

Employee ID Theft Resource Guide

ID Theft

Prevention

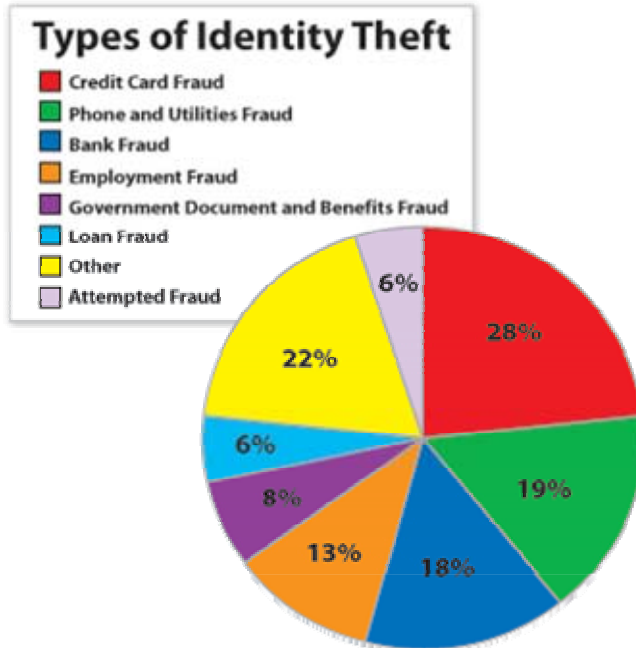
Resolution

Legal Resources ID Theft Assistance

Updates

What is Identity Theft?

- Identity Theft is a serious crime in which someone wrongfully obtains and uses:



(2008 Paradigm Innovations)

- a person's personal information, such as name, date of birth, social security number, driver's license, etc.
- and their financial identity, such as credit cards, bank accounts, phone cards, etc.
- to commit various types of fraud for economic gain.

How Can Your Identity Be Stolen?

- Dumpster diving
- Intercepting your mail
- Stealing your wallet
- Copying your account numbers
- Accessing your employer's files
- Via email, phishing, or the phone, "pretexting"
- Bank statements
- Credit card statements
- Social Security Administration
- Restaurants and bars where you swipe your credit and debit cards
- Department stores
- ATM machines
- Frequent flyer clubs
- Grocery store clubs
- Library cards
- Pay day check cashing outlets
- Sports associations
- Passport centers
- Car dealerships
- Via "change of address" forms at the Post Office.
- Steal personal information from home files.
- Shoulder Surfing
- Trojan horses or computer viruses
- Check washing
- Skimming
- Public announcements, birth, marriage, & death

How Do Identity Thieves Use Your Personal Information?

- They change the mailing address on an existing credit card and open new credit cards and bank accounts in your name.
- They are arrested in your name.
- They establish phone or wireless service in your name.
- They access medical insurance in your name.
- They may buy a car by taking out an auto loan in your name.
- They open bank accounts in your name.

Signs of Identity Theft Include:

- Receiving calls or letters from debt collectors for products you did not purchase.
- Failing to receive bills or other mail.
- Denial of credit or offers for credit at high interest rates.
- Denial of medical services or insurances.

Immediate Steps to Take if You Become a Victim

- **ALWAYS** keep accurate records.
- Close accounts that have been affected.
- Place a fraud alert on your credit reports and review them regularly.

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

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

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

- File a Police Report.
- File a complaint with the Federal Trade Commission.
 - www.consumer.gov/idtheft
 - call 877-438-4338
 - write: Identity Theft Clearinghouse
Federal Trade Commission
600 Pennsylvania Ave., NW
Washington, DC 20580

Medical Identity Theft

- Occurs when your identity is used by someone else to obtain medical goods or services.
- Most difficult type of ID Theft to fix:
 - Leaves a trail of false information – where have your medical records been disseminated?
 - Medical Providers
 - Insurance Companies
 - Government Agencies
- No centralized system for medical records – every time a thief uses your information a new record is created.
- Medical identity theft accounts for approximately 3% of all identity theft cases.

Consequences to the Victim

- Incorrect treatments due to false medical records.
- False medical and pharmaceutical bills.
- Denial of health insurance claims that are yours (can exhaust your lifetime caps).
- Denial of health or life insurance based on false medical records.
- Denial of employment.
- Time and expense of correcting false medical and insurance records.

Are Your Medical Records Safe?

- HIPPA does not require removal of incorrect information. Providers have 90 days to respond to incorrect records once notified, but they are not required to remove false information.
- Georgetown University Center on Medical Rights and Privacy maintains state by state guidelines to check your medical records:
<http://hpi.georgetown.edu/privacy/records.html>

Prevention

Security Freeze - New

A security freeze is a deterrent and a defensive tool in preventing false accounts being opened in your name. Most states have enacted laws that let consumers “freeze” their credit. By placing a credit freeze, potential creditors and other third parties will not be able to get access to your credit. An identity thief would not be able to open a new account in your name.

Credit freeze laws vary from state to state. Both Virginia and Maryland have credit freeze laws, enacted in January 2008, which allows individuals to place a freeze on their credit at a minimal cost. The cost of placing, temporarily lifting, and removing a credit freeze is typically between \$5 and \$10 per credit agency. However, the fee is waived if you show proof of Identity Theft via a police report or other certifiable methods.

How Do I Freeze My Credit?

To freeze your credit report, send a written request via certified mail. To place a security freeze on all three credit bureaus is a one-time fee of \$10 per credit bureau for Virginia residents, a one-time fee of \$5 for Maryland residents and a \$10 fee for DC residents for each credit bureau. You may easily remove the freeze by contacting the credit agencies. The manner by which you contact them is determined by them, but it may be by telephone, fax or over the internet. The Security Freeze law does not specify what information each credit reporting agency may require to place a freeze on your credit reports.

Please check each agency’s website for detailed instructions on how to obtain a credit freeze. The credit freeze option offered by most states is a superior and affordable option in the fight against identity theft. The three credit bureaus are:

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348
www.equifax.com

TransUnion Security Freeze

P.O. Box 6790
Fullerton, CA 92834-6790
888-909-8872
www.transunion.com

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013
800-821-8805
www.experian.com

Before using these template letters, please read the entire document for complete information.

SAMPLE FREEZE LETTER TO EQUIFAX

Date
Equifax
Security Freeze
P.O. Box 105788
Atlanta, GA 30348

Dear Equifax:

I would like to place a security freeze on my credit file. My name is:

My former name was (if applies):

My current address is:

My address has changed in the past 5 years. My former address was:

My social security number is:

My date of birth is:

I have enclosed photocopies of a government issued identity card AND proof of residence such as a utility bill or phone bill.

Circle one:

I am an identity theft victim and a copy of my police report or police docket number documenting identity theft is enclosed.

OR

I have enclosed the \$5 (for MD) or \$10 (for DC, VA) fee to place a security freeze on my credit account.

Yours Truly,

Your Name

Steps to Place a Freeze:

1. Send a certified letter, or after January 1, 2010 by telephone, email or secure electronic method if the means is provided by the consumer reporting agency;
2. If you are a victim of identity theft, you must include a copy of report of alleged identity fraud or an identity theft passport;
3. Provide your full name (including middle initial, as well as Jr., Sr., II, III, etc.,) address, social security number, and date of birth;
4. If you have moved in the past five years, supply all the addresses where you have lived over the prior five years.
5. Provide proof of current address such as a current utility bill or phone bill.
6. Send a photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. If you are not a victim, provide payment by check, money order or credit card (Visa, Master Card, American Express, or Discover cards only.)

How Long Does It Take to Place a Freeze?

Currently, the credit bureaus have up to three business days to place a freeze. After July 1, 2009, the credit bureau will have one day to place a freeze on your account after receiving your request. After receiving your request, the credit bureau has up to ten (10) business days, (5) in Maryland and DC to send you a confirmation with a unique password or PIN.

Credit Monitoring

Credit Monitoring does not *prevent* identity theft and is also ineffective at detecting it. It will alert you sometime after the identity theft crime has occurred. In fact, before a credit monitoring service alerts you to a credit-related activity, fraudulent or otherwise, all of the following conditions must be met:

- The activity must be reported to a credit agency.
- The credit agency to which the activity is reported must be one that you are monitoring.
- Both the Social Security Number *and* the name used in the transaction must match your credit report.

Security Freeze vs. Credit Monitoring

With a security freeze, you "lock" your three credit reports with a password or PIN. Then, the next time you apply for a line of credit, you temporarily unlock your credit report. Access to a credit report is critical for a lender to make a risk assessment. If the credit report is frozen, then the lender will not be able to open it and neither will a thief. Thus, credit freezing should reduce the risk of loans or credit cards being opened in your name fraudulently. If you are truly worried about identity theft, you are much better off freezing your credit than signing up for credit monitoring.

Not all identity theft is financial. Criminals will often assume someone else's identity to avoid prosecution. Credit monitoring services do not protect from this and other forms of identity theft. Please review the tables on the following pages regarding the benefits and limitations of both services.

Security Freeze	
<i>Benefits</i>	<i>Limitations</i>
Inexpensive - One time fee of \$10 per credit bureau, for a total of \$30. This price varies per state Ex. MD = \$5.00.	May hinder your ability to immediately obtain credit.
Prevents new accounts from being opened in your name.	Must call ahead to temporarily lift freeze.
Ability to lock and unlock your credit file.	Does not prevent all types of ID Theft.
Protects other sensitive information from being used to open fraudulent accounts.	Cannot request a freeze after business hours or on weekends.
Customer service provided 24 hours a day/seven days a week.	
A creditor cannot access a frozen file.	

Credit Monitoring	
<i>Benefits</i>	<i>Limitations</i>
Unlimited access to your credit reports and your credit score. (Not all monitoring services provide this).	Expensive/monthly fee between \$9.95 to \$25 per month
Automatic & daily alerts to changes on your credit within 24 hours via email or wireless. (Not all monitoring services provide this).	Many credit monitoring services only track one credit bureau. Make sure all three credit bureaus are monitored.
Customer service provided 24-hours a day/seven days a week.	

Prevention Tips

1. Place a Fraud Alert on your credit report and/or activate a Security Freeze.
2. Review credit reports from each of the three major credit bureaus once a year. Visit Legal Resources at www.legalresourcesplan.com.
3. Place passwords on your credit cards, bank and phone accounts.
4. Secure personal information in your home.
5. Ask about information security procedures at your workplace.
6. Don't carry your social security card with you. Leave it in a secure place. Check your insurance/voter registration cards for ID numbers that may be your social security number.
7. Don't give out your social security number unless it is absolutely necessary; ask to use other types of identifiers when possible.
8. Don't give out personal information over the phone, through the mail or over the internet unless you have initiated the contact or are sure you know with whom you are dealing.
9. Guard your mail and trash from theft. SHRED!
10. Stop pre-approved credit offers by calling 888-5OPTOUT or online at www.optoutprescreen.com.
11. Carry only the identification information and the number of credit/debit cards that you actually need.
12. Pay attention to your billing cycles - follow up with creditors if bills do not arrive on time.
13. Be wary of promotional scams.
14. Keep your purse or wallet in a safe place at work.
15. Notify your credit card company if you are planning to travel out of state, or out of the country.
16. Legal Resources can advise employees how to remove their name from the Pre-Approved Credit Card Lists.

17. Legal Resources can provide tips of how to reduce an employee's exposure to Identity Theft.
18. Sign the back of your credit card & debit cards.
19. Keep all your credit card receipts.
20. Cancel & destroy all unused cards & checks.
21. Do not print personal information on your checks.
22. Shred your junk mail.
23. Never place your out-going mail in an unsecured mailbox.
24. Don't respond to unsolicited requests for personal or account information.
25. Avoid online "phishing" scams.
26. Pick checks up at the bank.
27. Read all of your financial/medical statements.
28. Does your computer store your personal information, such as bank account number, tax returns or birth date? Keep your computer safe by:
 - a. Upgrading your virus protection
 - b. Do not open files, click on hyperlinks, or download programs sent to you by strangers
 - c. Use a secure browser
 - d. Try not to store financial information on your laptop
 - e. Use a "wipe" utility program when disposing a computer to overwrite the entire hard drive
 - f. Look for website privacy policies.

Cell Phone Safety

- Protect information stored in your cell phone.
- If you upgrade to a new model cell phone, consider these tips when disposing your old cell phone:
 - a. Remove the SIM card.
 - b. Delete all personal data.
 - c. Contact your wireless provider.
- Once "wiped clean," you have a choice of how to dispose of it.

Fraud Alert

Immediate steps to Take if You Become a Victim:

1. “**Close**” accounts affected by fraud.
2. Place a **fraud alert** on your credit reports and review them regularly.
3. The Fair and Accurate Credit Transactions Act (FACTA) was enacted into Federal law in December 2003. One of its provisions allows consumers to place fraud alerts on their credit reports. A Fraud Alert is an Identity Theft option if you do not want to freeze your credit. Fraud Alerts are appropriate to use if you suspect your identity has been compromised. There are three different types of Fraud Alerts:
 1. An **Initial Alert** is appropriate to use if your wallet has been stolen or if you’ve been a victim of a “phishing” scam. It stays on your credit for 90 days. You can order a free credit report from each credit bureau and protect your social security number by requesting only the last four digits to appear on your credit file.
 2. An **Extended Alert** is appropriate if you have been a victim of Identity Theft and you can provide the credit bureau with an “Identity Theft Report.” An Extended Fraud Alert stays on your credit report for seven years. You can order two free credit reports from each credit bureau each year. You may also request your name to be removed from marketing lists for pre-screened credit offers for five years.
 3. A **Military Alert** may be placed on your credit report to help minimize the risk of ID Theft while you are deployed if you are active duty military. Active duty alerts are in effect on your report for one year. If your deployment lasts longer, you can place another alert on your credit report.

How Do I Place A Fraud Alert?

1. Call one of the credit bureaus toll free:
Equifax 1-800-525-6285
Experian 1-888-397-3742
TransUnion 1-800-680-7289

Request that the alert be placed. The bureau you contact are required to contact the other two bureaus.

2. Place a fraud online. (See websites alone).
3. You may submit your written request to the credit bureau and include:
 - Proof of your identity.
 - Your Social Security number.
 - Name and address.
 - Any other information the credit bureau requests.
 - To file an Extended Fraud Alert, follow the two steps above, but a copy of your Identity Theft Report is also required.

Additional Fraud Alert Facts

- If a business sees the alert on your credit report, they must verify your identity before issuing you credit.
- There is no fee to place a Fraud Alert.
- A Fraud Alert on your credit report will not lower your credit score.

Resolution

Identity theft can be devastating and the process of restoring your name can be overwhelming and costly. As a subscriber of Legal Resources, if you become a victim of identity theft, a Legal Resources Identity Theft Specialist can assist you with recovery by providing you with the tools necessary to conduct identity theft resolution. In order to restore your credit as quickly as possible take the following steps:

- Notify one of the three major credit bureaus and place a fraud alert on your credit report.
- Contact the financial institutions and credit card companies that have been affected.
- Contact the Federal Trade Commission for an Identity Theft Affidavit.
- File a miscellaneous incident report with local police department or with the police department where the theft occurred.
- Contact all businesses that have opened accounts in your name.
- Notify the Federal Trade Commission.
- Report stolen mail.
- Report a stolen Social Security number.
- Report stolen checks.
- Alert the Securities & Exchange Commission (SEC).

Recovery services ensure that an employee who does fall victim to Identity Theft will remain productive during the time it takes to restore their identity. In the event a subscriber may have questions regarding this benefit, they may contact our Subscriber Relations department at 757-498-1220 or 800-728-5768 and speak directly to an Identity Theft Specialist.

Identity Theft Assistance Center (ITAC)

Many financial institutions have become members of an association called the Identity Theft Assistance Center (ITAC). ITAC is a cooperative initiative of the Financial Services Industry that provides free victim assistance service for customers of member companies. Once your financial services company has addressed any suspicious activity regarding your account and they determine you are a victim of identity theft, they will offer you the services of ITAC.

An ITAC representative, who has extensive experience in resolving financial fraud, will be assigned to you. They will:

- Work with consumers one-on-one throughout the identity theft resolution process.
- Review credit reports with the victim to find suspicious activity.
- Notify affected creditor(s).
- Place fraud alerts.
- Shares information with law enforcement officials and the FTC.
- Prepare documentation and make all phone calls needed to resolve your identity theft.
- Create a comprehensive case file to assist law enforcement and insurance.

For more information of the services provided by ITAC, you may visit there website at www.identitytheftassistance.org.

Legal Resources ID Theft Assistance

<p><u>ID Theft Consultation & Credit Protection</u> Unlimited consultation & advice. Preparation of letters relating to billing disputes, etc.</p>	<p>Included</p>
<p><u>Annual Credit Reports</u> Equifax, Experian, TransUnion - Visit www.legalresourcesplan.com</p>	<p>Included</p>
<p><u>ID Theft Prevention Education</u> Assisting employees with removing their name from pre-approved credit card lists.</p>	<p>Included</p>
<p><u>ID Theft Restoration Education</u></p>	<p>Included</p>
<p><u>Civil Action Defense Representation</u> of the covered person as a defendant at the Lower Court only. Claim must exceed \$400.</p>	<p>One Hour Free Initial Consultation – Covered 100% (lower court) 25% Discount (higher court)</p>
<p><u>Civil Action Plaintiff Representation</u> as plaintiff in connection with the filing of a civil action within the General District Court. Claim must exceed \$400.</p>	<p>One Hour Free Initial Consultation – Covered 100% (lower court) 25% Discount (higher court)</p>
<p><u>Civil Actions Filed in State Higher Court or Federal Court</u></p>	<p>One Hour Free Initial Consultation – 25% Discount</p>
<p><u>Credit Recovery Actions</u></p>	<p>One Hour Free Initial Consultation – 25% Discount</p>
<p><u>Expungement</u> of Criminal Record due to Identity Theft</p>	<p>One Hour Free Initial Consultation – 25% Discount</p>



Is it time to update your Legal Resources Identity Theft Resource Guide?

Periodically review and update your ID Theft Guide for news and announcements regarding Identity Theft.