



**IDENTITY
FRAUD** INC.

PROTECTION GUIDE

*Learn the Essentials & Immediate Steps
to Protect Your Identity*

Identity fraud occurs anytime your personal information is used without your authority and is more than just credit card fraud. There are nearly 10 million people victimized by identity fraud each year with individual victims spending countless hours resolving the frauds. Unfortunately, no one can guarantee that you won't become a victim. That's why taking preventative steps is critical. Learn the essentials and how to optimize your protection steps and strategies by reading the enclosed.





Contents

1.0 About Identity Fraud

- 1.1 Types of Identity Fraud
- 1.2 How Identity Fraud Occurs

2.0 Essential Prevention Steps

3.0 Victim Action Items

4.0 Protection Products – How to Optimize Your Protection



1-866-4ID-FRAUD
www.identityfraud.com



1.0 About Identity Fraud

Identity fraud is the unauthorized use of your personal information for abuse or gain.

Identity fraud and identity theft typically have the same meaning. However, some definitions have identity theft as the “taking” of personal information, with identity fraud representing the actual “misuse” of personal information.

Personal information susceptible to theft includes your name, Social Security Number, financial account numbers, date of birth, mother’s maiden name and many other personal identifiers. Regardless, anytime someone takes and misuses **any** of your sensitive personal information without your authority, you are a victim of identity fraud.

According to the FBI, identity fraud is the fastest growing white collar crime in America. The Federal Trade Commission’s (FTC) November 2007 Identity Theft report by Synovate indicates there were 8.3 million victims in 2005; nearly 5% of all adults.

The risks to identity fraud are real because personal information about adults and minor children is readily accessible, difficult to protect and easily abused. While we identify essential steps you can take to increase your protection, no one can guarantee that you won’t become a victim of identity fraud. As an individual, you need to take proactive steps to help ensure your personal protection and understand what resources are available to better optimize your position.

1.1. Types of Identity Fraud

There are over 25 different types of identity fraud ranging from healthcare and workers compensation identity fraud to credit card and employment fraud. While the list continues to grow as thieves become more creative and sophisticated in their attacks, we typically categorize identity fraud into the following main types:

Financial

Existing Account Fraud – Thieves obtain existing credit card, checking or savings account numbers and make fraudulent transactions over

the Internet or by creating counterfeit cards or checks. Addresses and contact details will often be changed to misdirect statements and avert your detection.

New Account Fraud – Personal information is used to open new accounts like a retail store credit card, auto or home loan. The FTC reports that victims of new account fraud typically learn of the frauds from a collection agency. Further, new account frauds can present a greater burden to victims than fraud on existing accounts.

Criminal

Another significant burden of identity fraud can occur when an imposter commits a misdemeanor or felony crime in your name, like speeding or drunk driving. For non-account related victims, the FTC indicates that twenty-seven percent (27%) of persons had their name given to law enforcement when the imposter was stopped or charged with a crime.

Other

A more complete list of various types of identity fraud can be found at www.identityfraud.com. A few examples include:

Healthcare Fraud – A thief uses your personal information to receive medical treatment. With 47 million people being uninsured in America, healthcare fraud is a significant growing problem.

Employment – A thief may use your SSN and obtain employment in your name creating tax and benefit problems.

1.2. How Identity Fraud Occurs

Unfortunately, identity fraud is easy to commit. It is also very profitable for thieves, which provides the motivation to overcome criminal deterrents.

Identity fraud begins by obtaining your personal information. Your personal information is virtually everywhere and is accessed by simple and sophisticated means. For example, stealing your mail and dumpster diving in your trash are very simple, yet yield valuable information. Conversely, designing a computer virus to



extract personal information from your computer may be considered sophisticated and is potentially more effective at extracting key pieces of information like passwords that allow access to online accounts.

Additional examples include:

- Lost Wallet or Purse
- Skimming / recording credit card information from the magnetic stripe
- Burglaries
- Friends/Family
- Shoulder surfing (eavesdropping) to memorize your account number or PIN
- Cell phone cameras
- Fellow employees
- Insider theft, rogue employees that steal or sell your information
- Database hacking or accidental loss exposing personal data
- Computer Virus or Spyware capable of recording your keystrokes
- Phishing and other email/phone scams
- Opportunists who normally wouldn't steal your data but 'just happen' to find and abuse your data
- Purchase – Stolen information is generally available for sale on the 'black market', either on a city street corner or the Internet underground.

Once your personal information is obtained, it is used to engage transactions for goods, create false and counterfeit documents or applications for credit and loans. Because the burdens of identity fraud are significant, taking precautions to reduce your risks is paramount.

2.0 Essential Prevention Steps

It's quite simple to engage basic and essential prevention steps that will reduce your risk to identity fraud. Implement the following practices:



Monitor Your Accounts – It is imperative to monitor your existing accounts for fraud. While you have certain protection by law that may restrict your

liability for unauthorized use and losses, you are required to notify your institution to limit your exposure. Generally, failure to notify your institution in a timely fashion (usually 60 days from the date you should have received your account statement) may cause your institution to incur losses they otherwise may have prevented. You may be held liable for those losses that could have been prevented, yet were incurred following your notification deadline. In many cases, this is thousands of dollars.

Thus, whether you incur fraud on credit cards, debit cards, checks or other accounts, have 'Zero Liability' protection or similar assurances against fraud, or never actually received your statements in the mail due to loss or theft, it is imperative to know your actual exposure by reading the customer or service agreements from your provider institution while paying particular attention to your notice requirements. At the end of the day, it is critical to watch out for your monthly statements, monitor your accounts for accuracy and to report any unauthorized activity immediately. If you do not receive your monthly statement, contact your institution for a copy.

Monitor Your Credit File(s) – To better detect new accounts being opened in your name, review your credit reports at least once a year for accuracy and possible fraud. Pursuant to the Fair and Accurate Credit Transactions Act of 2003 (FACTA), you may access one free report from each consumer reporting agency (CRA) once each year by visiting www.annualcreditreport.com or by calling 1-877-322-8228.

To enhance your monitoring capabilities, consider purchasing a credit monitoring tool from Identity Fraud, Inc. or one of the main credit reporting agencies. For roughly \$13 per month, you can monitor all three main agencies (Equifax, Experian and TransUnion) and be alerted to changes in your credit file. The sooner you are able to detect changes, the more quickly resolution can take effect.

Restrict Access to Your Credit Information – One of the best tools available to individuals today to prevent credit related identity theft is to place a “**credit freeze**” on your credit files.

Prior to a creditor issuing credit to you or any thief, they should evaluate your credit worthiness by reviewing your credit file. Because a credit freeze restricts access to your file, a proper evaluation is not made and therefore credit issuance and frauds should be prevented.

Because there is a cost (about \$10 per bureau) each time you elect to freeze and unfreeze your files, the credit freeze is most appropriate for individuals that do not need new credit. Simply freeze your credit file indefinitely. At some point in the future if you plan to obtain a new credit relationship, simply unfreeze your credit file.

Similar to the credit freeze, placing a “**fraud alert**” or “flag” on your credit file can restrict access and help prevent new accounts from being opened in your name. And, the fraud alert is free.

The fraud alert is a temporary (90 days) and free personal statement requesting creditors to contact you to verify your identity before issuing credit in your name and is intended for individuals that believe they are exposed to identity theft.

To place fraud alerts, call one of the three main credit bureaus and follow the automated telephone prompt system for placing fraud alerts. A successful fraud alert placed with one bureau will be automatically shared with the other two. You will receive letters confirming the fraud alert from each agency along with instructions on how to receive a free credit report. To place a fraud alert, call one of the following:

Equifax: 1-888-766-0008
Experian: 1-888-397-3742
TransUnion: 1-800-680-7289

Basic Prevention Practices – Each day, we interact with people and handle personal information. To increase your daily protection, you need to treat personal information as valuable information and restrict its accessibility and use.

Many common sense practices are appropriate to increase your protection. A few include:

- Shredding sensitive records
- Securing your mail
- Closing unnecessary accounts
- Never disclose your personal information to people that email or call you
- Secure your work and home office by making personal and business documents inaccessible



- Secure your computer, laptop and PDA
- Have strong passwords
- Memorize your SSN and don't carry it with you
- Make backups of personal and computer documents in case of theft or loss
- Generally, be suspicious and cautious

Purchase Protection – Your identity is a valuable asset that deserves special protection. You should protect your identity just like you protect your home, autos, health and other valuable assets against loss.

Securing professional support and identity insurance from or similar to that provided by Identity Fraud, Inc. is simply a smart choice to increase your protection and the remedies available to you if you become a victim. While it is best to prevent identity theft from occurring, accidents can and do happen. There is no way to prevent all types of identity theft. Identity theft is both rampant and evolving quickly. Protection is prudent, cost effective and better to have in place before a loss occurs.

For more information on IFI protection, simply call 1-866-4ID-FRAUD or visit www.identityfraud.com.

Other Prevention Tips – The FACTA not only allows you the opportunity to review a free credit report, but also allows you to review one free consumer report from “Specialty Consumer Reporting Agencies”.

While different than the credit bureaus, these agencies also compile and share data about you from your public records when relating to:


- Medical records or payments
- Residential or tenant history
- Check writing history
- Employment history
- Insurance claims

Like your credit report, it is a good idea to review these records for accuracy and possible fraud.

In summary, you should review the following:

ChoicePoint:

To request copies of your (auto/ home insurance) claims history report, visit www.ChoiceTrust.com or call 1-866-312-8076.



To request a copy of your employment history report, call 1-866-312-8075.

To request a copy of your tenant history report, call 1-877-448-5732.

For more information on these reports, visit www.ChoicePoint.com

ChexSystems/SCAN:

To request a copy of your banking history report from ChexSystems, visit www.consumerdebit.com

To request a copy of your banking history report from SCAN, visit www.consumerdebit.com or call 1-800-262-7771.

Medical Information Bureau (MIB Group):

To request a copy of your consumer file, visit www.mib.com or call 1-866-692-6901.

Pursuant to the FACT Act of 2003, credit reports and similar 'consumer reports' maintained by Consumer Reporting Agencies may be obtained once-per-year, at no cost. Simply visit www.annualcreditreport.com or call 1-877-322-8228.

3.0 Victim Action Items

Identity fraud can affect your ability to conduct normal daily affairs, like using your payment card to purchase groceries or making a mortgage payment.

While victims are not liable for losses (in most cases), you are often treated as a "guilty" party. The burdens are proving your innocence

and reversing fraudulent transactions and records created in your good name. For simple cases of identity fraud, like credit card fraud, the burdens are minimal. For more complex cases, the burdens are significant.



As a victim, you need to take certain "immediate" action steps in an attempt to stop further frauds from occurring. These immediate steps include:

- Contacting your financial institution(s) and other affected creditors to close existing accounts and to prevent ongoing fraudulent activity. Obtain replacement cards and set new passwords.
- Placing a fraud alert on your credit file by contacting one of the main credit reporting agencies. Equifax's toll-free fraud line is 1-877-766-0008. The 90-day alert will help prevent new credit accounts from being opened in your name and you'll have access to a free credit report, which details are provided in your alert confirmation letter sent by the bureaus. Lastly, victims have the option to extend their fraud alert for a period of seven years. This alert must be requested in writing and accompanied by supporting identity information and a police report.
- Contacting the Police and obtaining a police report to evidence your case.

The Federal Trade Commission also provides free consultations and direction to victims by calling 1-877-ID-THEFT or visiting www.ftc.gov/idtheft. Also, different state laws exist to support victims, for example, how many credit reports victims may obtain for free.

Once you have taken immediate steps to stop fraud, you will enter into a resolution phase that requires you to clear your good name. This process is administrative and may take some time, so be patient, professional and stay organized. We recommend that you keep detailed notes on who you speak with and when, their contact details, and expenses you incur. In most cases, a fraud affidavit will be required to accompany a police report in order to allow institutions the opportunity to investigate your case.

Because identity theft can affect many different institutions and different types of personal identifying information and records, you will need to work with each institution or government agency separately. For additional details on who to contact for different types of fraud, from check fraud to social security fraud, visit our web site at www.identityfraud.com.

Of course, the primary role of Identity Fraud, Inc. is to reduce or eliminate the burdens of fraud on victims. The solutions and services are affordable and appropriate and highlighted in Section 4.0.



4.0 Protection Products – How to Optimize Your Protection

There are many different products on the market today that can assist you in increasing your protection. But because personal information is everywhere and creating dynamic exposures, the solutions are quite diverse and range from computer software to identity insurance. Additionally, certain products or functionality you might otherwise pay for may actually be available for free, by law.

As an original designer and provider of identity fraud risk management products, we recommend the following solutions to optimize your protection.

⇒ Everyone has an identity that is a valuable and important asset; therefore everyone should have a basic level of protection that affords access to 1) Expert Resolution Services and 2) Insurance.

This protection provides the essential foundation for identity protection. Resolution services will help you save valuable time, money and frustration, while identity insurance provides added peace-of-mind and financial protection against many common expenses and in case expenses rise dramatically, as in complex cases. Like homeowners and auto insurance, this foundation will protect you against the uncertainties and burdens of loss. Thus, no matter what type or how identity theft occurs, you will have some level of protection in place.
- Best Value Item.

⇒ Take advantage of free resources, including:

- Free Credit Reports & other free Consumer Reports. Review these reports for accuracy and fraud
- Free Fraud Alerts – Restrict access to your credit files and help prevent new accounts from being opened in your name. The activation process takes

about three minutes.

- Best Value Item

- ⇒ Take advantage of a Credit Freeze. Although there may be a cost, it is a very small cost to lock perpetrators and credit grantors from your credit file.
- Best Value Item
- ⇒ Good Prevention Practices. By improving your information handling and disclosure practices and increasing your education about how to avoid identity theft, you can better optimize your fight against fraud. Usually, there is no cost.
- Best Value Item
- ⇒ Computer software. Virus, firewall and spyware are critical and essential if you maintain a computer.
- Best Value Item
- ⇒ Purchase a locking mailbox.
- ⇒ Purchase a shredder.
- ⇒ Purchase credit monitoring tools. If you do not engage a credit freeze and/or do not otherwise maintain a fraud alert on your credit file, monitoring tools provide value by alerting you to changes in your credit reports. The sooner you detect fraud, the better, as resolution is more efficient.
- ⇒ Personal records monitoring. Certain products allow you to datamine public records for changes. These may or may not be worth the investment, but nevertheless remain available.
- ⇒ Caveat Emptor / Buyer Beware. Most identity protection products are relatively new and there are important differences in terms, conditions and functionality, so caveat emptor. If a product sounds too good to be true, it probably is not credible. Similarly, if products guarantee that you will not become a victim, be sure to read the fine print.

Identity protection is timely and worthwhile. For more details on how to best optimize your protection, feel free to contact Identity Fraud, Inc. at 1-866-4ID-FRAUD or visit www.identityfraud.com. For a few dollars, you can obtain excellent protection and peace-of-mind.

