CREDITORG

IDENTITY THEFT

Table of Content

About Credit.org

Credit.org is a Nonprofit Consumer Credit Counseling Agency Formed in 1974

Our mission is simple, yet vital: Improve the financial well-being of individuals and families by providing quality financial education and counseling. We offer personal assistance with money, credit, and debt management through educational programs and confidential counseling.

Our Services

Financial Education Programs

We offer seminars, workshops, and educational materials on topics such as budgeting and money management, identity theft, and understanding credit.

Debt Management Programs

If you choose this option, we can work with your creditors to reduce costs and repay debt through one monthly payment.

Confidential Debt Counseling

Our certified consumer credit counselors will discuss your financial situation with you, help you understand what may cause financial stress, and help you create a personalized budget, an action plan and give you options to help manage your finances more effectively.

Credit Report Review

Our certified counselors work with you to break down your credit report, answer questions, and give guidance for improving your credit score over time.

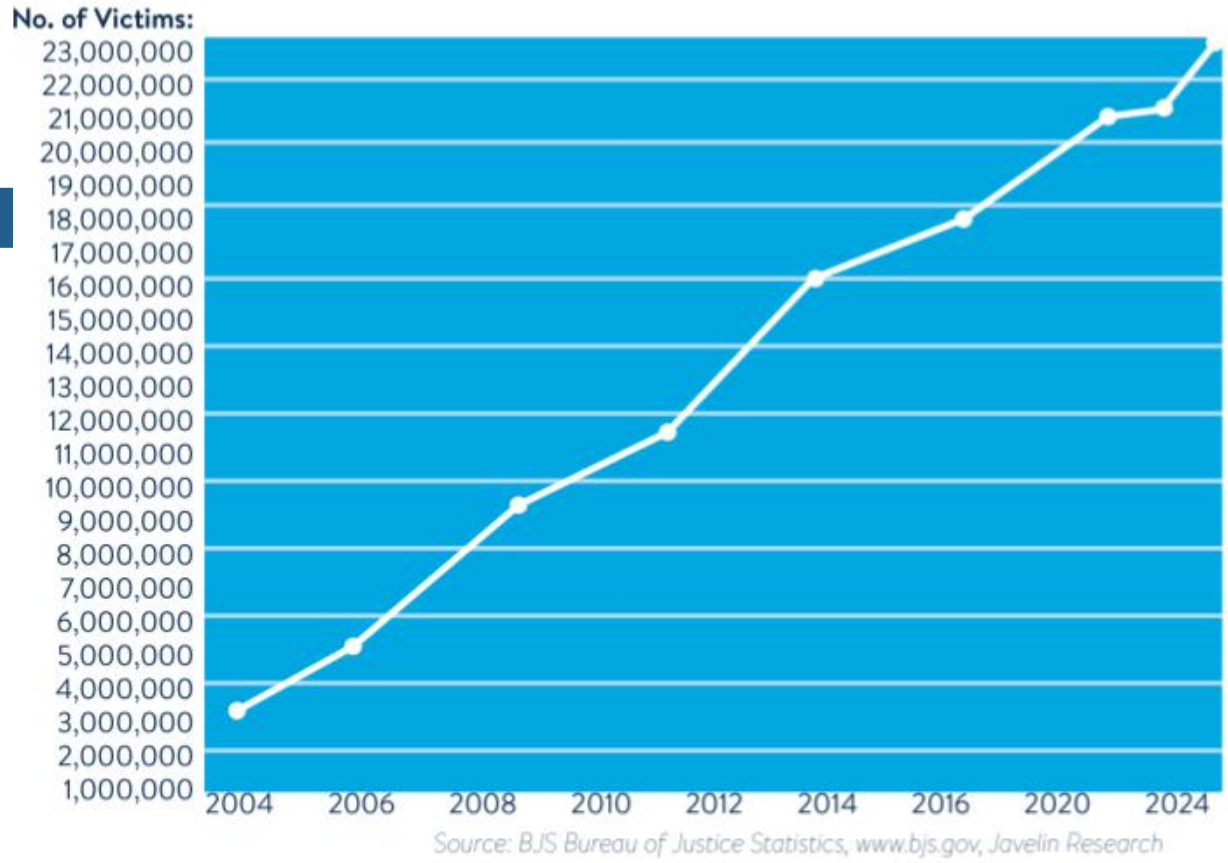
Housing Counseling

We are a HUD-approved housing counseling agency. We provide homebuyer education seminars, mortgage counseling, foreclosure prevention assistance, landlord/ tenant counseling, post-homebuyer education, and reverse mortgage counseling (please call ahead for reverse mortgage appointments).

Bankruptcy Pre-petition Credit Counseling

We provide counseling (and a certificate of completion as mandated by the bankruptcy reform law) for those considering bankruptcy. We also provide financial education (and a certificate of completion as mandated by the bankruptcy reform law) for those completing their bankruptcy discharge.

Introduction



Identity theft has been called the fastest-growing crime in the United States, with over twenty-three million victims per year. The crime has continued to expand over the past 20 years.

Some of the costs were:

- Average loss per victim $880
- Average time to resolve identity fraud is 60 hours

The Bureau of Justice Statistics reported that direct losses to consumers totaled $16.4 billion in 2021.

Not only do identity fraud victims spend money out of pocket to clear up their records, but while they are doing so, victims are unjustly harassed by debt collectors, denied credit or employment opportunities, lose their cars or their homes, or are repeatedly arrested for crimes they did not commit. The ID Theft Resource Center's survey found that 35% of victims had their ability to obtain credit affected, 22% were receiving calls from debt collectors, and 20% had their job (or ability to get a job) impacted.

Identity theft has been the number one consumer complaint filed with the Federal Trade Commission for the past 20 years. The term "identity theft" or "identity fraud" refers to crimes in which someone obtains and uses another person's personal identifying information to commit unlawful acts, usually for financial gain.

Introduction (Cont.)

- Crime impacts people of all ages and income levels. More than half of victims surveyed earn an annual income of less than $50,000.
- The fastest-growing type of Identity Fraud is cybercrime, which costs an estimated $445 billion per year world-wide.
- Consumers who have been involved in an online data breach are 9.5 times more likely to have their identity stolen.
- Each year, identity theft costs Americans more than all other types of property crimes combined.
- New account fraud is on the rise, with 1 in 4 victims with fraudulent new accounts reporting a cell phone or utility account opened. In 2017, account takeover fraud tripled over the previous year.
- Victims report many emotional impacts, with 41% reporting loss of sleep, 65% feeling rage or anger, and 16% reporting suicidal feelings.

1. Bureau of Justice Statisics (BJS), bjs.ojp.gov
2. See the “Federal Trade Commission – Identity Theft Survey Report,” from Synovate. Available at http://www.consumer.gov/idtheft/stats.html.
3. https://bjs.ojp.gov/document/vit21_sum.pdf
4. https://www.idtheftcenter.org/wp-content/uploads/2018/09/ITRC_Aftermath-2018_Web_FINAL.pdf
5. See the Federal Trade Commission’s “FTC Consumer Sentinel Network,” October 17, 2019, available at www.ftc.gov.
6. California Penal Code section 530.5 defines the crime as when a person “willfully obtains personal identifying information…of another person, and uses that information for any unlawful purpose, including obtaining, or attempting to obtain, credit, goods, services, or medical information in the name of the other person without the consent of that person…”
7. Small Business Innovation Research and Small Business Technology Transfer program, https://www.sbir.gov/tutorials/cyber-security/tutorial-1
8. Javelin Strategy & Research, www.javelinstrategy.com
9. Bureau of Justice Statistics, www.bjs.gov
10. ID Theft Resource Center, https://www.idtheftcenter.org/publication/2023-consumer-impact-report/

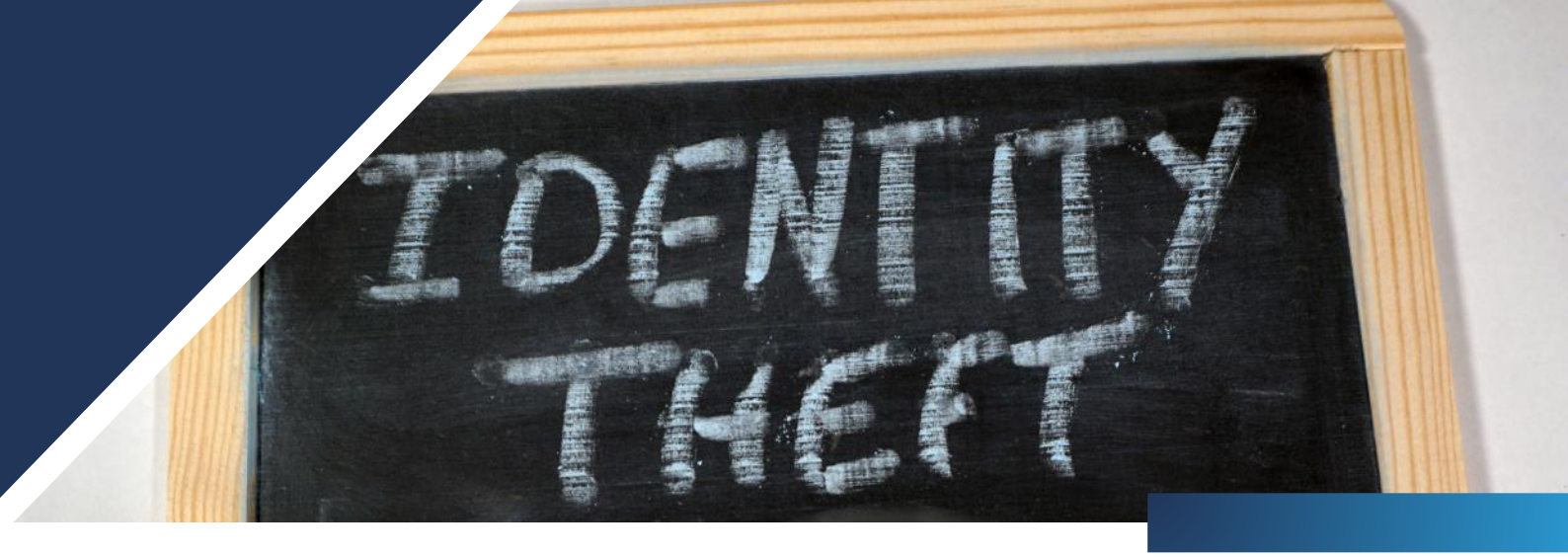
What is Identity Theft?

Identity Theft Basics: Identity theft occurs when thieves steal your personal information—such as your name, address, Social Security number, and financial account details—to commit fraud or other crimes. They might use this information to access your existing accounts, open new ones, or obtain goods and services fraudulently. Common methods include stealing wallets, purses, mail, or through 'dumpster diving' to find personal data. Thieves can also obtain your credit report by posing as someone with a legitimate need for it, like a landlord or employer, further breaching your privacy.

Digital Vulnerability: The digital realm offers additional avenues for identity thieves. They engage in phishing scams by sending emails that appear to be from reputable companies asking for personal information, which should always be treated as fraudulent. Social networking sites also pose a risk; thieves can access profiles to gather information used to guess passwords or security question answers. Moreover, insider theft is a concern, where individuals may pay for your personal information from applications for goods, services, or credit, making it essential to safeguard your data even in seemingly secure transactions.

Exploitation Tactics: Identity thieves are not just content with stealing identities; they exploit them in various damaging ways. They may change the mailing address on your credit card account and rack up charges, open new accounts in your name, establish services, or even file for bankruptcy to avoid paying debts incurred under your stolen identity. These actions can devastate your credit score and financial standing. Thieves might also counterfeit checks or debit cards, buy vehicles, or engage in other fraudulent purchases—all under your name. The sale of your personal information can compound the damage, making it difficult to trace the crime's source and resolve the issues.

Protection Strategies: Protecting yourself from identity theft requires vigilance. Be wary of unsolicited requests for personal information, secure your mail and personal documents, and monitor your financial statements regularly for any unauthorized transactions. In the digital sphere, enhance your cybersecurity measures and be cautious about the personal information you share online. Remember, awareness and proactive measures are your best defense against identity theft, helping you maintain control over your personal and financial information



Identity Theft Prevention Tips

While no one can be 100% safe from identity fraud, the key actions recommended should help to minimize the risks or the pain of becoming a victim of identity fraud. Avoiding identity theft is not simple, but there are several common-sense things that consumers can do. The identity theft problem has been studied for several years and here are some suggestions for consumers:

- Keep personal information in a safe place, such as a safe or lock box, and avoid storing documents in easily accessible places like vehicle glove boxes or day planners.
- Report lost or stolen cards and checks immediately.
- File a police report immediately, indicating the information that was stolen.
- Photocopy all the contents of your wallet. Copy both sides of each license, credit card etc. This way, you will know what you had in your wallet if it is stolen and you will have all the account numbers and phone numbers to call and report the theft. Keep photocopies in a safe place – fire proof lock box, safe, or safety deposit box. Also photocopy your passport.
- File your tax return as soon as possible to avoid the potential for an ID thief to intercept your refund.
- Cancel and cut up unused credit cards – or keep in a fire proof lock box or safe.
- Do not sign the back of your credit cards – instead put “Photo ID Required”
- Don’t give your Social Security or account numbers over the phone to anyone who has called you, or to anyone you don’t know. (Demand to know why your information is needed and how it will be used.)
- Shred documents that contain personal information (bank statements, credit solicitations, tax notices, investment statements, etc.).
- Cancel your paper bills and statements wherever possible and instead have your statements sent to you online and pay bills online.
- If you must use paper statements and receive them in the mail, pay attention to your billing cycles. Follow up with your creditors when your bills don’t arrive on time – it may be a sign that your address was changed by an identity thief who has taken over your account.
- Do not place outgoing mail in your mailbox. Deposit mail in a U.S. mailbox or at the post office to reduce the chance of mail theft.
- Monitor your statements for unauthorized charges and dispute them immediately.

- Refrain from carrying unnecessary information such as PINs, passwords, or Social Security numbers in your wallet or purse.
- Keep highly sensitive financial information (such as bank statements, log-ins for online banking accounts, ATM card PINs, or paper checks) away from where others, including family members, friends, neighbors, and domestic employees, could access it.
- Put passwords on your credit, bank, and phone accounts. Avoid using easily available information like your mother's family name, your birth date, the last four digits of your Social Security number, phone number or a series of consecutive numbers.
- When you order, checks have only your initials of your first and middle name with last name put on them. If someone takes your checkbook, they will not know if you signed your checks with your initials or your first name, but your bank will.
- Store new and canceled checks safely. Also, only carry your checkbook with you when necessary. Have your new checks mailed to a P.O. Box.
- When writing out checks, do not put the full account number in the memo section – only put the last four numbers.
- Retrieve paper mail promptly and deposit mail with sensitive information in a secure outgoing mailbox. Get a locking mail box for your home if you are unable to retrieve it quickly. Forward mail to a local post office when on vacation or business trips, or have a trusted neighbor pick up your mail.
- Find out who can access your personal information at work and verify that access is strictly controlled.
- When responding to email from financial institutions, ignore any Internet links provided and type the known address instead, or call them through their 800 number.
- Use and regularly update firewall, anti-spyware, and anti-virus software.
- Order a copy of your credit report by taking advantage of the free annual report from all three credit bureaus at www.annualcreditreport.com. It is recommended that you check your credit report often.
- Don't register while visiting websites or participate in phone surveys, marketing surveys, or contests (e.g. the car drawing at the mall). Once a company buys a list with your information, you will become a target of their marketing campaign, and this creates one more source for identity thieves to find and appropriate your personal information.
- Opt out of pre-screened or pre-approved credit offers. Contact the National Consumer Credit Reporting Agencies by calling 1-888-5OPT-OUT or 1-888-567-8688. They can stop the selling of your personal information to creditors for pre-approved offers.
- Remove your name from marketing lists. The Direct Marketing Association (DMA) is responsible for notifying its members that they must remove your name from lists they sell. Your name and address will remain in the DMA's consumer exclusion files for five years. Contact them at http://www.dmachoice.org/consumerassistance.php.
- When using social networking sites, take care to ensure the privacy of your personal information and limit what you share. Know the people with whom you are communicating, and only allow trusted individuals to access your profile.

Child Identity Theft

Sometimes thieves steal the identities of minor children. They use this information to get jobs, government benefits, utilities, loans, etc.
Since no one expects their child to need loans or credit, it's unusual to ask for a credit report for a child. Without a regular review of a credit report for signs of fraud, thieves are free to use the child's identity for years in some cases.

Preventing Child Identity Theft
Preventing this kind of fraud is similar to preventing adult ID theft:

- Keep documents secure, and shred anything you discard.
- If you are asked to share your child's Social Security Number, find out why it is needed, how it will be safeguarded, and for how long it will be needed. Don't share that information; if you're not comfortable it will be handled securely.
- Watch your child's internet use; be sure your computer is free of malware or spyware, and that your internet connections are secure.
- Your child's school should send you a disclosure under the Family Educational Rights and Privacy Act (FERPA), outlining your rights and giving you the right to opt out of the release of information to 3rd parties.

Teaching your child to be safe
Besides the usual prevention and recovery methods you would use for your own identity or your children, Teach your children to be careful with their security. Teach them to use secure passwords, and keep those passwords private. Teach them not to give out any information over the internet, and to keep your computers virus-free. Also teach your child to be on the lookout for phishing scams by email or fake popups designed to capture personal information.
Also teach your child to take special care with their social media accounts. Update their privacy settings and be careful what they share and with whom.

Warning signs of child ID theft

- You get a notice from the IRS that your child didn't pay taxes owed
- You are denied benefits because your child is already being paid benefits
- You get calls from bill collectors or credit card offers for your child
- A government agency contacts you to confirm your child's employment

For a form to help you with disputing fraudulent accounts in your child's name, see Appendix III of this booklet.

Medical Identity Theft

Medical records are a rich target for identity thieves–imagine getting a bill in the mail for an organ transplant, or finding out you have just given birth to a baby in a town you've never even visited. These are true stories we've encountered.

When a thief gains access to a victim's medical records, they typically have everything they need to steal an identity in full. And the consequences can be serious–if someone falsely uses your identity to access medical services, your records may be altered. If you have a serious allergy, but the ID thief doesn't, your life could be put in jeopardy if that allergy is removed from your records.

Medical ID Theft takes many forms:

Drug dealing: Thieves will use stolen identities to obtain prescription drugs they can then sell on the black market.

Professional fraud: Shady clinics and fly-by-night health care providers may misuse health records to over-bill your insurance company, falsely claim they provided services that you never received, or to access drugs for illicit uses.

Illegally borrowing Medicare IDs: Sometimes people will approach victims with a hard-luck story about needing life-saving medical care but being denied by the hospital. The well-meaning victim is asked to share their Medicare ID number.

Phony collections: Scammers call victims and claim to be collecting a payment toward a Medicare-related bill, and take payments right over the phone.

Be on the lookout for signs of fraud:

- If you are charged for medical services you never received.
- If you are billed for the same service more than once.
- The dates of medical services or office visits don't look familiar.
- You receive collection notices for medical services or equipment that aren't yours.

If you think your medical records may have been compromised, contact:

Report suspected Medicare fraud:
Department Of Health & Human Services
Office Of Inspector General Hotline
1-800-447-8477 (1-800-HHS-TIPS)
OIG.HHS.gov/fraud/hotline

Report questionable charges to Medicare:
Medicare Call Center and Senior Medicare Patrols
1-800-633-4227 (1-800-MEDICARE)
medicare.gov

See if your insurer uses Midas Protection: www.midasprotection.com

Tools for Victims

A key defensive tool that has been available to identity theft victims for several years is the fraud alert. A fraud alert is a message that an identity theft victim can place on his or her credit file, which alerts credit issuers who are doing a credit check in response to an application for new credit in the victim's name to fraud associated with the account.

An initial fraud alert lasts one year and is intended to prompt the credit issuer to call a given phone number or ask for additional proof of identity to verify that the applicant is not the imposter. Some victims reported that fraud alerts were not effective and that new accounts were opened in their names even though fraud alerts were in place. The extended fraud alert lasts 7 years and provides similar protections as the one-year alert, but longer. California's security freeze law, which took effect in July 2002, gives victims and other consumers the ability to control access to their credit files. A freeze stops essentially all access to a credit file and lasts until the consumer removes it or "thaws" it temporarily.1

Other new victim rights and tools were extended nationwide with amendments to the federal Fair Credit Reporting Act enacted in 2018.2 Some of these provisions simply codified existing practices of the credit bureaus, such as the single-call process, where a call to the fraud number of one credit bureau also notifies the other two, and the initial fraud alert. There is now an opportunity for the victim or potential victim to add his or her phone number to the fraud alert, indicating that a creditor should not issue new credit unless the victim is called to authorize it.

After the Equifax data breach of 2017, the Economic Growth, Regulatory Relief, and Consumer Protection Act amended the FCRA. This Act made obtaining a credit freeze free in all states. The victim may sue in state or federal court any entity who violates the FCRA.

Many states may still have their own consumer reporting laws, which may give consumers more rights than the federal law.

Among the new identity theft provisions in the Fair Credit Reporting Act that are still pending are "red flag" guidelines, procedures for creditors intended to allow them to spot and prevent fraudulent transactions before they are completed.

1. A consumer whose file is frozen is given a PIN to use to temporarily thaw or lift the freeze to seek new credit. When a security freeze is in place, access to the credit file is still available to the consumer; the consumer's existing creditors for account monitoring purposes, and debt collectors. See Civil Code section 1785.11.2 et seq.
2. Most of the new consumer and identity theft victim rights added to the Fair Credit Reporting Act took effect in fall 2018, with updated disclosures to consumers. - https://www.ftc.gov/system/files/545a_fair-credit-reporting-act-0918.pdf.

Your Rights Under the Law

Victims as Their Own Investigators
Victims of even the more common credit-related forms of identity theft report that they have to shoulder the burden of clearing up their records and performing much of the investigation of their own cases. This can involve hours of phone calls and letter writing over months and even years; victims have said that it's like having a second job.

In 2001, a California law was passed that gave identity theft victims who had a police report access to applications and other records on fraudulently opened accounts. An identity thief who remains at large can continue to use the victim's information, requiring the victim to go through the process of clearing up records over and over again.

In criminal identity theft cases, an at-large thief can nearly bring the victim's life to a halt: preventing the victim from driving, being insured or working, from having custody of his or her children, or from moving about without being arrested. The time and expense necessary to deal with the situation are significant.

The Worst-Case scenario: Criminal Identity Theft
Identity theft may involve far more than money and time. Criminal identity theft occurs when an imposter gives another person's name and personal information to a law enforcement officer upon arrest or during an investigation. In some cases, the imposter may provide a counterfeit driver's license or other identification card. The victim of this kind of identity theft may lose their driver's license, be arrested mistakenly and repeatedly, and be unable to get work, sometimes for years. The FTC found in its 2003 survey that 4% of identity theft victims are victims of criminal identity theft. Those numbers mean there were nearly 400,000 such victims nationwide in 2003.

California Identity Theft Registry
To address the extreme difficulties faced by criminal identity theft victims, legislation created the California Identity Theft Registry in the Department of Justice, along with court processes for getting into the Registry and for sealing or destroying wrongful criminal records. Victims of criminal identity theft who provide fingerprints and a Judicial Finding of Factual Innocence from a court can apply to enter the Registry. They are then given a PIN and the Registry's toll-free number, which the victims can use to clear themselves when stopped by police. Registry staff members also send letters to employers verifying a victim's status. The Registry has been available since 2001.

Your Rights Under FACTA

The Fair and Accurate Credit Transaction Act of 2003, (FACTA) amended the federal Fair Credit Reporting Act, (FCRA) by adding new sections intended primarily to help consumers fight the growing crime of identity theft. Accuracy, privacy, limits on information sharing, and new consumer rights to disclosure are included in FACTA. Below are a few of the new consumer rights:

Free Credit Reports
Recognizing the benefit of self-monitoring, Congress adopted a new rule that allows you a free copy of your credit report annually from each of the "big three." To order your free reports go to www.annualcreditreport.com where you can order your reports directly or download the Annual Credit Report Request form to mail in your request. You can also call 877-322-8228.

Placing Fraud Alerts on Your Credit File
There are two types of fraud alerts: an initial alert, and an extended alert.
An initial alert stays on your credit report for one year:
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 one free report from each of the three nationwide consumer reporting companies.

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." 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.
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 SSN, name, address, etc.
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. To compensate for possible delays this may cause, 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.

Red Flags Rule
Under the Identity Theft Red Flags Rule, creditors and lenders must implement programs designed to prevent identity theft by identifying suspicious behavior in borrowing. When applying for credit, you may face a stricter verification process to ensure your identity, and your accounts will be monitored for suspicious activity.

Active Duty Alerts For Military Personnel

The last thing you want to worry about while you're on deployment is someone assuming your identity to commit financial fraud. Now, you don't have to. Amendments to the Fair Credit Reporting Act allow you to place an "active duty alert" in your credit report. According to the Federal Trade Commission, one of the agencies that enforce the FCRA, the alert requires creditors to verify your identity before granting credit in your name.

Your credit report contains information on where you live, how you pay your bills, and whether you've been sued, arrested, or filed for bankruptcy. Nationwide consumer reporting agencies sell the information in your report to creditors, insurers, employers, and other businesses that use it to evaluate applications for credit, and a host of other activities, including insurance, employment, or renting a home.

Your credit report can be a tool to help you guard against – or discover – identity theft, which occurs when someone uses your personal information – like your name, social security number, or your credit card number – to commit fraud. Identity thieves may use your information to open a new credit card account in your name. Then, when they don't pay the bills, the delinquent account is reported on your credit report. Inaccurate or fraudulent information could affect your ability to get credit, insurance, or housing, now or in the future. People whose identities have been stolen can spend months or years cleaning up the mess the thieves have made of their names and credit records.

If you are a member of the military and away from your usual duty station, you may place an active duty alert on your credit reports to help minimize the risk of identity theft while you are deployed. When a business sees the alert on your credit report, it must verify your identity before issuing you credit. The business may try to contact you directly, but if you're on deployment, that may be impossible. As a result, the law allows you to use a personal representative to place or remove an alert. Active duty alerts on your report are effective for one year, unless your request that the alert be removed sooner. If your deployment lasts longer, you can place another alert on your credit report.

To place an active duty alert, or to have it removed, call the toll-free fraud number of one of the three nationwide consumer reporting companies: Equifax, Experian, or Trans Union. The company will require you to provide appropriate proof of your identity, which may include your social security number, your name, address, and other personal information. The company you call is required to contact the other two, and they will place an alert on their versions of your report. If your contact information changes before your alert expires, remember to update it.

When you place an active duty alert, you'll be removed from the credit reporting companies' marketing list for pre-screened credit card offers for two years - unless you ask to go back on the list before then. Prescreened offers – sometimes called "pre-approved" offers – are based on information in your credit report that indicates you meet certain criteria set by the offer.

Equifax : 1-800-525-6285 ; www.equifax.com
Experian : 1-888-EXPERIAN (397-3742) ; www.experian.com
TransUnion : 1-800-680-7289 ; www.transunion.com

Disputing Inaccurate Information

Previously, disputes about the accuracy of information in a consumer report had to be made directly to the consumer reporting agency. Under new FACTA provisions, a consumer may dispute inaccurate information directly with a "furnisher," that is, a creditor that is a financial institution. Upon notice of disputed information, the furnisher must investigate and cannot report negative information while the investigation is pending.

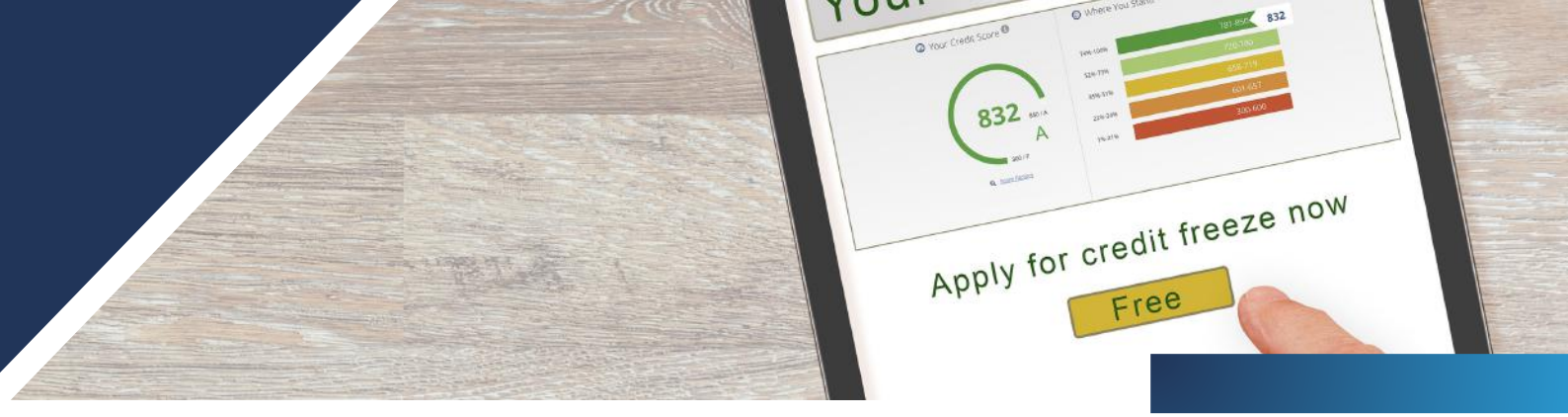
Notice of Negative Information
The number one tip for detecting identity theft is to check your credit report. Erroneous information about late payments and collection actions is what you don't want to see. Like a lot of people, ordering your credit report is probably high on your "to do" list, but it never seems to get to the top of that list.
FACTA now requires creditors to give you what might be called an "early warning" notice. This notice could alert you that something is amiss with an account. However, the notice is not a substitute for your own close monitoring of credit reports, bank accounts, and credit card statements. And, you may have to look closely to see this new notice even.

Nationwide Specialty Consumer Reporting Agencies
Consumer reports are generally thought to mean "credit" reports issued by one of the three national credit bureaus: Experian, TransUnion, or Equifax. However, consumer reports may also be issued for purposes other than credit applications. The FCRA also covers reports for insurance, employment, check writing, and housing rental history. Such reports are quite common, and many companies now specialize in providing reports for these specific purposes.

FACTA defines companies that issue non-credit reports as a "nationwide specialty consumer reporting agency" when reports relate to:

- Medical Records or payments (MIB)
- Residential or Tenant History (First Advantage SafeRent)
- Check writing history (CheckSystems/SCAN/Telecheck)
- Employment History Report (Choicepoint)
- Insurance Claims – Home/Auto insurance (Choicepoint)

As of December 2004, consumers may ask for a free report annually from any of the specialty agencies.
If you are a victim of identity theft, you may want to ask for a copy of the nationwide specialty consumer reports and inform them that you are as victim. If you have a negative entry due to identity theft on any of the
above specialty consumer reports, your rights allow you to dispute these items just as you would with one of the three credit reporting agencies. For more on "specialty" reports, see the Privacy Rights Clearinghouse (PRC) Fact Sheet 6b, The 'Other' Consumer Reports: What You Should Know about 'Specialty' Reports, https://privacyrights.org/consumer-guides/other-consumer-reports-what-you-should-know-about-specialty-reports.



Credit Security Freeze Law

All states now have credit security freeze programs, but not all programs are the same and vary from state to state depending on the laws each state has passed. You may search specifics for your state's credit freeze and security alerts at: www.idtheftcenter.org.
Since 2018, the security freeze is free of charge by federal law.
If you put a "security freeze" on your credit file, your file cannot be shared with potential creditors. A security freeze can help prevent identity theft. Most businesses will not open credit accounts without first checking a consumer's credit history. If your credit files are frozen, even someone who has your name and Social Security number would probably not be able to get credit in your name.
To place a freeze, you must write to each of the three credit bureaus and provide identifying information.

Equifax Security Freeze **P.O. Box 105788 Atlanta, GA. 30348**	**Include name, current and former address, Social Security Number, and date of birth. Enclose a copy of a current utility bill or other proof of current address.**
Send by certified Mail.	**Pay by check, money order, or credit card (AMEX, Visa, Master Card or Discover only). Give name of credit card, account number, expiration date, and Card Identification Number.**
Experian Security Freeze **P. O. Box 9554** **Allen, TX 75013**	**Include full name, with middle initial and Jr./Sr., etc. Include current address and home addresses for past two years, Social Security number, and birth date. Enclose a copy of a government identification card, such as a driver's license, state ID card or military ID card, and one copy of a utility bill, insurance or bank statement, etc., showing your name and current mailing address.**
Send by certified mail.	**Pay by check, money order or credit card. Give name of credit card, account number and expiration date.**

TransUnion Security Freeze **P. O. Box 6790** **Fullerton, CA 92834-6790**	**Include first name, middle initial, last name, Jr., etc. Current home address, Social Security number, and birth date.**
Send by regular or certified mail.	**Pay by credit card. Give name of credit card, account number and expiration date.**

Can I open new credit accounts if my files are frozen?

Yes. If you want to open a new credit account or get a new loan, you can lift the freeze on your credit file. You can lift it for a period of time. Or you can lift it for a specific creditor. After you send your letter asking for the freeze, each of the credit bureaus will send you a Personal Identification Number (PIN). You will also get instructions on how to lift the freeze. You can lift the freeze by phone, using your PIN. The credit bureaus must lift your freeze within three days.

Opting Out

Opting out of PRE-Screened/PRE-Approved Credit Offers of Credit Reports for Marketing

Can the information in my credit file be used for any other purposes?

Yes. The practice of generating and selling lists for use in “pre-approved” credit and insurance offers is allowed by law. TransUnion, Experian and Equifax all engage in selling lists of consumers who meet certain criteria in order to receive a “firm” offer of credit or insurance. This is the source of the many pre-approved credit offers most consumers receive in the mail. Pre-approved and so-called “firm” offers of credit, however, can be somewhat misleading. A creditor may legally look at your report before making the offer (soft inquiry). If you respond, the creditor may again access your report before you are actually granted credit (hard inquiry). They can deny your credit application at that time. This is explained in the fine print on the pre-approved offer.

The law does not allow credit reporting agencies to compile and sell information from credit reports for direct marketing. You can remove your name from any list compiled by a credit reporting agency, whether the list is for pre-approved credit offers or direct marketing. To “opt-out,” that is, to remove your name from mailing lists compiled by credit bureaus, call the toll-free number all credit reporting agencies are required by law to maintain for this purpose:

Call (888) 5-OPTOUT or (888) 567-8688 to opt out of pre-approved offers for credit or go online to www.optoutprescreen.com.
This phone number can be used to remove your name from the list of all three CRAs. You may also write to the credit reporting agencies:

You may remove your name from marketing lists. The Direct Marketing Association (DMA) is responsible for notifying its members that they must remove your name from lists they sell. Your name and address remain in the DMA’s consumer exclusion files for five years.
–Contact them at www.dmachoice.org/consumerassistance.php

What To Do if You Are a Victim?

You can protect yourself and, most importantly, educate yourself on what steps to take if you feel that you are a victim of identity theft. if any of your personal identifying information (social security number, financial account numbers, and/or password; birth date; name; address and telephone number) has been lost or stolen, or if you suspect that your personal information has been used to commit fraud or identity theft, take immediate action. Reporting this identity theft immediately and keeping detailed records of your actions are very important and can reduce the time it takes to resolve this crime.

Keep Accurate Records

Accurate and complete records will greatly improve your chances of resolving your identity theft case;

- Follow up in writing with all contacts you have made by phone or in person. Use certified mail, return receipt requested.
- Keep copies of all correspondence or forms you send.
- Keep a log and write down the name of anyone you talk to, what he or she told you, and the date and time of the conversation. Use the track your progress form in this booklet to help you.
- Keep the originals of supporting documentation, like police reports, and letters to and from creditors; send copies only.
- Set up a filing system for easy access to your paperwork.
- Keep old files even if you believe your case is closed. One of the most difficult and annoying aspects of identity theft is that errors can reappear on your credit reports or your information can be re-circulated. Should this happen, you'll be glad you kept your files.

Report Your Identity Theft

While resolving credit problems resulting from identity theft can be time consuming and frustrating, the good news is, there are procedures under the federal laws for correcting credit report and billing errors, and stopping debt collectors from contacting you about debts you don't owe.

What To Do if You Are a Victim? (Cont.)

Top Five Steps to Take:

1. Place a fraud alert on your credit report by contacting one of the major credit reporting agencies.
2. File a police report with your local law enforcement agency (police department or sheriff's department where the fraud occurred).
3. Call your creditors and banks and immediately; close any of your open accounts and obtain new account numbers with new PINs and passwords. Close all fraudulent accounts opened in your name.
4. Send an ID Theft Affidavit (certified mail, return receipt requested) to creditors, banks, collection agencies, credit reporting agencies to notify them of your case.
5. File a complaint with the Federal Trade Commission (FTC).

Identity Theft Checklist

Use the following checklist to help you clear up your records. It lists the actions most identity theft victims should take to limit the damage done by the thief. For more information, see the websites of the Federal Trade Commission at www.consumer.gov/idtheft, the Identity Theft Resource Center at www.idtheftcenter.org, and the Privacy Rights Clearinghouse at www.privacyrights.org.

Report fraud to the three major credit bureaus.
You can report the identity theft to all three of the major credit bureaus by calling any one of the toll-free fraud numbers below. You will reach an automated telephone system and you will not be able to speak to anyone at this time. The system will ask you to enter your Social Security number and other information to identify yourself. The automated system allows you to flag your file with a fraud alert at all three bureaus. This helps stop a thief from opening new accounts in your name. The alert stays on for 90 days. Each of the credit bureaus will send you a letter confirming your fraud alert and giving instructions on how to get a copy of your credit report. As a victim of identity theft, you will not be charged for these reports. Each report you receive will contain a telephone number you can call to speak to someone in the credit bureau's fraud department.

Experian 1-888-397-3742
Equifax 1-800-525-6285
Trans Union 1-800-680-7289

Write to the credit bureaus.
Write a letter to each credit bureau. Repeat what you said in your telephone call (see above). Send copies of your police report and completed ID Theft Affidavit. Remind the credit bureaus that they must block or remove any information that you, as an identity theft victim, say is a result of the theft. Send your letters by certified mail, return receipt requested. Keep a copy of each letter.

Equifax
P.O Box 740241
Atlanta, GA 30374-0241

Experian
P.O. Box 9530
Allen, TX 75013

Trans Union
P.O. Box 6790
Fullerton, CA 92834

As an alternative, you may dispute items with the credit bureaus online. Look for "dispute" on their web sites: www.equifax.com, www.experian.com, and www.transunion.com.

Identity Theft Checklist (Cont.)

Report the crime to the police.
You can report identity theft to your local police department. Ask the police to issue a police report of identity theft. Give the police as much information on the theft as possible. One way to do this is to provide copies of your credit reports showing the items related to identity theft. Black out other items not related to identity theft. Give the police any new evidence you collect to add to your report. Be sure to get a copy of your police report. You will need to give copies to creditors and the credit bureaus. For more information, see “Organizing Your Identity Theft Case” by the Identity Theft Resource Center, available at www.idtheftcenter.org/

Request information on fraudulent accounts.
When you file your police report of identity theft, the officer may give you forms to use to request account information from credit grantors, utilities or cell phone service companies. If the officer does not do this, you can use the form available from the Office of Privacy Protection at their web site, http://www.privacy.ca.gov/lawenforcement/lawenforcement.htm. Click the link titled “Requesting Fraudulent Transaction or Account Information”. When you write to creditors where the thief opened or applied for accounts, send copies of the forms, along with copies of the police report. Give the information you receive from creditors to the officer investigating your case.

Call creditors.
Call creditors for any accounts that the thief has opened or used. When you call, ask for the security or fraud department. Examples of creditors are credit card companies, other lenders, phone companies, other utility companies, and department stores. Tell them you are an identity theft victim. Ask them not to hold you responsible for new accounts opened by the thief. If your existing credit accounts have been used fraudulently, ask the credit issuers to close those accounts and to report them to credit bureaus as “closed at consumer’s request.” If you open a new account, have it set up to require a password or PIN to approve use. Don’t use your mother’s maiden name or the last four numbers of your Social Security number as your password. Ask the creditors to give you copies of documentation on the fraudulent accounts (see above item). For more information on what to tell creditors, see the Federal Trade Commission’s “Take Charge: Fighting Back Against Identity Theft,” available at http://www.ftc.gov/bcp/conline/pubs/credit/idtheft.htm

Identity Theft Checklist (Cont.)

Write to creditors.
Write a letter to each creditor where an account was opened or used in your name. Repeat what you said in your telephone call. Send a copy of your police report. Black out the account number of any accounts with other creditors on a copy of your completed ID Theft Affidavit and send it.

Review your credit reports carefully.
When you receive your credit reports, read them carefully. Look for accounts you don't recognize. Look in the inquiries section for names of creditors from whom you haven't asked for credit. You may find some inquiries identified as "promotional." These occur when a company has gotten your name and address from a credit bureau to send you an offer of credit. Promotional inquiries are not signs of fraud. (By calling to report identity theft, your name will be automatically removed from the mailing list to receive unsolicited credit offers of this kind.) Also, as a general precaution, look in the personal information section to verify your Social Security number, address, and name.
If you find anything you don't understand, call the credit bureau at the telephone number listed on the report. Tell them you want to block or remove any information on the report that is the result of identity theft. (You must send a police report of identity theft to support this request.) Order new credit reports every three months or so until your situation has cleared up. You may have to pay $8 or $9 for each report, but ask for additional free copies as an identity theft victim. For more on what to tell the credit bureaus, see the Privacy Rights Clearinghouse's "Identity Theft: What to Do When It Happens to You" at http://www.privacyrights.org/fs/fs17a.htm.

Use the ID Theft Affidavit.
Creditors may ask you to fill out fraud affidavits. The credit bureaus accept the Federal Trade Commission's ID Theft Affidavit and by most major creditors. Send copies of the completed form to creditors where the thief opened accounts in your name. Also send copies to creditors where the thief made charges on your account, to the credit bureaus, and to the police. The form is available on the FTC web site at http://www.ftc.gov/bcp/conline/pubs/credit/affidavit.pdf. File a complaint of identity theft with the FTC. See their web site at www.consumer.gov/idtheft. The FTC keeps a database of identity theft cases that is used by many law enforcement agencies.

Identity Theft Checklist (Cont.)

If your checks, ATM card or bank account information are lost or stolen
Call the bank and close your bank account. Open a new one with a new account number. Tell the bank you want to use a new password for access to your new account. Do not use your mother's maiden name or the last four digits of your Social Security number. Ask your bank to notify the check verification company it uses. Report stolen checks to the check verification companies that retail stores use. You can also contact major check verification companies.

Ask that they notify retailers who use their databases not accept the checks on your closed account. Call TeleCheck at 1-800-710-9898 and Certegy, Inc. at 1-800-437-5120. To find out if the identity thief has passed bad checks in your name, call SCAN at 800-262-7771. Follow up by writing to your bank. Send your letter by certified mail. Return receipt requested.

If a debt collector contacts you
Tell the debt collector that you are the victim of identity theft. Say that you dispute the validity of the debt. Say that you did not create the debt and are not responsible for it. Send the collector a follow-up certified letter saying the same things. Include a copy of your police report and of any documents you've received from
the creditor. Send the letter by certified mail. Return receipt requested. If the debt collector is not the original creditor, be sure to send your letter within 30 days of receiving the collector's first written demand for payment.

If your driver's license or DMV-issued ID card is stolen
Immediately contact your local Department of Motor Vehicles office to report the theft. Ask them to put a fraud alert on your license. Then call the toll-free DMV Fraud Hotline at 866-658-5758. If the thief is using your license as an identity card, you may want to change your license number. Ask the DMV for an appointment, and when you go, take a copy of the police report and copies of bills or other items supporting your claim of fraud. You will also need to prove your identity. Take current documents such as a passport, birth certificate, a certification of citizenship or naturalization, or a U.S. military photo ID. The DMV will issue a new driver's license or ID card number when you meet all the requirements. For more information, see "Identity Theft: Have You Been A Victim of Identity Theft? DMV Can Help," available at www.dmv.ca.gov/pubs/brochures/fast_facts/ffdl24.htm

Identity Theft Checklist (Cont.)

If your mail was stolen or your address changed by an identity thief
Notify the Postal Inspector if you think the identity thief has stolen your mail or filed a change of address request in your name. To find the nearest Postal Inspector, look in the white pages of the telephone book for the Post Office listing under United States Government. Or go to the Postal Inspection Service's web site at www.usps.com/postalinspectors/idthft_ncpw.htm.

If you are wrongly accused of a crime committed by an identity thief
"Criminal identity theft" is a label given to a particular type of identity theft. Criminal identity theft occurs when a suspect in a criminal investigation identifies himself or herself using the identity of another, innocent person. A special database in the California Department of Justice can help victims of this kind of identity theft. See the Office of Privacy Protection's Consumer Information Sheet 8: "How to Use the California Identity Theft Registry - A Guide for Victims of 'Criminal' Identity Theft," available on our Identity Theft Web page at http://www.privacy.ca.gov/cover/identitytheft.htm.

If someone uses your Social Security number to claim unemployment benefits or to work
If you suspect that someone else has claimed unemployment benefits using your Social Security number, call the California Employment Development Department's toll-free Fraud Hotline at 800-229-6297. For more information, see their website at www.edd.ca.gov. It's a good idea to check your Social Security earnings record by calling1-800-772-1213. Or get a Request for Social Security Statement (Form 7004) at http://www.ssa.gov/online/ssa-7004.html. If a thief is using your Social Security number, call the Social Security Fraud Hotline at 1-800-269-0271.

Stop pre-approved credit offers
Stop most pre-approved credit card offers. They make a tempting target for identity thieves who steal your mail. Have your name removed from the credit bureau marketing lists. Call toll-free 1-888-5OPTOUT (1-888-567-8688).

Identity Theft Checklist (Cont.)

If your Passport is lost or stolen

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 their website. You may access the USDS Passports page at www.travel.state.gov/passport/index.html, or call a local USDS field office. Local field offices are listed in the Blue Pages of your telephone directory.

If someone opened phone service in your name or you have fraudulent charges

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.

If Student Loans are taken out in your name fraudulently

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.

Identity Theft Checklist (Cont.)

Tax Fraud

Internal Revenue Service (IRS) www.treas.gov/irs/ci. The 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 website 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."

Bankruptcy Fraud

If you believe someone has filed for bankruptcy using your name, write to the U.S. Trustee in the region where the bankruptcy was filed or go to their nationwide office locator website at www.usdoj.gov/ust/ustofc.htm.

Real Estate/Mortgage Fraud

Thieves use fake documents, including bank account statements, and false or stolen driver's licenses and social security number, to buy the homes. In many cases, the properties were quickly sold or flipped for a profit.

Resources

Identity Theft Resource Center

A national nonprofit organization dedicated to helping people who are victims of identity theft and to advising governments and corporations about ID theft. 1-858-693-7935 www.idtheftcenter.org

Institute of Consumer Financial Education, ICFE

The Institute of Consumer Financial Education (ICFE) is a nonprofit education organization dedicated to helping consumers of all ages to improve their spending, increase savings and use credit more wisely. The ICFE trains and certifies Personal Finance Instructors for its own curriculum, The Money Instruction Book. It also has curriculums for ICFE Certified Credit Report Reviewers and ICFE Certified Identity Theft Risk Management Specialists.

Paul Richard, RFC, President
P.O. Box 34070
San Diego, CA. 92163
1-619-239-1401
www.ICFE.info and www.financial-education-icfe.org

Identity Theft Information and Assistance: California Office of Privacy Protection

The California Office of Privacy Protection (COPP), in the California Department of Consumer Affairs, is the only state agency in the country dedicated to consumer privacy. Created by legislation enacted in 2000, the four-year-old Office undertakes many activities to address identity theft.
One of the primary functions of COPP is to help consumers who contact it with privacy concerns or complaints. Individuals can contact COPP on its toll-free phone line, 866-785-9663, or by e-mail to privacy@dca.ca.gov. Identity theft is the most common concern of those who call or email the Office, representing 61% of all contacts: 9% are identity theft victims and 52% are concerned about becoming a victim. COPP also provides consumers with information and education on identity theft and other privacy issues. The primary vehicle for disseminating information is the COPP Web site, www.privacy.ca.gov, which contains materials for consumers, business and law enforcement. The Web site includes a page devoted entirely to identity theft, containing COPP's consumer information sheets and links to other resources.

Federal Deposit Insurance Corporation

Consumers are protected against liability for unauthorized accounts or transactions under federal and state law and by financial industry practices. The evolution of Identity theft includes the spread of fraudulent "phishing" e-mails. These are unsolicited emails purportedly from a legitimate source - perhaps your bank, utility company, well known merchants, your Internet service provider or even a trusted government agency such as the FDIC - attempting to trick you into divulging personal information. If you suspect an e-mail or Web site is fraudulent, please report this information to the real bank, company or government agency, using a phone number or e-mail address from a reliable source. Example: If your bank's Web page looks different or unusual, contact the institution directly to confirm that you haven't landed on a copycat Web site set up by criminals. Also, contact the Internet Crime Complaint Center (www.ifccfbi.gov), a partnership between the FBI and the National White Collar Crime Center. www.fdic.gov/consumers

Resources (Cont.)

Identity Theft Resource Center

A national nonprofit organization dedicated to helping people who are victims of identity theft and to advising governments and corporations about ID theft. 1-858-693-7935 www.idtheftcenter.org

Institute of Consumer Financial Education, ICFE

The Institute of Consumer Financial Education (ICFE) is a nonprofit education organization dedicated to helping consumers of all ages to improve their spending, increase savings and use credit more wisely. The ICFE trains and certifies Personal Finance Instructors for its own curriculum, The Money Instruction Book. It also has curriculums for ICFE Certified Credit Report Reviewers and ICFE Certified Identity Theft Risk Management Specialists.

Paul Richard, RFC, President
P.O. Box 34070
San Diego, CA. 92163
1-619-239-1401
www.ICFE.info and www.financial-education-icfe.org

Identity Theft Information and Assistance: California Office of Privacy Protection

The California Office of Privacy Protection (COPP), in the California Department of Consumer Affairs, is the only state agency in the country dedicated to consumer privacy. Created by legislation enacted in 2000, the four-year-old Office undertakes many activities to address identity theft.
One of the primary functions of COPP is to help consumers who contact it with privacy concerns or complaints. Individuals can contact COPP on its toll-free phone line, 866-785-9663, or by e-mail to privacy@dca.ca.gov. Identity theft is the most common concern of those who call or email the Office, representing 61% of all contacts: 9% are identity theft victims and 52% are concerned about becoming a victim. COPP also provides consumers with information and education on identity theft and other privacy issues. The primary vehicle for disseminating information is the COPP Web site, www.privacy.ca.gov, which contains materials for consumers, business and law enforcement. The Web site includes a page devoted entirely to identity theft, containing COPP's consumer information sheets and links to other resources.

Federal Deposit Insurance Corporation

Consumers are protected against liability for unauthorized accounts or transactions under federal and state law and by financial industry practices. The evolution of Identity theft includes the spread of fraudulent "phishing" e-mails. These are unsolicited emails purportedly from a legitimate source - perhaps your bank, utility company, well known merchants, your Internet service provider or even a trusted government agency such as the FDIC - attempting to trick you into divulging personal information. If you suspect an e-mail or Web site is fraudulent, please report this information to the real bank, company or government agency, using a phone number or e-mail address from a reliable source. Example: If your bank's Web page looks different or unusual, contact the institution directly to confirm that you haven't landed on a copycat Web site set up by criminals. Also, contact the Internet Crime Complaint Center (www.ifccfbi.gov), a partnership between the FBI and the National White Collar Crime Center. www.fdic.gov/consumers

Resources (Cont.)

U.S. Department of Justice

The Department of Justice prosecutes cases of identity theft and fraud under a variety of federal statutes. Federal prosecutors work with federal investigative agencies such as the Federal Bureau of Investigation, the United States Secret Service, and the United States Postal Inspection Service to prosecute identity theft and fraud cases. Call: 1-888-880-0240
http://www.usdoj.gov/criminal/fraud/idtheft.html

U.S. Secret Service

The Secret Service was established as a law enforcement agency in 1865. While most people associate the Secret Service with Presidential protection, our original mandate was to investigate the counterfeiting of U.S. currency--which we still do. Today, our primary investigative mission is to safeguard the payment and financial systems of the United States. Since 1984, our investigative responsibilities have expanded to include crimes that involve financial institution fraud, computer and telecommunications fraud, false identification documents, access device fraud, advance fee fraud, electronic funds transfers, and money laundering as it relates to our core violations.
www.secretservice.gov Financial Crimes Division:
www.treas.gov/usss/financial_crimes.shtml.

Credit Reporting Agencies

EXPERIAN
1-888-397-3742
https://www.experian.com/identity_fraud/victim_assistance.html

EQUIFAX
1-800-525-6285
https://ww2.equifax.com/identity-theft-protection

TRANSUNION
1-800-680-7289
http://www.transunion.com/identity-theft

Nationwide Specialty Consumer Reporting Agencies

A-PLUS Report
Insurance Services Office ISO
1-800-627-3487
www.iso.com/

CERTEGY Check Services (Previously Equifax Check Systems)
1-800-437-5120

CROSSCHECK
1-800-552-1900

TELECHECK
1-800-710-9898
https://www.firstdata.com/telecheck/index.htm

CHECKSYSTEMS
1-800-428-9623
http://chexsystems.com

Resources (Cont.)

Choicepoint
1-866-312-8076
https://personalreports.lexisnexis.com

CoreLogic SafeRent—Residential/Tenant History
1-888-275-4837
http://www.corelogic.com/landing-pages/saferent-consumer.aspx

MIB – Medical Records or payments
1-866-692-6901
TTY 1-866-346-3642
http://www.mib.com/

Federal government agencies

Attorney general's office
http://www.naag.org

Bankruptcy U.S. Trustee Offices
Click link “Nationwide Office Locator” on website
http://www.usdoj.gov/ust/

CA Department Of Motor Vehicles
1-866-658-5758
Email DLFraud@dmv.ca.gov

Federal Government Information Center Passport Office
1-800-688-9889

Federal Trade Commission
1-877-IDTHEFT or (1-877-438-4338)
http://www.consumer.gov/idtheft/

National Fraud Information Center Internet & Telemarketing Fraud
1-800-876-7060
http://www.fraud.org/

Office of Privacy
1-866-785-9663
www.privacy.ca.gov

Social Security Administration
1-800 269-0271 to report fraud or TTY number, 1-800-325-0778
http://www.oig.ssa.gov/report

Us Postal Inspection Service
1-800-275-8777 Office Locator Website
https://postalinspectors.uspis.gov

Appendix I

REQUEST FOR FRAUDULENT TRANSACTION/ACCOUNT INFORMATION

The facing page offers a sample letter to send to request account information from creditors and other financial institutions related to a fraudulently opened account or fraudulent transaction.

By law, you are entitled to this information free of charge, but some creditors are resistant to complying as it requires extra effort on their part. If you use the text we provide and enclose a copy of the relevant section of the Fair Credit Reporting Act (included on the next four pages), you should see speedier compliance by creditors and account-grantors.

You should re-type the letter on the following page, but we've provided the four-page enclosure in a format that can be photocopied for your convenience.

Besides the included sections from the FCRA, you will also want to include a copy of any police report or case # for the identity theft incident as well as a completed copy of the FTC's identity theft victim's affidavit, which is included in Appendix II of this booklet.

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

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

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

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

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

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

Please provide all information relating to the fraudulent transaction, including:
• Application records or screen prints of Internet/phone applications
• Statements
• Payment/charge slips
• Investigator's summary
• Delivery addresses
• All records of phone numbers used to activate the account or used to access the account
• Any other documents associated with the account.

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

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

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

(e) Information available to victims

(1) In general

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

(A) the victim;

(B) any Federal, State, or local government law enforcement agency or officer specified by the victim in such a request; or

(C) any law enforcement agency investigating the identity theft and authorized by the victim to take receipt of records provided under this subsection.

(2) Verification of identity and claim

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

(A) as proof of positive identification of the victim, at the election of the business entity--

(i) the presentation of a government-issued identification card;

(ii) personally identifying information of the same type as was provided to the business entity by the unauthorized person; or

(iii) personally identifying information that the business entity typically requests from new applicants or for new transactions, at the time of the victim's request for information, including any documentation described in clauses (i) and (ii); and

(B) as proof of a claim of identity theft, at the election of the business entity--

(i) a copy of a police report evidencing the claim of the victim of identity theft; and

(ii) a properly completed--

(I) copy of a standardized affidavit of identity theft developed and made available by the Commission; or

(II) an [FN1] affidavit of fact that is acceptable to the business entity for that purpose.

(3) Procedures

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

(A) be in writing;

(B) be mailed to an address specified by the business entity, if any; and

(C) if asked by the business entity, include relevant information about any transaction alleged to be a result of identity theft to facilitate compliance with this section including--

(i) if known by the victim (or if readily obtainable by the victim), the date of the application or transaction; and

(ii) if known by the victim (or if readily obtainable by the victim), any other identifying information such as an account or transaction number.

(4) No charge to victim

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

(5) Authority to decline to provide information

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

(A) this subsection does not require disclosure of the information;

(**B)** after reviewing the information provided pursuant to paragraph (2), the business entity does not have a high degree of confidence in knowing the true identity of the individual requesting the information;

(C) the request for the information is based on a misrepresentation of fact by the individual requesting the information relevant to the request for information; or

(D) the information requested is Internet navigational data or similar information about a person's visit to a website or online service.

(6) Limitation on liability

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

(7) Limitation on civil liability

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

(8) No new recordkeeping obligation

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

(9) Rule of construction

(A) In general

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

(B) Limitation

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

(10) Affirmative defense

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

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

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

(11) Definition of victim

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

(12) Effective date

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

(13) Effectiveness study

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

Appendix II

ID THEFT VICTIM'S AFFIDAVIT

The following five pages contain the Federal Trade Commission's Identity Theft Victim's Complaint and Affidavit.

This is an important document that you should complete carefully and make multiple copies of. You will be sending a copy of this completed form to every creditor, financial institution, credit bureau, law enforcement agency, and other entity affected by your identity theft case.

The form itself contains thorough instructions, and is the same form you can find on the FTC's web site.

After the FTC affidavit, the following two pages contain the IRS Identity Theft Affidavit, Form 14039.

Average time to complete: 10 minutes

Identity Theft Victims' Complaint and Affidavit

A voluntary form for filing a report with law enforcement and disputes with credit reporting agencies and creditors about identity theft-related problems. Visit ftc.gov/idtheft to use a secure online version that you can print for your records.

Before completing this form:

1. Place a fraud alert on your credit reports, and review the reports for signs of fraud.
2. Close the accounts that you know, or believe, have been tampered with or opened fraudulently.

About You *(the victim)*

Now

(1) My full legal name: _____
First Middle Last Suffix

(2) My date of birth: _____
mm/dd/yyyy

(3) My Social Security number: _____-_____-_____

(4) My driver's license: _____ _____
State Number

(5) My current street address:

_____
Number & Street Name Apartment, Suite, etc.

_____
City State Zip Code Country

(6) I have lived at this address since _____
mm/yyyy

(7) My daytime phone: (____)_____
My evening phone: (____)_____
My email: _____

This section is for the victim's information, even if he or she cannot complete the form.

Leave (3) blank until you provide this form to someone with a legitimate business need, such as when you are filing your report at the police station or sending the form to a consumer reporting company to correct your credit report.

At the Time of the Fraud

(8) My full legal name was: _____
First Middle Last Suffix

(9) My address was: _____
Number & Street Name Apartment, Suite, etc.

_____
City State Zip Code Country

(10) My daytime phone: (____)_____ My evening phone: (____)_____
My email: _____

Skip (8) - (10) if your information has not changed since the fraud.

The Paperwork Reduction Act requires the FTC to display a valid control number (in this case, OMB control #3084-0047) before we can collect – or sponsor the collection of – your information, or require you to provide it.

Victim's Name _____ *Phone number* (____)_____

About the Fraud

What & When

(11) My personal information or documents (for example, credit cards, birth certificate, driver's license, Social Security card, etc.) were *lost or stolen* on or about _____.
mm/dd/yyyy

(12) I ***discovered*** that my personal information had been *used* by someone else on or about _____.
mm/dd/yyyy

(12): Let us know the date you ***noticed*** – this may be some time after the thief began to use it.

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

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

Who

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

(15): Enter what you know (even if you can't complete everything) about anyone you believe was involved.

(A) Name: _____
First Middle Last Suffix

Address: _____
Number & Street Name Apartment, Suite, etc.

_____
City State Zip Code Country

Phone Numbers: (____)_____ (____)_____

Additional information about this person: _____

_____

_____

_____

Victim's Name _____ *Phone number* (____)_____

(B) Name: _____
First Middle Last Suffix

Address: _____
Number & Street Name Apartment, Suite, etc.

_____
City State Zip Code Country

(B) and (17): Attach additional sheets as needed.

Phone Numbers: (____)_____ (____)_____

Additional information about this person: _____

_____

_____

_____

_____

(16) I ☐ am OR ☐ am not willing to press charges and/or work with law enforcement if charges are brought against the person(s) who committed the fraud.

(17) Additional information (for example, how the identity thief gained access to your information or which documents or information were used):

_____

_____

_____

_____

_____

_____

_____

About the Information or Accounts

(18) I wish to dispute the following personal information (such as my name, address, Social Security number, or date of birth) in my credit report as inaccurate as a result of this identity theft:

(A) _____
(B) _____
(C) _____

(19) Credit inquiries from these companies appear on my credit report as a result of this identity theft:

Company Name: _____
Company Name: _____
Company Name: _____

Victim's Name ______________________ *Phone number* (____)____________

(20) Below are details about the different frauds committed using my personal information.

Name of Institution | Contact Person | Phone | Extension

Account Number | Routing Number | Affected check number(s)

Account Type: ☐ Credit ☐ Bank ☐ Phone/Utilities ☐ Loan
☐ Government Benefits ☐ Internet or Email ☐ Other

Select ONE:
- ☐ This account was opened fraudulently.
- ☐ This was an existing account that someone tampered with.

Date Opened or Misused (mm/yyyy) | Total Amount Obtained ($)

Name of Institution | Contact Person | Phone | Extension

Account Number | Routing Number | Affected check number(s)

Account Type: ☐ Credit ☐ Bank ☐ Phone/Utilities ☐ Loan
☐ Government Benefits ☐ Internet or Email ☐ Other

Select ONE:
- ☐ This account was opened fraudulently.
- ☐ This was an existing account that someone tampered with.

Date Opened or Misused (mm/yyyy) | Total Amount Obtained ($)

Name of Institution | Contact Person | Phone | Extension

Account Number | Routing Number | Affected check number(s)

Account Type: ☐ Credit ☐ Bank ☐ Phone/Utilities ☐ Loan
☐ Government Benefits ☐ Internet or Email ☐ Other

Select ONE:
- ☐ This account was opened fraudulently.
- ☐ This was an existing account that someone tampered with.

Date Opened or Misused (mm/yyyy) | Total Amount Obtained ($)

---

(20):
If there were more than three frauds, copy this page blank, and attach as many additional copies as necessary.

Enter any applicable information that you have, even if it is incomplete or an estimate.

If the thief committed two types of fraud at one company, list the company twice, giving the information about the two frauds separately.

Contact Person: Someone you dealt with, whom an investigator can call about this fraud.

Account Number: The number of the credit or debit card, bank account, loan, or other account that was misused.

Amount Obtained: For instance, the total amount purchased with the card or withdrawn from the account.

Victim's Name _____ *Phone number* (___) _____

Documentation

(21) I can verify my identity with these documents:

☐ A valid government-issued photo identification card (for example, my driver's license, state-issued ID card, or my passport).
If you are under 16 and don't have a photo-ID, a copy of your birth certificate or a copy of your official school record showing your enrollment and legal address is acceptable.

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

Take these documents and this form to your local law enforcement office, along with your FTC complaint number (if you already filed online or by phone with the FTC). Ask an officer to witness your signature, below, and to complete the rest of the information about his or her department and your law enforcement report. It's important to get your report number, whether or not you are able to file in person.

Signature

If possible, sign and date *IN THE PRESENCE OF* a law enforcement officer.

(22) I certify that, to the best of my knowledge and belief, all of the information on and attached to this complaint is true, correct, and complete and made in good faith. I understand that this complaint or the information it contains will be made available to federal, state, and/or local law enforcement agencies for such action within their jurisdiction as they deem appropriate. I understand that knowingly making any false or fraudulent statement or representation to the government may violate federal, state, or local criminal statutes, and may result in a fine, imprisonment, or both.

_____ _____
Signature Date Signed (mm/dd/yyyy)

Your Law Enforcement Report

(23) Select ONE:

☐ I was unable to file any law enforcement report.
☐ I filed an automated report with the law enforcement agency listed below.
☐ I filed my report in person with the law enforcement officer and agency listed below.

_____ _____ _____ _____
Law Enforcement Department State Report Number Filing Date (mm/dd/yyyy)

_____ _____ _____ _____
Officer's Name (please print) Officer's Signature Badge Number Phone Number

Did the victim receive a copy of the report from the law enforcement officer? ☐ Yes OR ☐ No

Victim's FTC complaint number (if available): _____

REMINDER: Attach copies of your identity documentation when sending your report to creditors and credit reporting agencies.

Appendix III

UNIFORM MINOR'S STATUS DECLARATION

If your minor child is the victim of Identity Theft, you can use the form on the following page to establish the child is a minor. Keep copies of that completed form and relevant documentation to use for disputes with credit reporting agencies or creditors.
This documentation should have attachments that are COPIES, not originals, of the following documents:
· the child's birth certificate
· if the child is adopted, a copy of the final adoption proceeding order or certificate
· the child's Social Security card
· your state issued identification card (Driver's license or military ID) that shows your current address
· a utility bill that includes your current address
· if you are a legal guardian rather than a parent, include a copy of a court order or other proof of guardianship

UNIFORM MINOR'S STATUS DECLARATION

ABOUT THE MINOR CHILD

Full Legal Name
First Middle Last, suffix
Date of Birth (mm/dd/yy)
Social Security Number
Current Street Address
City, State, Zip Code

The child has lived at this address since: (mm/dd/yy)
All other addresses where the child has lived within the last five years:

ABOUT ME

Full Legal Name
First Middle Last, suffix
Date of Birth (mm/dd/yy)
Social Security Number
Current Street Address
(if different from the child's address)
City, State, Zip Code

I have lived at this address since: (mm/dd/yy)
Daytime Telephone ( ) Evening Telephone ( )

I certify that, to the best of my knowledge and belief, all the information on the attached to this declaration is true, correct, and complete and made in good faith. I further certify that I am the Parent, adoptive parent, legal guardian, or legal representative of the child named in this declaration. I understand that this declaration or the information it contains may be made available to federal, state, and/or local law enforcement agencies for such action within their jurisdiction as they deem appropriate. I understand that knowingly making a false or fraudulent statement or representation to the government may constitute a violation of 18 U.S.C. § 1001 or other federal, state, or local criminal statutes, and may result in imposition of a fine or imprisonment or both.

Signature Date Signed

Identity Theft

Credit.org

1825 Chicago Avenue
Suite 240
Riverside, CA 92507

PO Box 5438
Riverside, CA 92517-5438

(800) WISE-PLAN (800) 947-3752

www.credit.org