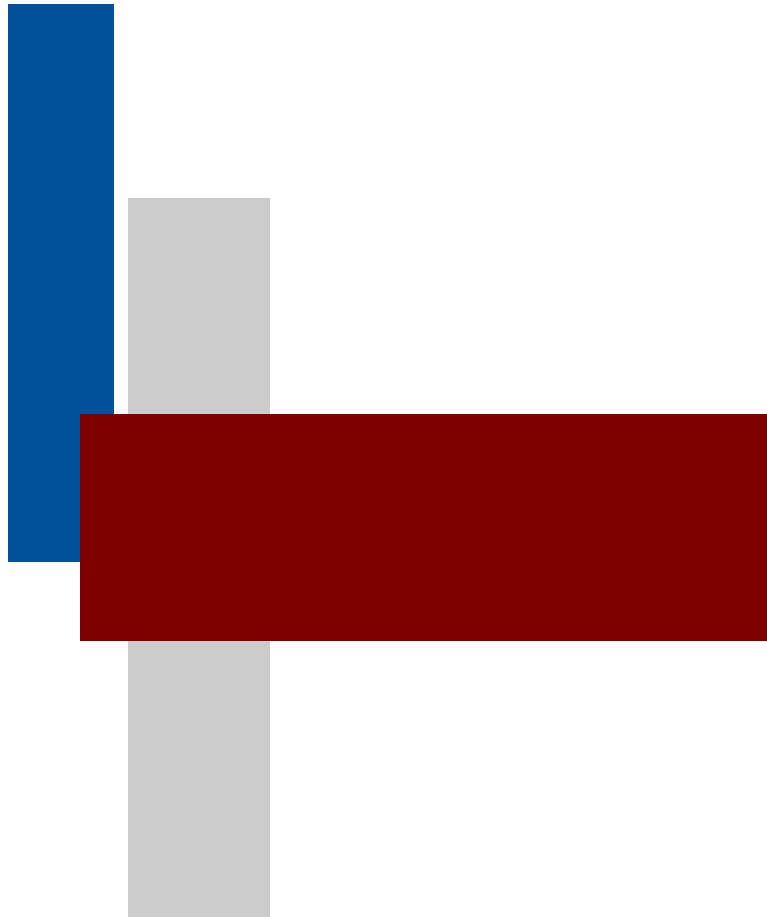




ID THEFT EMERGENCY RESPONSE KIT™





Emergency Response Kit

Identity Theft is the fastest growing crime in America, affecting more than 25 million people worldwide in the last 5 years!

Identity theft is one of the most devastating and fastest growing crimes today. It is estimated that **one out of five Americans**, or a member of their family, will become a victim of identity theft each year.

ID theft criminals are also becoming more brazen with their attempts to carry out large scale, systematic, fraud. Three of the largest banking institutions in the United States reported at least 350,000 accounts across the country were defrauded by a global theft ring, with potential losses in the millions of dollars to consumers. There is a daily barrage of newspaper headlines regarding private data theft, both locally and by global organized crime rings. In today's "data drenched" world, it is really a matter of "when, not if" one's private information will be stolen, misused or misreported by credit reporting agencies, creditors or business entities.

A common misconception about identity theft is that **"It will never happen to me."** Statistically, this is not the case. Unfortunately, identity theft already affects the lives of millions of Americans and more than half a million are being added each year according to the Federal Bureau of Investigation. Many victims may never discover that they are victims of identity theft until it is too late. Victims may never know that their identity has been stolen until unauthorized transactions appear on their credit card statements or collection notices appear. Victims who do learn the crime has occurred are left with little assistance to pick up the pieces.

Restoring your identity and credit can be an expensive and time-consuming process. On average victims of identity theft fraud will spend 170 hours researching the crime, 2-3 years correcting their credit reports, and up to \$4,849.00 in out of pocket expenses to restore their credit and identity. Victims are urged to report these matters to the authorities as soon as possible. Failure to expediently report identity theft could result in additional damage to a consumer's credit and can decrease their chances of recovery.

The most common form of identity theft is unauthorized use of name, social security number and other data to fraudulently obtain credit cards and open bank accounts. Another fast growing form of ID theft is "synthetic" in nature: a combination of private information from several people.

So how do identity thieves get your personal information?

1. They steal wallets, mail, and rummage through your trash.
2. They complete change of address forms to divert your mail.
3. They use your personal information found on the Internet or pose as employers or creditors to obtain copies of your credit report.
4. They also obtain credit card slips that you leave at restaurants or throw away.
5. They scam you through email or telephone solicitation, posing as legitimate companies.
6. They use creative software/cookies to steal your identity through your computer, laptop, PDA and your discarded cell phones.
7. They eavesdrop on conversations (or WIFI connections) to get PIN numbers, or they "shoulder surf" to get your PIN.
8. Your paper-carrier might even sell your "vacation hold," so the criminals know exactly what period of time your home will be empty for a unexpected "visit."

If You Are Victim of Identity Theft

Emergency! Take the following steps immediately:

- 1) Contact the credit bureaus
- 2) Close the accounts you believe have been fraudulently opened or accessed
- 3) Contact your local police department or the police where the identity theft took place
- 4) Contact the appropriate government agencies
- 5) Keep good records

1) Contact the credit bureaus and report that your identity has been stolen. Ask that a 90-day **fraud alert** be placed on your file and that no new credit be granted without your approval. Also, request a copy of your credit report from all 3 of the credit bureaus:

	Fraud Alert:	Copy of Report:
Experian	888-397-3742	888-397-3742
Equifax	800-525-6285	800-685-1111
TransUnion	800-680-7289	800-888-4213

Read each report carefully for errors!

Consider placing an **extended 7-year extended fraud alert** on your credit file once you have filed a police report (you will need to provide a copy of the police report to the credit bureaus). Or, alternatively, you may want to place a **security freeze** (a.k.a. credit freeze) on your credit file. A security freeze completely locks down your credit file and does not allow any new accounts to be opened in your name. This is the best way to protect your credit! Once a security freeze is requested, you will receive a PIN number which allows you to lift or “thaw” the freeze when you need to open a new account. Each state has it’s own laws regarding security freezes and you can view the law specific to your state by going to: http://www.consumersunion.org/campaigns/learn_more/003484indiv.html. The freeze does not affect your current accounts, however, you cannot open new accounts unless you lift the freeze (which typically takes only a day or two or in some cases can be done instantly online).

***You will find sample letters for requesting both a 7-year fraud alert and a security freeze attached to the end of this kit.**

Under the Fair Credit Reporting Act (FCRA), every United States citizen is entitled to one free credit file disclosure in a 12-month period (regardless if you are a victim or not). To request this free annual disclosure you may contact the Central Source on-line at www.annualcreditreport.com. You can also contact the Central Source to request this free annual disclosure by calling toll free (877) FACTACT or by using the mail request form available at the Central Source website. It is entirely your choice whether you order all three credit file disclosures at the same time or order one now and others later. The advantage of ordering all three at the same time is that you can compare them. (However, you will not be eligible for another free credit file disclosure from the Central Source for 12 months.) On the other hand, the advantage of ordering one now and others later (for example, one credit file disclosure every four months) is that you can keep track of any changes or new information that may appear on your credit file disclosure. Remember, you are entitled to receive one free credit file disclosure through the Central Source every 12 months from each of the nationwide consumer credit reporting companies - Equifax, Experian and TransUnion - so if you order from only one company today you can still order from the other two companies at a later date.

2) Close the accounts you believe have been fraudulently opened or accessed. If your credit card or ATM card has been tampered with, close the account and ask your bank or credit card company for the steps that need to be taken to dispute the account or charges. With most cases, this will include filling out a fraud affidavit and sending the financial institution a copy of your police report, but be sure to ask your institution what their policy is for disputing an account.

If your primary bank account has been compromised, seriously consider changing your accounts to an entirely new bank. (The thief will likely attempt to reach your “new” account using the same stolen information.) When you open new accounts, insist on password-only access.

If your checks have been stolen or lost, contact your financial institution immediately. They will put a stop payment on the lost or stolen checks. You may also want to contact the check-verification or check-guarantee companies. You may have to file a dispute with them if someone has been writing bad checks in your name. Following is a list of some of the more common check-verification companies:

SCAN	877-382-7226
ChexSystems	800-428-9623
Certegy	800-437-5120

If you were contacted by a collection agency about an account that does not belong to you, you can either (1) dispute the account with the collection agency or (2) send a Cease and Desist letter (sample letter attached) to the collection agency and dispute the account with the original creditor. A Cease and Desist letter states it is your policy not to deal with collection agencies and you intend to settle the debt with the original creditor. By law, once the collection agency receives the Cease and Desist they can only contact you one more time to tell you they received the letter. If they contact you more than once, they are violating the law and can be penalized.

Collection companies can be ruthless to deal with and a lot of times they will think you are trying to get out of paying your bills. Be persistent and try to keep a cool head when dealing with them. And remember, NEVER PAY FRAUDULENT BILLS. Even if the collection agency is threatening to ruin your credit, try to remain calm and demand the account be investigated due to identity theft.

3) Contact the police department and file a report.

a) If you are at home when the identity theft occurs, contact your local police department. File a report and obtain a copy of the report in case the bank, credit card company, collection agency, credit reporting agency or others need proof of the crime later on.

Some police departments will be more helpful than others. Be persistent! Bring as much documentation of the identity theft with you as possible (such as copies of your credit report, letters from collection agencies, etc.). Tell the police you need the report in order to dispute fraudulent accounts. If your local police will not file a report, consider going to the county or state police.

If the police department refuses to take a report, write down the officer’s name, badge number, date and location. You may need this “refusal” information later to dispute creditor claims, or to file with various state or federal agencies.

b) While traveling, if your personal documents or identification is stolen, contact the police department where you are and file a report. Make sure you get the report number and officer’s name if you will not be able to get a copy of the report immediately. **Do not wait until you get home to file a report.** In certain instances, a copy of the report will be vital, for example, if you are flying back home without identification. In these cases, you should let the officer know your travel plans and see if they can expedite getting you a copy of the report. If flying without identification, it is also recommended you contact the airline ahead of time and let them know the situation and if they have a specific policy to follow.

4) Contact appropriate government agencies. The following list is not all-inclusive. Contact **any** agency involved with your particular issue, such as the Department of Motor Vehicles, the Department of Education, etc.

Federal Trade Commission

If you’ve been a victim of identity theft, file a complaint with the Federal Trade Commission (FTC) by contacting the FTC’s Identity Theft Hotline by telephone: toll-free 1-877-IDTHEFT (438-4338); TDD: 202-326-2502; by mail: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC

20580; or online: www.consumer.gov/idtheft. Ask for a copy of *ID Theft: When Bad Things Happen to Your Good Name*, a free comprehensive consumer guide to help you guard against and recover from identity theft.

U.S. Postal Inspection Service

If you are a victim of identity theft and your mail is involved, call the Postal Inspection Service at 877-876-2455 to file a complaint or go online to <https://postalinspectors.uspis.gov/contactUs/filecomplaint.aspx>.

Social Security Administration

If you believe your Social Security number has been used to obtain work, contact the SSA and request a copy of your Social Security Earnings Statement. You can do this by going online to:

<https://secure.ssa.gov/apps6z/iss/main.html>. This statement is a reflection of your earnings history.

If your Social Security card has been lost or stolen, you can request a new card, however the SSA is not required to take any action to investigate the crime. It's the same if your Social Security number is being used fraudulently; the SSA does not investigate identity theft crimes. Go to www.ssa.gov for information on how to replace a lost or stolen social security card.

Internal Revenue Service

If you receive a notice or letter in the mail from the IRS that leads you to believe someone may have used your Social Security number fraudulently, respond immediately to the letter and follow the directions in the letter to dispute the matter.

If you believe you are the victim of identity theft and the IRS has not contacted you, complete Form 14039 – Identity Theft Affidavit. Go to <http://www.irs.gov/privacy/article/0,,id=186436,00.html> for instructions and to download the form.

If you have previously tried to resolve an identity theft issue and are still not been able to get the help you need, you should contact the IRS Identity Protection Specialized Unit at 1-800-908-4490.

5) Keep good records. This is very important. Maintain accurate records of your telephone conversations (including names of the people you spoke with, dates, and the essence of your conversation). If you send out letters by mail, use certified mail, return receipt requested (green card). Always send copies of your documents; keep your originals in a safe place. **Attached to this kit is a tracking form for your use.**

MEDICAL IDENTITY THEFT

The fastest growing form of identity theft is medical identity theft. Recent changes in the law are requiring medical records to become electronic. If someone steals your personal information in order to obtain medical treatment, the risk you are facing is not just financial. If your medical records are incorrect, your life is potentially at risk. For instance, your medical records could report the wrong blood type, serious allergies, surgeries you've never had, etc. Unfortunately, medical identity theft is not easily preventable either. All medical facilities require your personal information before you receive treatment. And, there's no way to prevent inside theft, such as the front desk clerk stealing your information.

You may be a victim of medical identity theft if:

- 1) Your credit report shows medical collection agencies you do not recognize.
- 2) A debt collector contacts you about medical debt you don't owe.
- 3) You get a bill for medical services you didn't receive.
- 4) You try to make a legitimate insurance claim and your health plan says you've reached your limit on benefits.
- 5) You are denied insurance because your medical records show a condition you don't have.

Preventative Steps to Take:

- 1) Monitor your medical records! Request copies of your medical records and your children's records regularly. Keep a current, up-to-date file in case your records become tampered with.
- 2) Check your credit report at least 3 times per year. Look for unpaid medical bills.
- 3) Thoroughly review explanation of benefits reports from insurers and immediately report any discrepancies.
- 4) Shred all personal and medical information, such as health insurance forms, prescription and physician statements.
- 5) Read authorization forms before signing and edit them to limit the sharing of information.

If you are a victim of medical identity theft:

- 1) File a police report.
- 2) If there are fraudulent medical bills, contact the collection agency or the original doctor's office or hospital, and dispute the charges. Handle the dispute just as you would with traditional identity theft.
- 3) Contact your insurance company immediately if your insurance card has been lost or stolen or false claims have been submitted.
- 4) Request a copy of your medical records and work with your medical provider on deleting all of the fraudulent information.
- 5) Every medical provider has a Privacy Officer. Contact the Privacy Officer and find out their specific policy for handling medical identity theft.

Additional Resources:

World Privacy Forum
www.worldprivacyforum.org

Center on Medical Record Rights and Privacy
<http://ihcrp.georgetown.edu/privacy/records.html>

If you believe your rights under HIPAA (the law that helps protect your private medical information) have been violated, you can file a complaint with:

U.S. Department of Health and Human Services
www.hhs.gov/ocr

Criminal Identity Theft

Criminal identity theft most commonly occurs when an imposter uses your information (name, DOB, SSN) when arrested for a crime or cited for a traffic violation. The imposter may actually have a counterfeit license with your information on it. You may not find out about the identity theft until you apply for a job and are turned down based on the background check or if you are pulled over for a traffic violation and find out there are warrants out for your arrest. In worst-case scenarios, you are actually arrested. Unfortunately, as with all types of identity theft, the burden is on you to prove you are a victim and not the criminal.

Your ultimate goal with criminal identity theft is to obtain a "clearance letter" and have your name removed from county, state, and/or federal criminal record databases. However, please note your name will likely still appear as an alias of the imposters in order to retain the accuracy of the investigation.

Recommended Steps:

- 1) Contact the arresting agency and explain your situation. You will need to confirm your identity with the agency. This might include fingerprints, photographs and/or copies of your personal documents (such as driver's license or social security card). Request to file an Impersonation Report.

- 2) If the arresting agency is in a different location, also contact your local police department and file a report. They may be able to assist you in filing the Impersonation Report as well.
- 3) Contact the district attorney's office or public defender's office where the arrest occurred. Again, explain your situation and they should have a procedure for you to follow to prove your case.
- 4) Work with the court system to get the issue resolved. If the imposter committed the crime in another state, the public defender's office should be able to represent you without you physically being there. The process varies from location to location. However, you should request an "identity hearing" where the judge will review the evidence and make a determination as to your innocence.
- 5) Once your innocence has been proven, you will need to contact the arresting agency and courts to find out what information brokers your criminal record might have been sold to. You will need to contact those brokers in order to have your information corrected.

If you are unable to resolve the situation and prove your innocence, it may be necessary to hire a criminal attorney.

Additional Resources:

Privacy Rights Clearinghouse
www.privacyrights.org

Protecting Your Children from Identity Theft

Children can become victims of identity theft just like adults. Sometimes children are alluring targets because their credit has not been used and it gives the fraudster a clean slate to work with. Protecting your children's personal information is just as important as protecting your own. Don't carry your children's social security cards around with you and be cautious when giving it out.

If you suspect your child is a victim, go to TransUnion's website and complete their Child Identity Theft Inquiry.

<https://www.transunion.com/corporate/personal/fraudIdentityTheft/fraudPrevention/childIDInquiry.page>

TransUnion will then search your child's name and social security number to see if there is an active credit file.

IF a credit file exists for your child, then your child is a victim of identity theft and you will need to dispute those accounts immediately on their behalf. Follow the steps outlined in the section titled "If You are a Victim of Identity Theft" on page 2. When disputing the accounts, do not hesitate to mention that the account was opened when your child was a minor and was not legally able to enter into a contract. In a lot of these instances, you may be required to provide a copy of your child's birth certificate.

Also, it is very important that you freeze your child's credit report while you are working on cleaning up the mess. To protect your child, keep the credit frozen until the child becomes an adult.

You also may wonder if it's a good idea to try to change your child's social security number. In most cases, the Social Security Administration advises against changing the number because it can create new problems. However, when dealing with a minor and if the case is severe enough, changing the social security number should be considered. Ultimately, the Social Security Administration decides whether the case is severe enough to warrant changing the SSN. Go to the Social Security Administration's website for more information about applying for a new SSN:
<http://www.socialsecurity.gov/pubs/10064.html#new>.

FAQ: Consumer Reports and Credit Reporting Agencies (CRA)

If you've ever applied for a charge account, a personal loan, insurance, a job, or a house/apartment rental/purchase there's a file about you. This file contains information on where you work and live, how you pay your bills, and whether you've been sued, arrested, or filed for bankruptcy.

Companies that gather and sell this information are called Consumer Reporting Agencies (CRAs). The most common type of CRA is a credit bureau, such as TransUnion, Experian and Equifax. The information CRAs sell about you to creditors, employers, landlords, utilities, insurers, and other businesses is called a "consumer report."

The Fair Credit Reporting Act (FCRA), enforced by the Federal Trade Commission, is designed to promote accuracy and ensure the privacy of the information used in consumer reports. Recent amendments to the Act (FACTA) expand your rights and place additional requirements on CRAs. Businesses that supply information about you to CRAs, and those that use consumer reports also have new responsibilities under the law.

Here are some questions consumers commonly ask about consumer reports and CRAs - and the answers. Note that you may have additional rights under state laws. Contact your state Attorney General, a private attorney or local consumer protection agency for more information.

Q. Do I have a right to know what's in my report?

A. Yes, if you ask for it. The CRA must tell you everything in your report, including medical information, and in most cases, the sources of the information. The CRA also must give you a list of everyone who has requested your report within the past year - two years for employment related requests.

Q. What can I do about inaccurate or incomplete information?

A. Under the new law, both the CRA and the information provider have responsibilities for correcting inaccurate or incomplete information in your report. To protect all your rights under this law, contact BOTH the CRA and the information provider.

First, tell the CRA in writing what information you believe is inaccurate. CRAs must reinvestigate the items in question - usually within 30 days - unless they consider your dispute frivolous. They also must forward all relevant data you provide about the dispute to the information provider. After the information provider receives notice of a dispute from the CRA, it must investigate, review all relevant information provided by the CRA, and report the results to the CRA. If the information provider finds the disputed information to be inaccurate, it must notify all nationwide CRAs and they must correct this information in your file.

When the reinvestigation is complete, the CRA must give you the written results and a free copy of your report if the dispute results in a change. If an item is changed or removed, the CRA cannot put the disputed information back in your file unless the information provider verifies its accuracy and completeness, and the CRA gives you a written notice that includes the name, address, and phone number of the provider.

Second, tell the creditor or other information provider in writing that you dispute an item. Many providers specify an address for disputes. If the provider then reports the item to any CRA, it must include a notice of your dispute. In addition, if you are correct - that is, if the information is inaccurate - the information provider may not use it again.

Q. What can I do if the CRA or information provider won't correct the information I dispute?

A. A reinvestigation may not resolve your dispute with the CRA. If that's the case, ask the CRA to include your statement of the dispute in your file and in future reports. If you request, the CRA also will provide your statement to anyone who received a copy of the old report in the recent past. There usually is a fee for this service.

If you tell the information provider that you dispute an item, a notice of your dispute must be included anytime the information provider reports the item to a CRA.

Q. What should I know about "investigative consumer reports"?

A. "Investigative consumer reports" are detailed reports that involve interviews with your neighbors or acquaintances about your lifestyle, character, and reputation. They may be used in connection with insurance and employment applications. You'll be notified in writing when a company orders such a report. The notice will explain your right to request certain information about the report from the company you applied to. If your application is rejected, you may get additional information from the CRA. However, the CRA does not have to reveal the sources of the information.

Q. How long can a CRA report negative information?

A. Seven years. There are certain exceptions:

- Information about criminal convictions may be reported without any time limitation. Bankruptcy information may be reported for 10 years.
- Information reported in response to an application for a job with a salary of more than \$75,000 has no time limit.
- Information reported because of an application for more than \$150,000 worth of credit or life insurance has no time limit.
- Information about a lawsuit or an unpaid judgment against you can be reported for seven years or until the statute of limitations runs out, whichever is longer.

Q. Can anyone get a copy of my report?

A. No. Only people with a legitimate business need, as recognized by the FCRA. For example, a company is allowed to get your report if you apply for credit, insurance, employment, to rent an apartment/house, to open a utility account or to check your credit by one of your current creditors.

Q. How can I stop a CRA from including me on lists for unsolicited credit and insurance offers?

A. Creditors and insurers may use CRA file information as a basis for sending you unsolicited offers. These offers must include a toll-free number for you to call if you want to remove your name and address from lists for two years; completing a form that the CRA provides for this purpose will keep your name off the lists permanently.

A. You can also "opt-out" of such offers by calling toll free: 888-567-8688. One call covers all: Equifax, TransUnion, Experian and Innovis. (Note: this is not the same as the "Direct Marketing Association" list for junk mail.)

Q. Are there other laws I should know about?

A. Yes. If your credit application was denied, the Equal Credit Opportunity Act (ECOA) requires creditors to specify why - if you ask. For example, the creditor must tell you whether you were denied because you have "no credit file" with a CRA or because the CRA says you have "delinquent obligations." The ECOA also requires creditors to consider additional information you might supply about your credit history. You may want to find out why the creditor denied your application before you contact the CRA.

Q. Where should I report violations of the law?

A. Although the FTC can't act as your lawyer in private disputes, information about your experiences and concerns is vital to the enforcement of the Fair Credit Reporting Act. Send your questions or complaints to: Consumer Response Center - FCRA, Federal Trade Commission, Washington, DC 20580 or go to <https://www.ftccomplaintassistant.gov/>

Your credit report--a type of consumer report--contains information about where you work and live and how you pay your bills. It also may show whether you've been sued or arrested or have filed for bankruptcy. Companies called "consumer reporting agencies" (CRAs), or credit bureaus, compile and sell your credit report to businesses. Because businesses use this information to evaluate your applications for credit, insurance, employment, and other purposes

allowed by the Fair Credit Reporting Act (FCRA), it's important that the information in your report is complete and accurate.

Some financial advisors suggest that you periodically review your credit report for inaccuracies or omissions. This could be especially important if you're considering making a major purchase, such as buying a home or car. Checking in advance on the accuracy of information in your credit file could speed the credit-granting process.

In addition to writing to the CRA, tell the creditor or other information provider in writing that you dispute an item. Again, include copies (NOT originals) of documents that support your position. Many providers specify an address for disputes. If the provider then reports the item to any CRA, it must include a notice of your dispute. In addition, if you are correct-that is, if the disputed information is not accurate-the information provider must not use it again. However, when "negative information" is accurate, only the passage of time can assure its removal. Accurate "negative information" can generally stay on your report for (7) years.

Adding Accounts to Your File

Your credit file may not reflect all your credit accounts. Although most national department store and all-purpose bank credit card accounts will be included in your file, not all creditors supply information to CRAs: Some travel, entertainment, gasoline card companies, local retailers, and credit unions are among those creditors that don't. If you've been told you were denied credit because of an "insufficient credit file" or "no credit file" and you have accounts with creditors that don't appear in your credit file, ask the CRA to add this information to future reports. Although they are not required to do so, many CRAs will add verifiable accounts for a fee. However, you should understand that if these creditors do not report to the CRA on a regular basis, these added items would not be updated in your file.

Contest Bills That Are a Result of Identity Theft. Attorneys, consumer and privacy advocates recommend not paying any portion of a bill that is a result of identity theft and not filing for bankruptcy. This will involve disputing credit card charges with the card company by writing to the address for "billing error" disputes - not the bill payment address. You should follow the directions given by the credit card company for disputing charges. The company must provide this information. Your credit rating should not be permanently affected, and no legal action should be taken against you as a result of identity theft. If any merchant, financial institution or collection agency suggests otherwise, simply restate your willingness to cooperate, but don't allow yourself to be coerced, or intimidated, into paying fraudulent bills. Report such attempts to state and government regulators immediately, especially if the intimidation is to threaten to harm your credit score!

Note: This Emergency Response Kit includes the following sample letters and documents:

- 1) Identity Theft Affidavit
- 2) Dispute letter to a credit reporting agency
- 3) 7-year fraud alert letter
- 4) Request for credit freeze (also known as "security freeze")
- 5) Collection Agency – Sample "Cease and Desist" Letter
- 6) Identity Theft Tracking Form

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 the accounts were opened or used in your name.

A working group of credit grantors and consumer advocates and the Federal Trade Commission (FTC) developed the attached 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. (Often, the creditor has its own form it prefers you to complete. You should cooperate and complete its form as requested.)

The 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 write to.

When you send the affidavit to the companies, attach copies (NOT ORIGINALS) of any supporting documentation (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. Delay can slow down the investigation.

Be as accurate 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 clearing the debt. If you write, be sure to 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 the 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 to help stop further fraud. If this affidavit is requested in a lawsuit, the company might provide it to the requesting party. **Be truthful and accurate!**

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

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

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

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 disputed accounts.

Call the **fraud department at each creditor, bank, or utility service** that provided the identity theft 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.

Call your local **police department**. Ask the officer to take a report and give you a copy of the report once it is completed. Sending a copy of the 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 and the name and phone number of the officer overseeing the investigation. If the officer refuses to take a report, get the officer's name, badge number and note the date of the "refusal." You may need this information later when a creditor or CRA demands a copy of a police report. (Remember, a creditor or CRA will often suspect you as not being truthful, even though you are actually the victim. Dishonest people generally do not attempt to file a police report.)

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.

The content hereof, together with any attachments, are subject to Federal and State Copyright and Trademark protections. This content may not be used, reproduced or distributed in any manner, in whole or in part, without the prior written consent of CLC Incorporated.

Name _____ Phone number _____

ID Theft Affidavit

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 _____
(month/day/year)
4. My Social Security number is _____
5. My driver's license or identification card state and number are _____
(state – number)
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

Name _____

Phone number _____

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 _____.
(month/day/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 identify thief gained access to your information.)

(Attach additional pages as necessary.)

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

Name _____

Phone number _____

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)

Office/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).

Name _____

Phone number _____

- 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)

(phone number)

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

Name _____

Phone number _____

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	1234567-89	Auto loan	01/05/2002	\$25,500.00
NOTE: see additional Account Statement on page 6				

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

Name _____

Phone number _____

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	1234567-89	Auto loan	01/05/2002	\$25,500.00

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

Sample Dispute Letter to Credit Reporting Agency

(Send certified mail, return receipt- green card- requested; keep a copy for your records.)

Date

Your Name

Your Address

Your City, State, Zip Code

Complaint Department

Name of Credit Reporting Agency

Address City, State, Zip Code

Dear Sir or Madam:

I am writing to dispute the following information in my credit file. The items in dispute are also encircled on the attached copy of the credit report 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.)

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, as required under the FCRA and FACTA.

Sincerely,

Your name

Enclosures: (List what you are enclosing)

7-Year Fraud Alert

To add a 7 year fraud alert to your personal credit report, please mail the following letter, along with one copy of your police report, a government issued identification card, such as a driver's license, state ID card, military ID card, etc., **and** one copy of a utility bill, bank or insurance statement, etc. Make sure that each copy is legible (enlarge if necessary), displays your name and current mailing address, and the date of issue (statement dates must be recent). Send **copies** of all documents; **always retain your originals**.

(Send certified mail, return receipt- green card- requested; keep a copy for your records.)

MAIL TO:

TransUnion
P.O. Box 6790
Fullerton, CA 92834

Experian
P.O. Box 9554
Allen, TX 75013

Equifax Consumer Fraud Division
P.O. Box 740256
Atlanta, GA 30374

Date: _____

Your Identification Information:

Name: _____

Address: _____

Social Security Number: _____

Date of Birth: _____

Home Telephone Number: _____

Business/alternate Telephone Number: _____

Report Number: _____

I am requesting that an extended 7-year fraud alert be added to my personal credit file.

Additional Comments: _____

Sincerely,

Your Name

Enclosures: (List what you are enclosing)

Request for Security Freeze / Credit Freeze

Please review the instructions specific to your state before sending this letter. Go to:

http://www.consumersunion.org/campaigns/learn_more/003484indiv.html

In general, a security freeze is free for victims of identity theft and typically costs about \$10.00 per agency for non-victims. However, your state might be different. Send **copies** of all documents; **always retain your originals**.

(Send certified mail, return receipt- green card- requested; keep a copy for your records.)

Date

MAIL TO:

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30349

TransUnion Security
Freeze
P.O. Box 6790
Fullerton, CA 92834-6790

To Whom It May Concern:

I would like to place a security freeze on my credit report.

My name is:

My current address is:

My previous address was:

My social security number is:

My date of birth is:

I am a victim of identity theft and have enclosed a copy of my [police report, identity theft report] along with a copy of my government identification and proof of address [current utility bill, phone bill].

Thank you for your immediate attention to this matter.

Sincerely,

Your Name

Enclosures: [List what you are enclosing]

Collection Agency - Cease and Desist Letter

Your Name
Your Mailing
Address

**Via Certified Mail
Return Receipt Requested**

Date

Attn:
Collection Agency
Mailing
Address

Re: Account #

Dear:

This letter will serve as your legal notice under federal law that regulates the activities of collection agencies and their legal representatives.

1. You are hereby notified under provisions **Public Law 95-109, Section 805-C, The Fair Debt Collection Practices Act** to hereby **Cease and Desist** in **any** and **all** attempts to collect the debt referenced above.
2. Your failure to do so **will** result in charges being filed against you with the state and federal regulatory agencies empowered with enforcement.
3. Since it is my position **not** to recognize and/or work with collection agencies, I will settle this matter directly with the original creditor.
4. You are hereby put on notice of the following:
 - ❖ Do not call me at home.
 - ❖ Do not call me at work.
 - ❖ I have Caller ID and I tape all of my phone calls.
5. Finally, **please let this letter serve as my official disputation of the debt you're attempting to collect.** Failure to honor this notice will be construed as a direct violation of both the Fair Credit Billing Act and the Fair Debt Collection Practices Act.

Furthermore, if any negative information is placed on my credit bureau reports by your agency after receipt of this notice, this will cause me to file suit against you and your organization, both personally and corporately, to seek any and all legal remedies available to me by law.

Since it is my policy neither to recognize nor deal with collection agencies, I intend to settle this account with the original creditor.

Sincerely,

Your Name

IDENTITY THEFT TRACKING FORM

Credit Bureaus

Experian 888-397-3742

Date	Contact Person	Comments

Equifax 800-525-6285

Date	Contact Person	Comments

TransUnion 800-680-7289

Date	Contact Person	Comments

Credit Card Companies / Banks / Collection Companies

Name of Company: _____ Phone: _____

[illegible]

Law Enforcement Agency

Police Department: _____ Phone: _____

Date	Contact Person	Comments

Other Contacts:**Federal Trade Commission 877-438-4338**

Date	Contact Person	Comments

U.S. Postal Inspection Service 877-876-2455

Date	Contact Person	Comments

Social Security Administration 800-269-0271

Date	Contact Person	Comments