334.834.1500 | www.HatTeam.com

SANDRANICKEL
HAT TEAM, REALTORS®

Identity Theft

Prevention and Response Manual

www.TheCreditRoadMap.com and

Courtesy of
The CREDIT Road Map

A practical guide for navigating your way to good credit

by PATRICK RITCHIE

Sandra Nickel
ABR, CRS, SRES
Sandra@hatteam.com

1-800-HATLADY
(1-800-428-5239)
office 334-834-1500
fax 334-269-4083
1044 E Fairview
Montgomery AL 36106

Identity theft has become a crime that affects 9 million Americans from all walks of life each year. The average victim spends 175 hours trying to combat the effects of identity theft. I have compiled a response manual to help people save themselves the time of researching exactly what to do if they ever were to become a victim. Save this packet, hopefully you will never need it. But just like a fire extinguisher, keep it handy in case the need ever arises. I suggest putting it in a kitchen drawer or a filing cabinet.

When it comes to identity theft you have to move quickly. Your emotions will be running high, and unfortunately remedying the situation can be confusing. Follow the steps in this manual. Seek the advice and recommendations of the individual creditors involved in the theft - they may have internal procedures you will want to be aware of.

If you don't already have a copy of your credit report I advise you to get a copy right now. After reviewing it place the report in a safe place, such as a safety deposit box. The reason for this is that you will have a record of what your credit history looks like now; giving you a map of where you need to get back to if the worst case scenario happens in an ID theft situation. I also advise you to photocopy the front and back of everything in your wallet. Place this with your credit report so in the event your wallet is ever lost or stolen you will have the contact numbers on the back of your credit cards and you will know what items were lost.

Preventative measures are the key to avoiding ID theft, so you will find a section in this manual dedicated to preventing ID theft from occurring in the first place. Take as many precautions as you can. However, some circumstances are out of our personal control. One example would be a security breach where a computer system containing our personal information is infiltrated. Check out the preventative measures detailed in this manual so you can do your best to avoid ID theft happening to you.

Sincerely,

Patrick Ritchie
Author, *The Credit Road Map*

P.S. My book *The Credit Road Map* can be ordered through my website at www.TheCreditRoadMap.com either by credit card or by check with the downloadable order form. There is also a DVD of my class on credit available for purchase on the website. The book can also be found on www.Amazon.com or at www.REALTOR.org on the Real Estate Bookshelf. Orders of 5 or more books qualify for discount pricing; email me at Patrick@TheCreditRoadMap.com for details. There are free articles and reports available on my website for you to view.

I. Preventing Identity Theft ……..**3**
II. How Do Thieves Steal an Identity? ……..**3**
III. Steps for Identity Theft Victims ……**4**
a. Notify all businesses involved in the theft/fraud ……...**4**
b. File a police report ……**5**
c. Place a fraud alert on your credit report ……**6**
d. Submit an ID theft affidavit/report to all creditors involved ….**7**
e. File an online complaint with the Federal Trade Commission ..**8**
IV. Credit Bureau Obligations ……..**9**
V. Information Provider (creditor) Obligations ……...**9**
VI. Misc. ID Theft Situations
a. Should I apply for a new Social Security number? ……**9**
b. What do thieves do with a stolen identity? ……**10**
c. How can you find out if your identity was stolen? ……**10**
d. How long can the effects of identity theft last? ……**11**
e. Bank Accounts and Fraudulent Withdrawals ……**11**
f. Fraudulent Electronic Withdrawals ……...**11**
g. Fraudulent Checks and Other "Paper" Transactions ……..**12**
h. Fraudulent New Accounts ……..**13**
i. Bankruptcy Fraud ……...**13**
j. Correcting Fraudulent Information in Credit Reports ……**13**
k. Credit Cards ……**14**
l. Criminal Violations ……**14**
m. Debt Collectors ……**15**
n. Driver's License ……...**15**
o. Mail Theft ……**16**
p. Medical Identity Theft ……**16**
q. Passport Fraud ……**16**
r. Phone Fraud ……**16**
s. Social Security Number Misuse ……...**17**
t. Student Loans ……...**17**
u. Tax Fraud ……..**17**
v. What if I'm still having problems? ……...**17**
VII. Sample Letters
a. Request for Fraudulent Transaction/Account Information ……...**18**
b. Dispute Letter for Existing Accounts ……...**18**
c. Dispute Letter for New Accounts ……..**19**
d. Blocking Letter Credit Bureaus ……**19**
VIII. Federal Trade Commission ID Theft Affidavit Instructions ……..**20**
IX. FCRA 609(e) (15 U.S.C. § 1681g(e)) Disclosures to Consumers - Information Available to Victims ……...**27**

Preventing Identity Theft

- Don't give out personal information on the phone, through the mail or over the Internet unless you've initiated the contact
- Never carry your social security card on anything you could lose such as a purse or wallet
- Deposit outgoing mail in post office collection boxes or at your local post office, rather than in an unsecured mailbox. Promptly remove mail from your mailbox. 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.
- To thwart an identity thief who may pick through your trash or recycling bins to capture your personal information, 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. If you do not use the pre-screened credit card offers you receive in the mail, you can opt out by calling 1-888-5-OPTOUT (1-888-567-8688) or go to www.optoutprescreen.com. Please note that you will be asked for your Social Security number in order for the credit bureaus to identify your file so that they can remove you from their lists and you still may receive some credit offers because some companies use different lists from the credit bureaus' lists.
- Carry only the identification information and the number of credit and debit cards that you'll actually need.
- Ask about information security procedures in your workplace or at businesses, doctor's offices or other institutions that collect personally identifying information from you.
- Give your SSN only when absolutely necessary. Ask to use other types of identifiers when possible. If your state uses your SSN as your driver's license number, ask to substitute another number. Do the same if your health insurance company uses your SSN as your account number.
- Pay attention to your billing cycles. Follow up with creditors if your bills don't arrive on time. A missing bill could mean an identity thief has taken over your account and changed your billing address to cover his tracks.
- Be wary of promotional scams. Identity thieves may use phony offers to get you to give them your personal information
- Pick up a copy of *The Credit Road Map* for a more in depth look at preventing ID theft

How do thieves steal an identity?

Identity theft starts with the misuse of your personally identifying information such as your name and Social Security number, credit card numbers, or other financial account information. For identity thieves, this information is as good as gold.
Skilled identity thieves may use a variety of methods to get hold of your information, including:

1. **Dumpster Diving.** They rummage through trash looking for bills or other paper with your personal information on it.
2. **Skimming.** They steal credit/debit card numbers by using a special storage device when processing your card.
3. **Phishing.** They pretend to be financial institutions or companies and send spam or pop-up messages to get you to reveal your personal information.
4. **Changing Your Address.** They divert your billing statements to another location by completing a change of address form.
5. **Old-Fashioned Stealing**. They steal wallets and purses; mail, including bank and credit card statements; pre-approved credit offers; and new checks or tax information. They steal personnel records, or bribe employees who have access.
6. **Pretexting.** They use false pretenses to obtain your personal information from financial institutions, telephone companies, and other sources.

Introduction

When it comes to identity theft you have to create as much evidence as possible. View it as going into a courtroom to defend yourself; you want to have as much evidence as possible to prove your innocence. Filing police reports, filling out the FTC ID theft complaint form, submitting an affidavit to creditors, saving all correspondence, along with tracking your actions and who you spoke to will create the evidence you need to prove you were a victim, not a perpetrator. Look at it this way: 5 years down the road if a potential creditor or employer (yes, employers may want to look at your credit during the interviewing process or when you are up for promotion) asks you to explain and document a derogatory account that stemmed from an ID theft, will you be prepared? Will they just have to 'take your word' for it? Don't place yourself in the position to be presumed guilty (because it is not innocent until proven guilty in this arena), build your case, and protect your credit along with your sanity.

Notify all businesses involved (even potentially) in the theft/fraud

Call and speak with someone in the security or fraud department of each company. Follow up in writing (see sample letters, request mailing address), and include copies (NOT originals) of supporting documents. It is important to notify credit card companies and banks in writing. Send your letters by certified mail, return receipt requested, so you can document what the company received and when. Keep a file of your correspondence and enclosures.

When you open new accounts, use new Personal Identification Numbers (PINs) and passwords. Avoid using easily available information like your mother's maiden name, your birth date, the last four digits of your Social Security number or your phone number, or a series of consecutive numbers.

If the identity thief has made charges or debits on your accounts, or has fraudulently opened accounts, ask the company for the forms to dispute those transactions:

- For charges and debits on existing accounts, ask the representative to send you the company's fraud dispute forms. If the company doesn't have special forms, use the sample letter to dispute the fraudulent charges or debits. In either case, write to the company at the address given for "billing inquiries," NOT the address for sending your payments.
    - Use the FTC affidavit at the back of this manual if the company does not have its own form.
- For new unauthorized accounts, you should file a dispute directly with the company AND file a report with the police (since you are not a customer you may not be treated well by the company). Provide a copy of the police report to the company.
    - If the company has already reported these unauthorized accounts or debts on your credit report, an Identity Theft Report from the police will require them to stop reporting that fraudulent information.

Once you have resolved your identity theft dispute with the company, ask for a letter stating that the company has closed the disputed accounts and has discharged the

fraudulent debts. This letter is your best proof if errors relating to this account reappear on your credit report or you are contacted again about the fraudulent debt.

File a police report

Call your local police department and tell them that you want to file a report about your identity theft. Ask them if you can file the report in person. If you cannot, ask if you can file a report over the internet or telephone. See below for information about Automated Reports.
If the police are reluctant to take your report, ask to file a "Miscellaneous Incident" report, or try another jurisdiction, like your state police. You also can check with your state Attorney General's office to find out if state law requires the police to take reports for identity theft.

Be aware that you may have to file the police report in the jurisdiction of the crime. This can get tricky if the crime occurred online, be diligent and do not be afraid to try every department in a jurisdiction until one takes the report. The good news is that most law enforcement agencies are now fully aware of the ramifications of ID theft; some even have detectives specifically assigned to investigate ID theft. Filing a police report not only helps you, but it can help lead authorities to busting up ID theft rings by tracking patterns and matching up similar crimes. In one case every victim in a string of ID crimes shared the same doctor. When the police spoke to the doctor it was discovered that the computer technician hired by the doctor had been stealing social security numbers of patients and selling them to thieves.

Ask the officer to attach or incorporate the ID Theft Complaint (anything you have filed with the company or the complaint filed with the FTC online) into their police report. Tell them that you need a copy of the Identity Theft Report (the police report with your ID Theft Complaint attached or incorporated) to dispute the fraudulent accounts and debts created by the identity thief. (In some jurisdictions the officer will not be able to give you a copy of the official police report, but should be able to sign your Complaint and write the police report number in the “Law Enforcement Report” section.)

What do I do if the police only take reports about identity theft over the Internet or telephone?

The FTC ID Theft Complaint has a special section for police reports that are not filed face-to-face, to help you use it to supplement an automated police report. If you file a police report online or over the phone, complete the “Automated Report Information” block of the ID Theft Complaint. Attach a copy of any filing confirmation received from the police.

If you have a choice, however, you should file your police report in person and not use an automated report. It is more difficult for the consumer reporting company and information provider to verify the information in an automated report, and they will likely require additional information and/or documentation.

What do I do if the local police won't take a report?

There are efforts at the federal, state and local level to ensure that local law enforcement agencies understand identity theft, its impact on victims, and the importance of taking a police report.

However, we still hear that some departments are not taking reports. The following tips may help you to get a report if you're having difficulties:

- 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 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.
- If you're told that identity theft is not a crime under your state law, ask to file a Miscellaneous Incident Report instead.
- If you can't get the local police to take a report, try your county sheriff. If that doesn't work, try your state police. Beyond the state police try the state attorney general office or the FBI.

Some states require the police to take reports for identity theft. Check with the office of your State Attorney General, which can be found at www.naag.org, to find out if your state has this law.

How do I prove that I'm an identity theft victim?

Applications or other transaction records related to the theft of your identity may help you prove that you are a victim. For example, you may be able to show that the signature on an application is not yours. These documents also may contain information about the identity thief that is valuable to law enforcement. By law, companies must give you a copy of the application or other business transaction records relating to your identity theft if you submit your request in writing, accompanied by a police report.

Place a fraud alert on your credit report

Fraud alerts can help prevent an identity thief from opening any more accounts in your name. Contact the toll-free fraud number of any of the three consumer reporting companies below to place a fraud alert on your credit report. You only need to contact one of the three companies to place an alert. The company you call is required to contact the other two, which will place an alert on their versions of your report, too. If you do not receive a confirmation from a company, you should contact that company directly to place a fraud alert.

Equifax: 1-800-525-6285; www.equifax.com; P.O. Box 740241, Atlanta, GA 30374-0241

Experian: 1-888-EXPERIAN (397-3742); www.experian.com; P.O. Box 9532, Allen, TX 75013

TransUnion: 1-800-680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790

Once you place the fraud alert in your file, you're entitled to order one free copy of your credit report from each of the three consumer reporting companies, and, if you ask, only the last four digits of your Social Security number will appear on your credit reports. Once you get your credit reports, review them carefully. Look for inquiries from companies you haven't contacted, accounts you didn't open, and debts on your accounts that you can't explain. Check that information, like your Social Security number, address(es), name or initials, and employers are correct. If you find fraudulent or inaccurate information, get it removed.

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

- **An initial alert stays on your credit report for at least 90 days.** You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial alert is appropriate if your wallet has been stolen or if you've been taken in by a "phishing" scam. When you place an initial fraud alert on your credit report, you're entitled to order one free credit report from each of the three nationwide consumer reporting companies, and, if you ask, only the last four digits of your Social Security number will appear on your credit reports.
- **An extended alert stays on your credit report for seven years.** You can have an extended alert placed on your credit report if you've been a victim of identity theft and you provide the consumer reporting company with an Identity Theft Report. An automated Identity Theft Report, such as the printed ID Theft Complaint available from this Web site, should be sufficient to obtain an extended fraud alert. When you place an extended alert on your credit report, you're entitled to two free credit reports within twelve months from each of the three nationwide consumer reporting companies. In addition, the consumer reporting companies will remove your name from marketing lists for pre-screened credit offers for five years unless you ask them to put your name back on the list before then.

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

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

Here is the reality about a fraud alert: ***it is not a strong approach to thwarting future ID theft.*** *Your credit report is still accessible and an experienced thief will be able to easily create a state ID with his or her picture in your name. The best method is to 'freeze' your credit report. Currently 25 states have this law on the books, so half of the country does not have this safeguard available to use. It is time to tighten up the ID theft laws, follow this link to tell your representative to help Americans protect their identity:* https://www.uspirg.org/action/financial-privacy/call-to-stop-identity-theft.

Continue to check your credit reports periodically, especially for the first year after you discover the identity theft, to make sure no new fraudulent activity has occurred.

Submit an ID theft affidavit/report to all creditors involved

What is an Identity Theft Report?
An Identity Theft Report can be used to permanently block fraudulent information from appearing on your credit report. An Identity Theft Report will also make sure these debts do not reappear on your credit report. An Identity Theft Report can prevent a company from continuing to collect debts that result from identity theft, or selling them to others for collection. It's also needed to place an extended fraud alert on your credit report.

Creating an Identity Theft Report may require two steps:

Step One is obtaining a copy of a report filed with a local, state, or federal law enforcement agency, like your local police department, your State Attorney General, the FBI, the U.S. Secret Service, the FTC, or the U.S. Postal Inspection Service. There is no federal law requiring a federal agency to take a report about identity theft; however, some state laws require local police departments to take reports. The law requires the report to provide as much information as you can about the crime, including anything you know about the dates of the identity theft, the fraudulent accounts opened and the alleged identity thief. If you do not provide detailed information, it may be impossible for consumer reporting companies and creditors to comply with your requests. It is suggested that you file an online complaint form with the FTC, and then ask your local police department to incorporate a copy of the printed ID Theft Complaint into the police report. By following this procedure, the consumer reporting company and the information provider may require less additional information and/or documentation under Step Two, below.

Step Two of an Identity Theft Report depends on the policies of the consumer reporting company and the information provider (the business that sent the information to the consumer reporting company). That is, they may ask you to provide information or documentation in addition to that included in the law enforcement report which is reasonably intended to verify your identity theft. They must make their request within 15 days of receiving your law enforcement report, or, if you already obtained an extended fraud alert on your credit report, the date you submit your request to the credit reporting company for information blocking. The consumer reporting company and information provider then have 15 more days to work with you to make sure your Identity Theft Report contains everything they need. They are entitled to take five days to review any information you give them. For example, if you give them information 11 days after they request it, they do not have to make a final decision until 16 days after they asked you for that information. If you give them any information after the 15-day deadline, they can reject your Identity Theft Report as incomplete; you will have to resubmit your Identity Theft Report with the correct information.

You may find that most federal and state agencies, and some local police departments, offer only 'automated' reports, reports that do not require a face-to-face meeting with a law enforcement officer. Automated reports may be submitted online, or by telephone or mail. If you have a choice, do not use an automated report. The reason? It's more difficult for the consumer reporting company or information provider to verify the information. Unless you are asking a consumer reporting company to place an extended fraud alert on your credit report, if you use an automated report the consumer reporting company or information provider will probably ask you to provide additional information or documentation.

File an online complaint with the Federal Trade Commission

You can file a complaint with the FTC using the online complaint form available at www.ftc.gov; or call the FTC's Identity Theft Hotline, toll-free: 1-877-ID-THEFT (438-4338); TTY: 1-866-653-4261; or write Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Be sure to call the Hotline to update your complaint if you have any additional information or problems.

By sharing your identity theft complaint with the FTC, you will provide important information that can help law enforcement officials across the nation track down identity thieves and stop

them. The FTC can refer victims' complaints to other government agencies and companies for further action, as well as investigate companies for violations of laws the agency enforces.

Additionally, you can provide a printed copy of your online Complaint form to the police to incorporate into their police report. The printed FTC ID Theft Complaint, in conjunction with the police report, can constitute an Identity Theft Report and entitle you to certain protections. This Identity Theft Report can be used to (1) permanently block fraudulent information from appearing on your credit report; (2) ensure that debts do not reappear on your credit report; (3) prevent a company from continuing to collect debts that result from identity theft; and (4) place an extended fraud alert on your credit report.

Credit Bureau Obligations

Consumer reporting companies will block fraudulent information from appearing on your credit report if you take the following steps: Send them a copy of an Identity Theft Report and a letter (see sample letter) telling them what information is fraudulent. The letter also should state that the information does not relate to any transaction that you made or authorized. In addition, provide proof of your identity that may include your Social Security number, name, address, and other personal information requested by the consumer reporting company.

The consumer reporting company has four business days to block the fraudulent information after accepting your identity theft report. It also must tell the information provider that it has blocked the information. The consumer reporting company may refuse to block the information or remove the block if, for example, you have not told the truth about your identity theft. If the consumer reporting company removes the block or refuses to place the block, it must let you know.

The blocking process is only one way for identity theft victims to deal with fraudulent information. There's also the "reinvestigation process," which was designed to help all consumers dispute errors or inaccuracies on their credit reports.

Information Provider (Creditor) Obligations

Information providers stop reporting fraudulent information to the consumer reporting companies once you send them an Identity Theft Report and a letter explaining that the information that they're reporting resulted from identity theft. But you must send your Identity Theft Report and letter to the address specified by the information provider. Note that the information provider may continue to report the information if it later learns that the information does not result from identity theft.

Any consumer reporting company that has accepted your Identity Theft Report is obligated to notify the information provider about the block. If a consumer reporting company tells an information provider that it has blocked fraudulent information in your credit report, the information provider may not continue to report that information to the consumer reporting company. The information provider also may not collect the debt that relates to the fraudulent account, or sell that debt to anyone else who would try to collect it.

Should I apply for a new Social Security number?

Under certain circumstances, the Social Security Administration may issue you a new Social Security number - at your request - if, after trying to resolve the problems brought on by identity theft, you continue to experience problems. Consider this option carefully. A new Social Security

number may not resolve your identity theft problems, and may actually create new problems. For example, a new Social Security number does not necessarily ensure a new credit record because credit bureaus may combine the credit records from your old Social Security number with those from your new Social Security number. Even when the old credit information is not associated with your new Social Security number, the absence of any credit history under your new Social Security number may make it more difficult for you to get credit. And finally, there's no guarantee that a new Social Security number wouldn't also be misused by an identity thief.

What do thieves do with a stolen identity?

Once they have your personal information, identity thieves use it in a variety of ways.
Credit card fraud:

- They may open new credit card accounts in your name. When they use the cards and don't pay the bills, the delinquent accounts appear on your credit report.
- They may change the billing address on your credit card so that you no longer receive bills, and then run up charges on your account. Because your bills are now sent to a different address, it may be some time before you realize there's a problem.

Phone or utilities fraud:

- They may open a new phone or wireless account in your name, or run up charges on your existing account.
- They may use your name to get utility services like electricity, heating, or cable TV.

Bank/finance fraud:

- They may create counterfeit checks using your name or account number.
- They may open a bank account in your name and write bad checks.
- They may clone your ATM or debit card and make electronic withdrawals your name, draining your accounts.
- They may take out a loan in your name.

Government documents fraud:

- They may get a driver's license or official ID card issued in your name but with their picture.
- They may use your name and Social Security number to get government benefits.
- They may file a fraudulent tax return using your information.

Other fraud:

- They may get a job using your Social Security number.
- They may rent a house or get medical services using your name.
- They may give your personal information to police during an arrest. If they don't show up for their court date, a warrant for arrest is issued in your name.

How can you find out if your identity was stolen?

The best way to find out is to monitor your accounts and bank statements each month, and check your credit report on a regular basis.

Unfortunately, many consumers learn that their identity has been stolen after some damage has been done.

- You may find out when bill collection agencies contact you for overdue debts you never incurred.
- You may find out when you apply for a mortgage or car loan and learn that problems with your credit history are holding up the loan.

- You may find out when you get something in the mail about an apartment you never rented, a house you never bought, or a job you never held.

How long can the effects of identity theft last?

It's difficult to predict how long the effects of identity theft may linger. That's because it depends on many factors including the type of theft, whether the thief sold or passed your information on to other thieves, whether the thief is caught, and problems related to correcting your credit report.

Victims of identity theft should monitor financial records for several months after they discover the crime. Victims should review their credit reports once every three months in the first year of the theft, and once a year thereafter. Stay alert for other signs of identity theft.

Don't delay in correcting your records and contacting all companies that opened fraudulent accounts. Make the initial contact by phone, even though you will normally need to follow up in writing. The longer the inaccurate information goes uncorrected, the longer it will take to resolve the problem.

Bank Accounts and Fraudulent Withdrawals

Different laws determine your legal remedies based on the type of bank fraud you have suffered. For example, state laws protect you against fraud committed by a thief using paper documents, like stolen or counterfeit checks. But if the thief used an electronic fund transfer, federal law applies. Many transactions may seem to be processed electronically but are still considered "paper" transactions. If you're not sure what type of transaction the thief used to commit the fraud, ask the financial institution that processed the transaction.

Fraudulent Electronic Withdrawals

The Electronic Fund Transfer Act provides consumer protections for transactions involving an ATM or debit card, or another electronic way to debit or credit an account. It also limits your liability for unauthorized electronic fund transfers. You have 60 days from the date your bank account statement is sent to you to report in writing any money withdrawn from your account without your permission. This includes instances when your ATM or debit card is "skimmed"- that is, when a thief captures your account number and PIN without your card having been lost or stolen.

If your ATM or debit card is lost or stolen, report it immediately because the amount you can be held responsible for depends on how quickly you report the loss:

- If you report the loss or theft within two business days of discovery, your losses are limited to $50.
- If you report the loss or theft after two business days, but within 60 days after the unauthorized electronic fund transfer appears on your statement, you could lose up to $500 of what the thief withdraws.
- If you wait more than 60 days to report the loss or theft, you could lose all the money that was taken from your account after the end of the 60 days.

Note: VISA and MasterCard voluntarily have agreed to limit consumers' liability for unauthorized use of their debit cards in most instances to $50 per card, no matter how much time has elapsed since the discovery of the loss or theft of the card.

The best way to protect yourself in the event of an error or fraudulent transaction is to call the financial institution and follow up in writing by certified letter, return receipt requested so you can prove when the institution received your letter. Keep a copy of the letter you send for your records.

After receiving your notification about an error on your statement, the institution generally has 10 business days to investigate. The institution must tell you the results of its investigation within three business days after completing it and must correct an error within one business day after determining that it occurred. If the institution needs more time, it may take up to 45 days to complete the investigation but only if the money in dispute is returned to your account and you are notified promptly of the credit. At the end of the investigation, if no error has been found, the institution may take the money back if it sends you a written explanation.

Fraudulent Checks and Other "Paper" Transactions

In general, if an identity thief steals your checks or counterfeits checks from your existing bank account, stop payment, close the account, and ask your bank to notify Chex Systems, Inc. or the check verification service with which it does business. That way, retailers can be notified not to accept these checks. While no federal law limits your losses if someone uses your checks with a forged signature, or uses another type of "paper" transaction such as a demand draft, state laws may protect you. Most states hold the bank responsible for losses from such transactions. At the same time, most states require you to take reasonable care of your account. For example, you may be held responsible for the forgery if you fail to notify the bank in a timely manner that a check was lost or stolen. Contact your state banking or consumer protection agency for more information.

You can contact major check verification companies directly for the following services:

To request that they notify retailers who use their databases not to accept your checks, call:

- TeleCheck at 1-800-710-9898 or 1-800-927-0188
- Certegy, Inc. (previously Equifax Check Systems) at 1-800-437-5120

To find out if the identity thief has been passing bad checks in your name, call:

- SCAN: 1-800-262-7771

If your checks are rejected by a merchant, 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 your check should give you its check verification company contact information so you can find out what information the thief is using. If you find 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, work with your DMV or other identification issuing agency to get new identification with new numbers. Once you have taken the appropriate steps, your checks should be accepted.

Note:

- The check verification company may or may not remove the information about the MICR code or the driver's license/identification number from its database because this information may help prevent the thief from continuing to commit fraud.

- If the checks are being passed on a new account, contact the bank to close the account. Also contact Chex Systems, Inc. to review your consumer report to make sure that no other bank accounts have been opened in your name.
- Dispute any bad checks passed in your name with merchants so they don't start any collections actions against you.

Fraudulent New Accounts

If you have trouble opening a new checking account, it may be because an identity thief has been opening accounts in your name. Chex Systems, Inc. produces consumer reports specifically about checking accounts, and as a consumer reporting company, is subject to the Fair Credit Reporting Act. You can request a free copy of your consumer report by contacting Chex Systems, Inc. If you find inaccurate information on your consumer report, follow the procedures under Correcting Fraudulent Information in Credit Reports to dispute it. Contact each of the banks where account inquiries were made, too. This will help ensure that any fraudulently opened accounts are closed.

Chex Systems, Inc.: 1-800-428-9623; www.chexhelp.com
Fax: 602-659-2197
Chex Systems, Inc.
Attn: Consumer Relations
7805 Hudson Road, Suite 100
Woodbury, MN 55125

Bankruptcy Fraud

If you believe someone has filed for bankruptcy in your name, write to the U.S. Trustee in the region where the bankruptcy was filed. A list of the U.S. Trustee Programs' Regional Offices is available at www.usdoj.gov/ust, or check the Blue Pages of your phone book under U.S. Government Bankruptcy Administration.

In your letter, describe the situation and provide proof of your identity. The U.S. Trustee will make a criminal referral to law enforcement authorities if you provide appropriate documentation to substantiate your claim. You also may want to file a complaint with the U.S. Attorney and/or the FBI in the city where the bankruptcy was filed. The U.S. Trustee does not provide legal representation, legal advice, or referrals to lawyers. That means you may need to hire an attorney to help convince the bankruptcy court that the filing is fraudulent. The U.S. Trustee does not provide consumers with copies of court documents. You can get them from the bankruptcy clerk's office for a fee.

Correcting Fraudulent Information in Credit Reports

The Fair Credit Reporting Act (FCRA) establishes procedures for correcting fraudulent information on your credit report and requires that your report be made available only for certain legitimate business needs.

Under the FCRA, both the consumer reporting company and the information provider (the business that sent the information to the consumer reporting company), such as a bank or credit card company, are responsible for correcting fraudulent information in your report. To protect your rights under the law, contact both the consumer reporting company and the information provider.

Credit Cards

The Fair Credit Billing Act establishes procedures for resolving billing errors on your credit card accounts, including fraudulent charges on your accounts. The law also limits your liability for unauthorized credit card charges to $50 per card. To take advantage of the law's consumer protections, you **must**:

- Write to the creditor at the address given for "billing inquiries," NOT the address for sending your payments. Include your name, address, account number, and a description of the billing error, including the amount and date of the error. See Sample Dispute Letter for Existing Accounts.
- Send your letter so that it reaches the creditor within 60 days after the first bill containing the error that was mailed to you. If an identity thief changed the address on your account and you didn't receive the bill, your dispute letter still must reach the creditor within 60 days of when the creditor would have mailed the bill. This is one reason it's essential to keep track of your billing statements, and follow up quickly if your bills don't arrive on time.

You should send your letter by certified mail, and request a return receipt. It becomes your proof of the date the creditor received the letter. Include copies (NOT originals) of your police report or other documents that support your position. Keep a copy of your dispute letter.

The creditor must acknowledge your complaint in writing within 30 days after receiving it, unless the problem has been resolved. The creditor must resolve the dispute within two billing cycles (but not more than 90 days) after receiving your letter.

Criminal Violations

Procedures to correct your record within criminal justice databases can vary from state to state, and even from county to county. Some states have enacted laws with special procedures for identity theft victims to follow to clear their names. You should check with the office of your state Attorney General, but you can use the following information as a general guide.

If wrongful criminal violations are attributed to your name, contact the police or sheriff's department that originally arrested the person using your identity, or the court agency that issued the warrant for the arrest. File an impersonation report with the police/sheriff's department or the court, and confirm your identity: Ask the police department to take a full set of your fingerprints, photograph you, and make copies of your photo identification documents, like your driver's license, passport, or travel visa. To establish your innocence, ask the police to compare the prints and photographs with those of the imposter.

If the arrest warrant is from a state or county other than where you live, ask your local police department to send the impersonation report to the police department in the jurisdiction where the arrest warrant, traffic citation, or criminal conviction originated.

The law enforcement agency should then recall any warrants and issue a "clearance letter" or "certificate of release" (if you were arrested/booked). You'll need to keep this document with you at all times in case you're wrongly arrested again. Ask the law enforcement agency to file the record of the follow-up investigation establishing your innocence with the district attorney's (D.A.) office and/or court where the crime took place. This will result in an amended complaint. Once your name is recorded in a criminal database, it's unlikely that it will be completely

removed from the official record. Ask that the "key name" or "primary name" be changed from your name to the imposter's name (or to "John Doe" if the imposter's true identity is not known), with your name noted as an alias.

You'll also want to clear your name in the court records. To do so, you'll need to determine which state law(s) will help you with this and how. If your state has no formal procedure for clearing your record, contact the D.A.'s office in the county where the case was originally prosecuted. Ask the D.A.'s office for the appropriate court records needed to clear your name. You may need to hire a criminal defense attorney to help you clear your name. Contact Legal Services in your state or your local bar association for help in finding an attorney.

Finally, contact your state Department of Motor Vehicles (DMV) to find out if your driver's license is being used by the identity thief. Ask that your files be flagged for possible fraud.

Debt Collectors

The Fair Debt Collection Practices Act prohibits debt collectors from using unfair or deceptive practices to collect overdue bills that a creditor has forwarded for collection, even if those bills don't result from identity theft.

You can stop a debt collector from contacting you in two ways:

- Write a letter to the collection agency telling them to stop. Once the debt collector receives your letter, the company may not contact you again with two exceptions: They can tell you there will be no further contact, and they can tell you that the debt collector or the creditor intends to take some specific action.
- Send a letter to the collection agency, within 30 days after you received written notice of the debt, telling them that you do not owe the money. Include copies of documents that support your position. Including a copy (NOT original) of your police report may be useful. In this case, a collector can renew collection activities only if it sends you proof of the debt.

If you don't have documentation to support your position, be as specific as possible about why the debt collector is mistaken. The debt collector is responsible for sending you proof that you're wrong. For example, if the debt you're disputing originates from a credit card you never applied for, ask for a copy of the application with the applicant's signature. Then, you can prove that it's not your signature.

If you tell the debt collector that you are a victim of identity theft and it is collecting the debt for another company, the debt collector must tell that company that you may be a victim of identity theft.

While you can stop a debt collector from contacting you, that won't get rid of the debt itself. It's important to contact the company that originally opened the account to dispute the debt, otherwise that company may send it to a different debt collector, report it on your credit report, or initiate a lawsuit to collect on the debt.

Driver's License

If you think your name or Social Security number is being used by an identity thief to get a driver's license or a non-driver's ID card, contact your state Department of Motor Vehicles

(DMV). If your state DMV uses your Social Security number as your driver's license number, ask to substitute another number.

Mail Theft

The U.S. Postal Inspection Service (USPIS) is the law enforcement arm of the U.S. Postal Service and investigates cases of identity theft. The USPIS has primary jurisdiction in all matters infringing on the integrity of the U.S. mail. If an identity thief has stolen your mail to get new credit cards, bank or credit card statements, pre-screened credit offers, or tax information, or has falsified change-of-address forms or obtained your personal information through a fraud conducted by mail, report it to your local postal inspector.

You can locate the USPIS district office nearest you by calling your local post office, checking the Blue Pages of your telephone directory, or visiting www.usps.gov/websites/depart/inspect.

Medical Identity Theft

Medical identity theft occurs when someone uses your personal information without your knowledge or consent to obtain, or receive payment for, medical treatment, services, or goods.

Victims of medical identity theft may find that their medical records are inaccurate, which can have a serious impact on their ability to obtain proper medical care and insurance benefits.

To detect medical identity theft, consider the following steps:

- Closely monitor any "Explanation of Benefits" sent by public or private health insurers. If anything appears wrong, raise questions with the insurer or the provider. Do not assume that there are no problems simply because you may not owe any money.
- Once a year (or more often, if you believe there is cause for concern), request a listing of benefits paid in your name by any health insurers that might have made such payments on your behalf.
- Monitor your credit reports with the nationwide credit reporting companies – Equifax, Experian, and TransUnion – to identify reports of medical debts.

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.

Passport Fraud

If you've lost your passport, or believe it was stolen or is being used fraudulently, contact the United States Department of State (USDS) through www.travel.state.gov/passport/passport_1738.html, or call a local USDS field office. Local field offices are listed in the Blue Pages of your telephone directory.

Phone Fraud

If an identity thief has established phone service in your name, is making unauthorized calls that seem to come from and are billed to your cellular phone, or is using your calling card and PIN, contact your service provider immediately to cancel the account and/or calling card. Open new accounts and choose new PINs. If you're having trouble getting fraudulent phone charges removed from your account or getting an unauthorized account closed, contact the appropriate agency below:

- For local service, contact your state Public Utility Commission.
- For cellular phones and long distance, contact the Federal Communications Commission (FCC) at 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: Federal Communications Commission, Consumer Information Bureau, 445 12th Street, SW, Room 5A863, Washington, DC 20554. You can file complaints online at www.fcc.gov, or e-mail your questions to fccinfo@fcc.gov.

Social Security Number Misuse

If you have specific information of Social Security number misuse that involves the buying or selling of Social Security cards, may be related to terrorist activity, or is designed to obtain Social Security benefits, contact the Social Security Administration (SSA) Office of the Inspector General. You may file a complaint online at www.socialsecurity.gov/oig, call toll-free: 1-800-269-0271, fax: 410-597-0118, or write: SSA Fraud Hotline, P.O. Box 17768, Baltimore, MD 21235.

You also may call SSA toll-free at 1-800-772-1213 to verify the accuracy of the earnings reported on your Social Security number, request a copy of your Social Security Statement, or get a replacement Social Security number card if yours is lost or stolen. Follow up in writing.

Student Loans

Contact the school or program that opened the student loan to close the loan. At the same time, report the fraudulent loan to the U.S. Department of Education. Call the Inspector General's Hotline toll-free at 1-800-MIS-USED; visit www.ed.gov/about/offices/list/oig/hotline.html?src=rt;
or write: Office of Inspector General, U.S. Department of Education, 400 Maryland Avenue, SW, Washington, DC 20202-1510.

Tax Fraud

The Internal Revenue Service (IRS) is responsible for administering and enforcing tax laws. Identity fraud may occur as it relates directly to your tax records. Visit www.irs.gov and type in the IRS key word "Identity Theft" for more information.

If you have an unresolved issue related to identity theft, or you have suffered or are about to suffer a significant hardship as a result of the administration of the tax laws, visit the IRS Taxpayer Advocate Service www.irs.gov/advocate/ or call toll-free: 1-877-777-4778.
If you suspect or know of an individual or company that is not complying with the tax law, report it to the Internal Revenue Service Criminal Investigation Informant Hotline by calling toll-free: 1-800-829-0433 or visit www.irs.gov and type in the IRS key word "Tax Fraud."

What if I'm still having problems?

There are cases where victims do everything right and still spend years dealing with problems related to identity theft. The good news is that most victims can get their cases resolved by being vigilant, assertive and organized. Don't procrastinate on contacting companies to address the problems. Don't be afraid to go up the chain of command or make complaints, if necessary. Keep organized files. If you haven't filed a complaint with the FTC or updated it, you should do so and provide details of the problems that you are having. You also can call the FTC hotline (1-877-ID-THEFT) to talk with one of their counselors. If your problems are stemming from a failure of a party to perform its legal obligations, you may want to consult an attorney who specializes in such violations. Contact Legal Services in your state or your local bar association for help in finding an attorney.

Sample Letter - Request for Fraudulent Transaction/Account Information

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.

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]
Enclosures: (what you are including as supporting evidence)

Sample Dispute Letter for Existing Accounts

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

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

Dear Sir or Madam:

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

Enclosed is a copy of my Identity Theft Report supporting my position.

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

Sincerely,
[Your Name]
Enclosures: (what you are including as supporting evidence)

Sample Dispute Letter for New Accounts

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

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

Dear Sir or Madam:

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

Enclosed is a copy of my Identity Theft Report supporting my position.

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

Sincerely,
[Your Name]

Enclosures: (what you are including as supporting evidence)

Sample Blocking Letter Credit Bureaus

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

Complaint Department
[Name of Credit Bureau]
[Address]
[City, State, Zip Code]

Dear Sir or Madam:

I am a victim of identity theft. I am writing to request that you block the following fraudulent information in my file. This information does not relate to any transaction that I have made. The items also are circled on the attached copy of the report I received. (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.)

Enclosed is a copy of the law enforcement report regarding my identity theft. Please let me know if you need any other information from me to block this information on my credit report.

Sincerely,
[Your Name]
Enclosures: (What you are including as supporting evidence)

Instructions for Completing the ID Theft Affidavit

To make certain that you do not become responsible for the debts incurred by the identity thief, you must provide proof that you didn't create the debt to each of the companies where accounts where opened or used in your name.

A working group composed of credit grantors, consumer advocates and the Federal Trade Commission (FTC) developed this ID Theft Affidavit to help you report information to many companies using just one standard form. Use of this affidavit is optional for companies. While many companies accept this affidavit, others require that you submit more or different forms. Before you send the affidavit, contact each company to find out if they accept it.

You can use this affidavit where 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 to find out what to do.)

This affidavit has two parts:

- **ID Theft Affidavit** is where you report general information about yourself and the theft.

- **Fraudulent Account Statement** is where you describe the fraudulent account(s) opened in your name. Use a separate Fraudulent Account Statement for each company you need to write to.

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

Complete this affidavit as soon as possible. Many creditors ask that you send it within two weeks of receiving it. Delaying could slow the investigation.

Be as accurate and complete as possible. You *may* choose not to provide some of the information requested. However, incorrect or incomplete information will slow the process of investigating your claim and absolving the debt. Please print clearly.

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

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

If you cannot 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.

DO NOT SEND AFFIDAVIT TO THE FTC OR ANY OTHER GOVERNMENT AGENCY

If you haven't already done so, report the fraud to the following organizations:

1. Each of the three **national consumer reporting agencies**. Ask each agency to place a "fraud alert" on your credit report, and send you a copy of your credit file. When you have completed your affidavit packet, you may want to send them a copy to help them investigate the disputed accounts.

- **Equifax Credit Information Services, Inc.**
  (800) 525-6285/ TDD 1-800-255-0056 and ask the operator to call the Auto Disclosure Line at 1-800-685-1111 to obtain a copy of your report.
  P.O. Box 740241, Atlanta, GA 30374-0241
  www.equifax.com

- **Experian information Solutions, Inc.**
  (888) 397-3742/ TDD (800) 972-0322
  P.O. Box 9530, Allen, TX 75013
  www.experian.com

- **TransUnion**
  (800) 680-7289/ TDD (877) 553-7803
  Fraud Victim Assistance Division
  P.O. Box 6790, Fullerton, CA 92634-6790
  www.transunion.com

2. The **fraud department at each creditor, bank, or utility/service** that provided the identity thief with unauthorized credit, goods or services. This would be a good time to find out if the company accepts this affidavit, and whether they require notarization or a copy of the police report.

3. Your local **police department**. Ask the officer to take a report and give you a copy of the report. Sending a copy of your police report to financial institutions can speed up the process of absolving you of wrongful debts or removing inaccurate information from your credit reports. If you can't get a copy, at least get the number of the report.

4. The FTC, which maintains the Identity Theft Data Clearinghouse – the federal government's centralized identity theft complaint database – and provides information to identity theft victims. You can visit **www.consumer.gov/idtheft** or call toll-free **1-877-ID-THEFT (1-877-438-4338)**.

   The FTC collects complaints from identity theft victims and shares their information with law enforcement nationwide. This information also may be shared with other government agencies, consumer reporting agencies, and companies where the fraud was perpetrated to help resolve identity theft related problems.

DO NOT SEND AFFIDAVIT TO THE FTC OR ANY OTHER GOVERNMENT AGENCY

Victim Information

(1) My full legal name is _____
(First) (Middle) (Last) (Jr., Sr., III)

(2) (If different from above) When the events described in this affidavit took place, I was known as

_____
(First) (Middle) (Last) (Jr., Sr., III)

(3) My date of birth is _____
(day/month/year)

(4) My Social Security number is_____

(5) My driver's license or identification card state and number are_____

(6) My current address is _____

City _____ State _____ Zip Code _____

(7) I have lived at this address since _____
(month/year)

(8) (If different from above) When the events described in this affidavit took place, my address was

_____

City _____ State _____ Zip Code _____

(9) I lived at the address in Item 8 from _____ until _____
(month/year) (month/year)

(10) My daytime telephone number is (____)_____

My evening telephone number is (____)_____

DO NOT SEND AFFIDAVIT TO THE FTC OR ANY OTHER GOVERNMENT AGENCY

How the Fraud Occurred

Check all that apply for items 11 - 17:

(11) ❑ I did not authorize anyone to use my name or personal information to seek the money, credit, loans, goods or services described in this report.

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

(13) ❑ My identification documents (for example, credit cards; birth certificate; driver's license; Social Security card; etc.) were ❑ stolen ❑ lost on or about _____.
(day/month/year)

(14) ❑ To the best of my knowledge and belief, the following person(s) used my information (for example, my name, address, date of birth, existing account numbers, Social Security number, mother's maiden name, etc.) or identification documents to get money, credit, loans, goods or services without my knowledge or authorization:

_____ Name (if known)	_____ Name (if known)
_____ Address (if known)	_____ Address (if known)
_____ Phone number(s) (if known)	_____ Phone number(s) (if known)
_____ Additional information (if known)	_____ Additional information (if known)

(15) ❑ I do NOT know who used my information or identification documents to get money, credit, loans, goods or services without my knowledge or authorization.

(16) ❑ Additional comments: (For example, description of the fraud, which documents or information were used or how the identity thief gained access to your information.)

_____

_____

_____

_____

_____

(Attach additional pages as necessary.)

DO NOT SEND AFFIDAVIT TO THE FTC OR ANY OTHER GOVERNMENT AGENCY

Victim's Law Enforcement Actions

(17) (check one) I ❑ am ❑ am not willing to assist in the prosecution of the person(s) who committed this fraud.

(18) (check one) I ❑ am ❑ am not authorizing the release of this information to law enforcement for the purpose of assisting them in the investigation and prosecution of the person(s) who committed this fraud.

(19) (check all that apply) I ❑ have ❑ have not reported the events described in this affidavit to the police or other law enforcement agency. The police ❑ did ❑ did not write a report. *In the event you have contacted the police or other law enforcement agency, please complete the following:*

_____	_____
(Agency #1)	(Officer/Agency personnel taking report)
_____	_____
(Date of report)	(Report number, if any)
_____	_____
(Phone number)	(email address, if any)
_____	_____
(Agency #2)	(Officer/Agency personnel taking report)
_____	_____
(Date of report)	(Report number, if any)
_____	_____
(Phone number)	(email address, if any)

Documentation Checklist

Please indicate the supporting documentation you are able to provide to the companies you plan to notify. Attach copies (NOT originals) to the affidavit before sending it to the companies.

(20) ❑ A copy of a valid government-issued photo-identification card (for example, your driver's license, state-issued ID card or your passport). If you are under 16 and don't have a photo-ID, you may submit a copy of your birth certificate or a copy of your official school records showing your enrollment and place of residence.

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

DO NOT SEND AFFIDAVIT TO THE FTC OR ANY OTHER GOVERNMENT AGENCY

(22) ❑ A copy of the report you filed with the police or sheriff's department. If you are unable to obtain a report or report number from the police, please indicate that in Item 19. Some companies only need the report number, not a copy of the report. You may want to check with each company.

Signature

I declare under penalty of perjury that the information I have provided in this affidavit is true and correct to the best of my knowledge.

_____ _____
(signature) (date signed)

Knowingly submitting false information on this form could subject you to criminal prosecution for perjury.

_____
(Notary)

[Check with each company. Creditors sometimes require notarization. If they do not, please have one witness (non-relative) sign below that you completed and signed this affidavit.]

Witness:

_____ _____
(signature) (printed name)

_____ _____
(date) (telephone number)

DO NOT SEND AFFIDAVIT TO THE FTC OR ANY OTHER GOVERNMENT AGENCY

Fraudulent Account Statement

Completing this Statement

- Make as many copies of this page as you need. **Complete a separate page for each company you're notifying and only send it to that company.** Include a copy of your signed affidavit.
- List only the account(s) you're disputing with the company receiving this form. **See the example below.**
- If a collection agency sent you a statement, letter or notice about the fraudulent account, attach a copy of that document (**NOT** the original).

I declare (check all that apply):

❑ As a result of the event(s) described in the ID Theft Affidavit, the following account(s) was/were opened at your company in my name without my knowledge, permission or authorization using my personal information or identifying documents:

Creditor Name/Address *(the company that opened the account or provided the goods or services)*	**Account Number**	**Type of unauthorized credit/goods/services provided by creditor** *(if known)*	**Date issued or opened** *(if known)*	**Amount/Value provided** *(the amount charged or the cost of the goods/services)*
Example Example National Bank 22 Main Street Columbus, Ohio 22722	01234567-89	auto loan	01/05/2002	$25,500.00

❑ During the time of the accounts described above, I had the following account open with your company:

Billing name _____

Billing address _____

Account number _____

DO NOT SEND AFFIDAVIT TO THE FTC OR ANY OTHER GOVERNMENT AGENCY

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 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.