

6. Verify the activity on the account and dispute all fraudulent charges in writing by filling out the enclosed *Identity Theft Affidavit (part 2 of Form) found in this kit*

7. If you require additional assistance, contact the customer service department of the affected online account.

**SYNTHETIC IDENTITY THEFT**

Synthetic identity theft occurs when thieves use pieces of data from different victims to create new identities, such as one person’s name and another person’s Social Security number, rather than stealing just one person’s information and using it for fraud.

This form of identity theft is one of the least detected because banks and other financial organizations will file these accounts as “sub files.” These accounts never actually reach victims until substantial damage has been done and they are finally contacted by bill collectors for all the expenses incurred under their identity.

**Steps to Resolve Synthetic Identity Theft:**

Follow the steps provided in this kit that are relevant to your specific information that was stolen (e.g. if your Social Security number was stolen, follow the tips for Resolving Stolen Social Security number).

**AUTOMOBILE IDENTITY THEFT**

Identity theft does not apply only to individuals. There are many sophisticated criminals who steal the identity of someone’s car by using the car’s Vehicle Identification Number (VIN). They steal the legitimate VIN numbers from cars in parking lots, in gas stations or from car sales on the Internet. They then attach the numbers to stolen vehicles of the same model and offer them for sale or distribute them in different states. One car can be registered in two states at the same time as states do not automatically check registration details in other areas. Many cars with altered VINs are sold to other criminals and then turn up at auto auction houses and car dealerships. Cars are then sold to buyers who are unaware of the fraud.

This type of fraud is not detected until:

- An individual tries to register the vehicle and learns that there is a duplicate;
- An insurance company notices that a car has been insured twice simultaneously;
- The insurance crime bureau or the police discover that there are two or more vehicles with the same VIN registered in different places.

**Steps to Resolve Automobile Identity Theft:**

1. File a police report at the station closest to your home. This report will serve as proof of crime.
2. Place a fraud alert on your credit records and send the police report to the three credit bureaus, along with a letter detailing the situation. These agencies are required to send the police report and the letter to any company requesting your credit information.
3. Contact the local DMV office and report the incident.

---

*73% of US adults have been the victim of some kind of cybercrime.*

— Norton 2010 Cybercrime Report: The Human Impact
In 2002 the FTC released a tool to help victims of identity theft restore their good names. The Identity Theft Affidavit is a model form that can be used to report information to many companies, simplifying the process of alerting companies where a fraudulent account was opened in an identity theft victim’s name. Previously, victims of identity theft often had to fill out a separate reporting form for each fraudulent account opened by the identity thief. Developed by the FTC in conjunction with banks, credit grantors and consumer advocates, the Identity Theft Affidavit is accepted by participating credit issuers, retailers, banks and other financial institutions.

This affidavit has two parts:

- **Part One**, the Identity Theft Affidavit is where you report general information about yourself and the theft.
- **Part Two**, the Fraudulent Account Statement is where you describe the fraudulent account(s) opened in your name. Use a separate Fraudulent Account Statement for each company you need to write to.

**INSTRUCTIONS FOR COMPLETING THE IDENTITY THEFT AFFIDAVIT**

To make certain that you do not become responsible for any debts incurred by an identity thief, you must prove to each of the companies where accounts were opened or used in your name that you didn’t create the debt. While many companies accept this affidavit, others require that you submit more or different forms.

1. Before you send the Identity Theft Affidavit, contact each company to find out if they accept it. It will be necessary to provide the information in this affidavit anywhere a new account was opened in your name.

   The information will enable the companies to investigate the fraud and decide the outcome of your claim. If someone made unauthorized charges to an existing account, call the company for instructions.

2. When you send the affidavit to the companies, attach copies (NOT originals) of any supporting documents (for example, driver’s license or police report). Before submitting your affidavit, review the disputed account(s) with family members or friends who may have information about the account(s) or access to them.

3. Complete this affidavit as soon as possible. Many creditors ask that you send it within two weeks. Delays on your part could slow the investigation. Be as accurate and complete as possible and print clearly.

   You may choose not to provide some of the information requested. However, incorrect or incomplete information will slow the process of investigating your claim and absolving you of the debt.

4. Make a copy of everything you submit.

5. When you have finished completing the affidavit, mail a copy to each creditor, bank or company that provided the thief with the unauthorized credit, goods or services you describe. Attach a copy of the Fraudulent Account Statement with information only on accounts opened at the institution to which you are sending the packet, as well as any other supporting documentation you are able to provide.

   Send the appropriate documents to each company by certified mail, return receipt requested, so you can prove that it was received. The companies will review your claim and send you a written response telling you the outcome of their investigation.

If you are unable to complete the affidavit, a legal guardian or someone with power of attorney may complete it for you. Except as noted, the information you provide will be used only by the company to process your affidavit, investigate the events you report and help stop further fraud. If this affidavit is requested in a lawsuit, the company might have to provide it to the requesting party.

Completing this affidavit does not guarantee that the identity thief will be prosecuted or that the debt will be cleared.
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: ______________________________________

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: _____________________________________

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

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

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

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

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):

________________________________________________________________
________________________________________________________________
________________________________________________________________
________________________________________________________________
________________________________________________________________
________________________________________________________________

(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).

(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.

<table>
<thead>
<tr>
<th>Name of Institution</th>
<th>Contact Person</th>
<th>Phone</th>
<th>Extension</th>
<th>Account Number</th>
<th>Routing Number</th>
<th>Affected Check Number(s)</th>
<th>Account Type:</th>
<th>Select ONE:</th>
<th>Date Opened or Misused (mm/yyyy)</th>
<th>Date Discovered (mm/yyyy)</th>
<th>Total Amount Obtained ($)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Credit</td>
<td>This account was opened fraudulently.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Bank</td>
<td>This was an existing account that someone tampered with.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Phone/Utilities</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Loan</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Government Benefits</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Internet or Email</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Other</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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.

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
Sample Letter For Dispute Of Fraudulent Charges

Your name
Your address
Your phone

Company’s name
Company’s address
Company’s fax
Company’s e-mail
Dear Sir or Madam (or name of the person you spoke to):

Following our phone conversation please find attached my ID Theft Affidavit. Please note that I am writing to dispute the following information in my file for account/credit card number_____________________. The items I want to dispute are also circled on the attached copies of the documents I received. (Identify item(s) disputed by name of source, such as creditors or tax court, and identify type of item, such as credit account, judgment, etc. Use Fraudulent Account Statement of the ID Theft Affidavit).

This item is (inaccurate or incomplete) because (describe what is inaccurate or incomplete and why). I am requesting that the item be deleted (or request another specific change) to correct the information.

Enclosed are copies of (use this sentence if applicable and describe any enclosed documentation, such as payment records, court documents) supporting my position. Please reinvestigate this (these) matter(s) and (delete or correct) the disputed item(s) as soon as possible.

Sincerely,

Your name