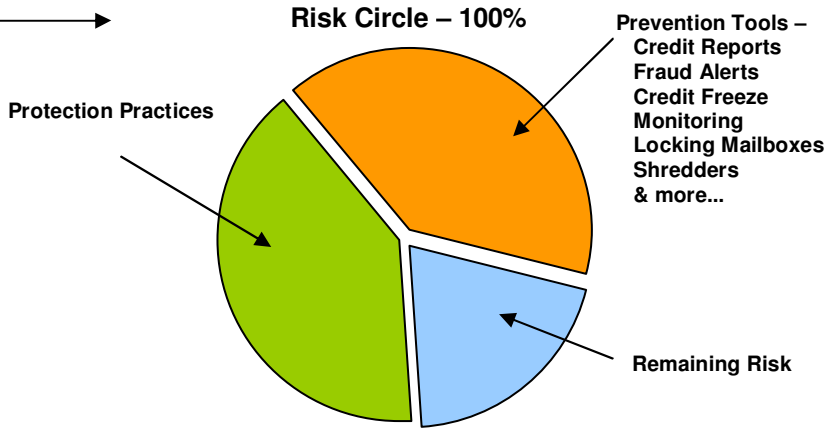
Dear Member:

We appreciate your participation in the Identity Fraud, Inc. *Core Identity Protection program* and believe you are taking an important step in reducing your potential of becoming an identity fraud victim.

The Loss Prevention and Resource Guide is a tool meant to educate and guide you in taking various actions both now, and as part of your daily practices. We are confident that by following the guidelines, you will reduce your risk. Unfortunately, no one can guarantee that you will not become a victim of fraud. That is why we provide you with VRS Elite™ Unlimited victim resolution services and important identity insurance coverage to reduce the burdens in the event you do become a victim.

Throughout the Loss Prevention & Resource Guide, our efforts are geared upon identity fraud risk management. Risk management is a term we use that comprises all of the tools and actions available to us that help us reduce risk. As a starting point, it is important to be educated on how identity fraud occurs. From this point, we can work to incorporate tools for protection to reduce risk. However, it is important to realize that some degree of identity fraud risk will always remain. If, and when, you become a victim, you can access our toll-free VRS Elite™ FCRA certified resolution specialists to help clear your good name, and we will guide you in submitting a claim for reimbursement of certain identity fraud related expenses you may incur.

We illustrate how risk management efforts, like adopting good protection practices and using prevention tools, can effectively reduce risk. Although some degree of risk will always remain, the more protection and prevention you implement, the more you can reduce your risk to identity fraud.



Identity fraud is a troubling and evolving problem. Criminals will continue to find new ways to abuse our personal information. Therefore, it is important to take action, keep abreast of changes, and seek assistance when you need it most.

We look forward to serving you with integrity and professionalism both now and in the future. Having been a victim of identity fraud myself, I hope you never become a victim, but if you do, we will do our best to get you back on track in a timely fashion, helping you recover from the burdens that identity fraud creates.

Sincerely,

Thomas A. Widman

Thomas A. Widman
President & CEO

1700 N Broadway, Suite 370, Walnut Creek, CA 94596
T: (925) 296-2600; F: (925) 296-2606
www.identityfraud.com

Loss Prevention & Resource Guide

Version 5.0

Prepared by

Identity Fraud, Inc.

DISCLAIMER

Neither Identity Fraud, Inc. nor the Loss Prevention & Resource Guide can prevent you from becoming a victim of identity fraud. The Loss Prevention Guide is designed as a tool to help identify areas where you might take action to reduce your exposure. The exposures to identity fraud are various and neither Identity Fraud, Inc. nor the Loss Prevention Guide can address all types of exposures. The Loss Prevention Guide is not a legal document. Should you require legal assistance, we recommend you seek professional legal counsel.

IDENTITY FRAUD, INC. PROVIDES THE LOSS PREVENTION & RESOURCE GUIDE TO YOU "AS IS". TO THE FULLEST EXTENT PERMISSIBLE UNDER APPLICABLE LAW, NEITHER IDENTITY FRAUD, INC. NOR ITS AFFILIATES MAKE ANY REPRESENTATION OR WARRANTIES OF ANY KIND WHATSOEVER THAT THE CONTENT, PRODUCTS OR SERVICES AVAILABLE WILL BE ERROR-FREE. IN ADDITION, IDENTITY FRAUD, INC. AND ITS AFFILIATES DISCLAIM ALL EXPRESSED OR IMPLIED WARRANTIES, INCLUDING TITLE, MERCHANT ABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT AND INFORMATIONAL CONTENT. THEREFORE, YOU AGREE THAT YOUR USE OF OUR LOSS PREVENTION & RESOURCE GUIDE, PRODUCTS, SERVICES AND CONTENT ARE AT YOUR OWN RISK. BY USING OUR LOSS PREVENTION & RESOURCE GUIDE, YOU ACKNOWLEDGE AND AGREE THAT NEITHER IDENTITY FRAUD, INC. NOR ITS AFFILIATES HAVE ANY LIABILITY TO YOU (WHETHER BASED IN CONTRACT, TORT, STRICT LIABILITY OR OTHERWISE) FOR ANY DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL OR SPECIAL DAMAGES ARISING OUT OF OR IN ANY WAY CONNECTED WITH YOUR ACCESS TO OR USE OF OUR LOSS PREVENTION & RESOURCE GUIDE, CONTENT, PROTECTION PLANS, PRODUCTS OR SERVICES (EVEN IF WE HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES).

Loss Prevention & Resource Guide

Table of Contents

Special Note:

The IFI Loss Prevention & Resource Guide is for your individual use only (including family member) and subject to the terms and conditions of your Identity Fraud, Inc. Membership Agreement. Any unauthorized copying or distribution without our express written approval is a violation of United States of America copyright laws and may be punishable by fines of up to $100,000.00 per incident.

Section I - Overview

The IFI Loss Prevention Guide & Resource Guide is an identity fraud risk management guide that will help you reduce your exposures to loss. You, as an individual, must ultimately take the appropriate action steps to reduce your exposures. As an active member with Identity Fraud, Inc., the IFI Loss Prevention & Resource Guide and VRS Elite™ Victim Assistance will assist you in your efforts to combat identity fraud.

Unfortunately, the first burden of identity fraud is the need to take any action at all. But if you do not take the appropriate steps, you will most certainly increase the chance of becoming a victim. Thus, think of the actions you take now as an investment into your future. If you become a victim, you will be better prepared to act and remedy the situation, as you will become more educated and aware of the obstacles you must overcome.

At best, identity fraud is an inconvenience to your daily routine. At worst, identity fraud is a nightmare that can cripple you financially or render you guilty of crimes you did not commit. Various state and federal laws that have passed and new laws that are now being given significant attention by lawmakers may assist you. For example, identity fraud is currently a Federal crime under Title 18 USC 1028 (The Identity Theft and Assumption Deterrence Act or The ID Theft Act) with penalties up to 15 years of imprisonment and a maximum fine of $250,000. Before this law passed in October 1998, identity theft was not defined as a crime. Rather identity thieves would commit crimes using false identities that would fall under different criminal codes and result in separate prosecution. However, identity fraud is still the fastest growing white-collar crime in American. Today, identity theft is far too easy to commit and, unfortunately, law enforcement has limited resources to fight individual identity fraud cases.

Why is identity fraud such a growing problem today? We have identified a few possible reasons as follows:

- **Trust** – We need to trust people and institutions in order to interact in society. Unfortunately there are people in positions of trust that breach trust relationships and take advantage of their positions to commit crimes. Historically, people would earn trust through physical interactions, handshakes, and reputations in the community. Today, we trust and interact with people locally, and with the World Wide Web, virtually, seldom truly knowing who they are.
- **Technology** – With technological advancements, a home computer and printer can produce amazingly accurate counterfeit documents like checks, driver's licenses, etc. Technology allows us to process, search, and store information making knowledge more attainable. Technology allows us to monitor most activities, and it can be used steal, destroy, or disrupt computer systems, which have become the foundation on which we operate.
- **The Information Age** – Vast databases containing personal information exist with information being bought or sold, legally or illegally. Databases available to the public may be hacked or they may simply be improperly managed. Data collection and monitoring has never been easier; but if information is gathered, information is also accessible.
- **The Internet Age** – On one hand, the Internet has brought tremendous anonymity to society. For example, we no longer need to go to the bank to deposit, withdraw funds, or pay bills. We do not need to be present at stores to purchase goods. On the other hand, certain computer programs can use the Internet to track your every move and even your computer keystrokes.
- **Big Business** – Personal information is an asset. Big business uses information to sell new products. For example, consider American credit card issuers who mail nearly 5 billion pieces of direct mail solicitations each year. Criminals can easily attain the pre-approved credit card offers in the mail and commit identity fraud (card marketing).

- **Government** – Various State and Federal agencies act independently with differing objectives and often times with a lack of coordination. Some state DMV's have actually sold personal records to marketing firms. Many government records are public information that is posted on the web that can be accessed for fraudulent abuse. Consider the social security number, which was never intended to be a unique identifier; it is currently used as one of the main identifiers that support the issuance of credit, benefits, and other primary forms of identification.
- **Freedom** – In the United States, we enjoy freedoms unlike any other nation. Some freedoms increase our risks to fraud. For example, you can go to a variety of web sites and obtain information about anyone. We are also free to download software that help people build viruses or teaches people how to hack.
- **Criminals** – As long as the benefits of crime appear to outweigh the costs, crimes will continue to occur. Burglary, robbery, murder, theft, etc. are all crimes that continue to be done in spite of being illegal and having severe consequences if one is caught. Currently, according to the Federal Trade Commission, the probability of getting caught for identity fraud crimes is one chance in ten. Criminal activity will continue to evolve and take advantage of vulnerabilities in our society.

Solutions to identity fraud are equally varied because of the vast array of exposures and because the problems are rooted in how we operate as a society. Any changes or solutions can impact the freedoms we enjoy and will require extensive efforts to sway or balance the interests and abilities of all the parties involved (i.e. individuals, privacy advocates, laws, business, government, law enforcement, etc.) As we evolve as a society and recognize the inherent problems we face through interaction, solutions will be developed. They will be a combination of laws, liability, technology and business change to name a few.

With this Loss Prevention & Resource Guide, we attempt to identify various solutions or steps you can take in today's world to reduce the potential for fraud. Knowing our environment will continue to evolve, it becomes important to remain active in identity fraud risk management protection practices. Even as exposures change, the risk management process remains the same. The process is described as follows:

1. Education
2. Identification and Evaluation of Exposures
3. Implementing Solutions
4. Monitoring and Adapting to Change

We encourage you to play an active role in promoting the privacy of your information. One of the easiest ways to voice your opinion is by exercising your power to vote. Vote for legislation that will increase privacy and security for consumers, as well as those that will stiffen the punishment for the criminals who commit identity theft. Supporting certain laws and political representatives can help bring about change. You can also be proactive by taking risk management action steps and educating those around you.

Section I.A. – How to Use the Loss Prevention & Resource Guide

The Loss Prevention Guide is designed to guide you through a variety of action items that will reduce the chance of becoming a victim of identity fraud, as well as provide you with guidance and documents that will assist you if you become a victim.

⟶ **If you are a new VICTIM of identity fraud, please go straight to *Section IV*.**

Our Loss Prevention Guide is divided into four main sections. In the beginning sections, we guide you to forms and checklists that should be reviewed and completed to reduce your risk. For example, starting in *Section III*, you should utilize the forms located in the Appendix to document your existing financial accounts. By identifying which financial relationships you have, you will be better prepared to know what to protect and who will need to be contacted in the event of an incident.

Section III identifies areas that should be given your full attention to prevent loss. By taking appropriate steps in this section, you will further increase your protection. We acknowledge that you might not purchase the products (like personal computer firewalls) that we identify or take steps that we recommend; however, we also assume that you do not want to become a victim of identity fraud. By building in more protections, you can lessen the chance of becoming a victim. But which risk management steps you take is up to you, we can only uncover important areas to consider and provide you with tools or direction on which steps we feel are important.

Section IV begins to address "post-loss" victim assistance and actions you may need to take to rectify an identity fraud incident. When an incident does occur, you will be provided access to our 24/7 VRS Elite™ support. You may receive a Claim Kit to help manage and navigate the process of restoring your good name. Once again, the level of your activity and diligence in managing the post-loss restoration process will influence how quickly you can overcome the burdens. If you become a victim, we hope you will understand that the burdens can be overcome. The process will require patience, diligence, and careful organization to document your specific case. Although experiencing identity fraud can be very traumatic and emotional, we hope any actions on your part will be conducted in a professional manner with an appropriate amount of aggressiveness. After all, you will need to work with individuals at various companies to help rectify facts and records. You want these individuals to help you and this may be influenced by the manner in which you interact with them.

Section V is our Appendix section that provides various supporting information and forms that will be helpful to review and utilize as appropriate.

As identity fraud evolves and we learn about new criminal schemes or protection practices and tools, we will update our Loss Prevention & Resource Guide and attempt to build the solutions into our membership plans and/or web-site offerings and as an active participant of an Identity Fraud Membership Plan, you will always have access to our latest Guide. In the meantime, we recommend that you start to get organized and educated, create a personal identity fraud file (perhaps a three-ring binder), download, print, and use this Guide today. Be sure to review future versions for notable changes. The version you are reading now is Version 5.0.

Section II – Facts, Figures, and Laws

The identity fraud landscape is filled with opportunities for criminals to abuse personal information. Much of the information that criminals can access is available in the public domain. Access of public records is made easy via public databases that are searchable with the Internet. Other proprietary personal information, like the social security number, can be accessed quite easily via fraudulent routes discussed in this Guide.

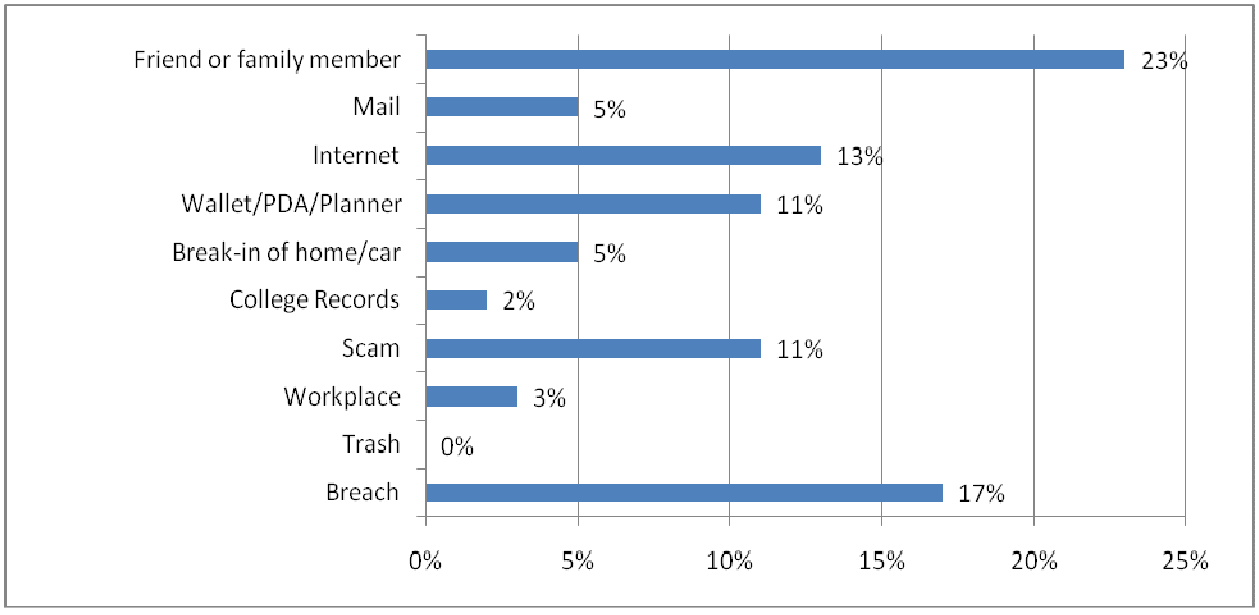
Statistics indicate identity fraud is the fastest growing white-collar crime in America today. In 2009, the Federal Trade Commission reports identity theft was the #1 consumer complaint filed, which numbered 278,078 complaints. Recent data from Javelin Strategy & Research indicates that there 11.1 million victims of identity fraud in 2009, an increase of 12% from 2008. The total costs of identity fraud in 2009 reached $54 billion. The following information summarizes certain findings on identity fraud as reported in a survey by the Identity Theft Resource Center (ITRC).

Impact on Victims (2009)

	New Account Fraud	Existing Account Fraud
Percentage (%) of fraud victims	55%	34%
Costs to victims	$2,104	$527
Victim hours repairing damage	141	68

While it is very apparent that identity theft is the new crime of the millennium and is growing rapidly, it is also useful to evaluate how information is being obtained. The following information provides individual victim responses to survey questions on how data was obtained.

Individuals who knew how their data was obtained



(Source: Identity Theft Resource Center. *Identity Theft: The Aftermath 2009)*

Legislation

There are several laws that impact the use and abuse of our information. Over the years, abuse has focused on our financial information. Laws were established to control financial information handling and sharing practices. Most notably is the Fair Credit Reporting Act that addresses the sensitive information found in consumer credit rep
orts.

We identify below older and newer laws that influence the privacy and security of our information. Please note that this list is not exhaustive. A more detailed explanation of certain laws can be found in our Appendix section. Please note the summary under the FACT Act, which provides details on how you are able to receive free copies of your credit report, once-per-year, from each major credit bureau.

Relevant laws include:

CHILDRENS ONLINE PRIVACY PROTECTION ACT of 1998 (COPPA)

Regulation of unfair and deceptive acts and practices in connection with the collection and use of personal information from and about children on the Internet.

COMPUTER FRAUD AND ABUSE ACT

Section 1030 of the Act addresses fraud and related activity in connection with computers. This section was also amended by the USA Patriot Act to increase the scope of abuse and severity of the penalties.

ECONOMIC ESPIONAGE ACT (EEA)

The Economic Espionage Act of 1996 makes it a federal crime to take, download, receive or possess trade secret information obtained without the owner's authorization.

ELECTRONIC FUNDS TRANSFER ACT (EFTA)

The EFT Act was established primarily because existing consumer protection legislation was unclear when considering the use of electronic funds transfer systems.

FAIR AND ACCURATE CREDIT TRANSACTIONS ACT (FACTA)

The Fair and Accurate Credit Transactions Act of 2003 incorporates specific provisions relating to identity theft, including allowing individuals to access one free credit report from each main credit reporting agency, Experian, Equifax, and TransUnion, as located at www.annualcreditreport.com.

FAIR CREDIT BILLING ACT (FCBA)

The Fair Credit Billing Act attempts to address errors and disputes in billing where the law applies to "open end" credit accounts, such as credit cards, and revolving charge accounts - such as department store accounts.

FAIR CREDIT REPORTING ACT (FCRA)

The FCRA is a federal law that became effective in 1970 and later amended in 1996. One of its primary purposes was to restrict who had access to consumer reports.

FAIR DEBT COLLECTION PRACTICES ACT (FDCPA)

Congress recognized that the collection practices of debt collectors are often abusive, deceptive, and unfair.

FREEDOM OF INFORMATION ACT (FOIA)

The Freedom of Information Act establishes a presumption that records in the possession of agencies and departments of the Executive Branch of the United States government are accessible to the people.

GRAMM-LEACH-BLILEY ACT (GLBA)

The Gramm-Leach-Bliley Act, which passed in 1999, removed barriers traditionally held between banks, investment banks, and insurance companies changing laws that have been in effect for over 60 years. Known as the Financial Modernization Act, it also began to address information sharing practices among financial institutions having control over non-public personal information.

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)

HIPAA provisions address a multitude of healthcare practices including the privacy and security of our healthcare information. The Privacy Rule was added in 2003 to limit the uses and disclosures of personal health information, further define patient's control of their own health information, and strengthen the enforcement of HIPAA.

HEALTH INFORMATION TECHNOLOGY FOR ECONOMIC AND CLINICAL HEALTH ACT (HITECH)

The HITECH Act promotes the adoption and meaningful use of health information technology. It also addresses the privacy and security concerns relating to electronic transmissions of health information.

THE IDENTITY THEFT ASSUMPTION AND DETERRANCE ACT (ID Theft Act)

The ID Theft Act addresses "Fraud and Related Activity in Connection with Identification Documents and Information". The Act, which became effective October 30, 1998, makes identity theft a Federal crime with penalties up to 15 years imprisonment and a maximum fine of $250,000.

INTERNET FALSE IDENTIFICATION PREVENTION ACT

The Act criminalizes the use of computer equipment and the Internet to create false identification documents and also outlaws the practice of producing false identification documents containing easily removable disclaimers.

THE PRIVACY ACT OF 1974

The Privacy Act of 1974 is a companion to the FOIA. The Privacy Act regulates federal government agency record keeping and disclosure practices.

THE USA PATRIOT ACT

The Patriot Act was passed on October 24, 2001 as a result of and following the terrorist acts on September 11, 2001. The full name of the Act is "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism", i.e. USA PATRIOT. The Act was established "To deter and punish terrorist acts in the United States and around the world, to enhance law enforcement investigatory tools, and for other purposes".

In addition to having more focused legislation on security and privacy, there is a trend towards having companies be more accountable for the information they maintain. This includes a higher standard of care for the personal information they maintain and a need for adequate procedures and computer security to prevent unauthorized access to information. If companies fail to secure personal information, they may be liable for their negligence.

Certain new laws require companies to notify customers and/or employees if personal information has been compromised. Additional laws require the destruction of personal records prior to disposal. In California, a "shredding" law under proposal requires individual homeowners to destroy personal documents of persons they employ or face liability if thieves later access information.

Existing and future law provides important protection against fraud. For example, credit card fraud is a very common occurrence. Any time you experience card fraud on your existing accounts, your liability is limited to $50 by law and many firms have adopted "zero liability" policies. However, any time you are a victim of credit card fraud on your existing accounts, you should be alerted that someone, somewhere, is abusing your information. Although fraud and fraud attempts are increasing, newer technologies are helping detect and prevent fraudulent transactions.

If your information is not stolen via dumpster diving, mail theft, or lost wallets, etc., unscrupulous individuals employed at business organizations that have access to information may steal information for their own abuse or will sell the information to criminals who will abuse it. The combination of having vast amounts of information stored in databases coupled with fraud threats and vulnerabilities and the power of the Internet and today's technologies has helped put privacy and computer security issues at the forefront of our society. It is important for individuals to exercise caution and to develop good practices to reduce the potential to becoming victimized.

Section III – Pre-loss Protection

We hope you never become a victim of identity fraud. *Section III* will identify and guide you through a series of actions you can take that will reduce your exposures to becoming a victim. Because exposures to identity fraud are so varied, it is important to look at the "big picture" and consider all the areas where you can reduce your risks. As a fundamental approach, we want you to become more conscious and more cautious with how you share and manage your information. The guides we provide in this section are not exhaustive and likely do not cover all areas where you may be exposed. Thus, it is important to consider your personal situation and take the appropriate steps that you feel will help reduce your risks.

We divide *Section III* into several main categories of protection, including:

1. Account Identification
2. Staying Current
3. Physical Risk Management
4. Technology Risk Management
5. Credit Monitoring Tools
6. Practices for Employees
7. Claim Process

It is important to emphasize that adopting prudent risk management steps and protection practices helps reduce the chance of becoming a victim **but is no guarantee** against becoming a victim. If and when you become a victim, there are few places you can turn for assistance. You must take control of your specific circumstances. However, with the Identity Protection Plan provided by Identity Fraud, Inc., you have access to VRS Elite™ assistance that will help you overcome your burdens.

We recommend that you follow our guide with diligence and with consideration as to how the steps will apply (or not apply) to your specific situation.

Section III.A. – Account Identification

Section III.A. provides both a guide and a worksheet. We recommend that you allocate some time to complete this section to the best of your abilities. Getting organized and identifying exposures is the fundamental beginning point for any risk management protection effort.

Step One – Getting Organized

We suggest that you take the following steps to begin the process of getting organized.

1. Print and Read this Guide
2. Organize the Loss Prevention Guide into a 3-ring binder
    a. Separate the sections with tabs
3. Complete the worksheets provided
4. Keep the binder secure and protected

Getting organized will be very helpful in several ways. Namely, you will save time knowing what you need to do and will feel more confident about overcoming hurdles. Under *Section IV*, Victim Action Items, we will uncover additional steps to staying organized. Documenting your activities is not only a time saver but **very important** as you will need good records to support your identity theft case, whether in phone conversations or when sending letters, affidavits, or other documents.

Step Two – Identifying Current Account Relationships

Part of becoming organized is determining with whom you have existing financial relationships. This is information you know (or should know). By keeping track and monitoring existing relationships, you will have a greater chance of detecting fraudulent activity. Unfortunately, identity fraudsters typically open new accounts that you may not be aware of. We discuss steps in the following sections on how best to detect new accounts being opened in your name, i.e. credit solutions like credit monitoring.

The information that you compile here will serve to identify all of your current relationships (*it may even serve as a financial management sheet to reflect on how many dollars you are spending on each or how many necessary or unnecessary accounts you have*) and what the important contact numbers are, common billing dates, and passwords, if you wish. We suggest you add this worksheet to your identity binder to help keep you organized. But the worksheet will contain sensitive information and therefore, we suggest you keep your identity binder or the worksheet in an accessible but protected area away from prying eyes or thieves.

The worksheet outlined on the following page and located in our Appendix is intended to help you monitor and track relationship activity, like when bills should be arriving in the mail or who to contact when you need to cancel lost or stolen cards. It serves as a worksheet that can help keep you organized.

Canceling credit cards or other accounts is very important if you have lost cards or recognize fraud occurring on your accounts. There are services that will act on your behalf and report lost cards to your vendors in order to save you time. You may wish to select one of these service providers and supply them with your pertinent account details. We want to emphasize some caution. Although these services can be useful in saving you time, they require you to disclose sensitive information, i.e. your account details. Identity Fraud, Inc. does not provide these services as we strive to limit who has access to proprietary and sensitive information. We want to start building a cautionary approach to managing your information. By limiting who has your information, you begin to take control of its access and abuse and by completing the worksheet provided in the Appendix, your own organization will save you valuable time.

Worksheet 1 – Identification of Accounts (See Appendix for Actual Worksheet)

(Keep the worksheet in a safe place)

Type / Firm	Account #	Password	New Password	Mail Date	Monthly	Contact
Financial						
Credit Cards						
Example: Citi	4000-1111-2222-3333	XYZ12ab	Change 10/1	4th	$500	1-800-123-4567

Type / Firm: Example, credit card, utility, etc. Firm or company account is with. Consider all accounts, financial, utility, health, leisure, Internet, etc.

Account #: The account number(s) you have with the firm(s).

Password: Current Password on this account. If you forget, you can always refer to this sheet but remember to keep this document safe.

New Password: Every three months or sooner, you should change your passwords, especially if you maintain the same password on your different accounts. This worksheet should help remind you when to change your passwords.

Mail Date: Bills typically arrive on the same days each month. By monitoring when you receive bills, you can better detect if a fraudster has assumed your identity and changed your address to a new location. If so, your bills may not appear in the mail. This should be a warning and you should contact your vendor to determine if and when a bill was mailed and to what address.

Monthly: Estimated monthly costs or balance(s). Any large deviation may mean fraud.

Contact: The telephone number for customer service or fraud hot line to report stolen or misplaced cards. As soon as you lose a card(s), don't hesitate to contact your vendor. Quickly contacting your vendor may prevent fraudulent use of your account and may result in apprehending the thief when they attempt to use your account.

This worksheet is a tool to help organize and manage your relationships. The categories can be changed to fit your individual desire for organization. This is your worksheet. If you feel information should be added or omitted, feel free to modify the worksheet. We provide a worksheet that you can download in the Members Section of our website. This is only a guide. Monitoring your account activity, managing passwords, and having contact details for emergency notification will each add value to your identity theft prevention efforts.

Section III.B. – Staying Current

Identity Fraud, Inc. produces a quarterly newsletter that speaks to identity fraud issues and other pertinent information we feel may be of value to you. Our newsletter may be mailed to you via e-mail with copies also residing in our Members Only section for your continued reference. In addition to the newsletter, you should pay attention to information in the newspapers, radio, magazines, television, etc. that can alert you to scams, like phishing scams, legislative efforts, or other relevant information.

The topic of identity fraud is part of larger social issues involving privacy and security that are at the forefront of our society. As our risks to financial fraud, terrorists, and cyber crimes become more apparent and real, we have to consider the problems and the solutions. Certain solutions that increase our security will have costs. For example, individuals and corporations must become more diligent in their computer security practices to safeguard our (and their own) information. This requires allocating funds to computer security. Similarly, America has increased its efforts to fight terrorism. Taxpayers will need to pay for increased levels of security. As we increase our efforts for greater security, the results will hopefully provide a safer environment for us to live.

In many cases, increasing security will also result in increasing our privacy, like having restricted access to our medical information. However, in some cases, increasing security may decrease our privacy. Currently in airports, we must allow our luggage and persons to be searched indiscriminately. Although we should understand the reasons why this is needed, it can feel like an invasion of our privacy. Similarly, communications over the telephone and Internet, etc. can be screened and analyzed for threatening information by our own government. The increased need for security may delve into our private affairs. The costs must be weighed against the benefits.

Privacy and security are important issues today because of the convergence of many influencing factors. Technology has developed to the point where small nuclear or biological weapons can cause catastrophic losses. We also use technology in our infrastructures to help provide us with goods and services, like distributing energy, performing financial transactions, etc. Technology also allows for the creation of vast databases of our personal information and with technology, we have almost immediate access to information. Technology threats like information warfare or even a simple computer virus could seriously damage our infrastructure at considerable cost.

Staying current about identity fraud, privacy and security issues are important because they affect each of us in our daily lives. As we address these issues in our current environment, they will influence how we interact and how future generations will interact. Thus, we encourage you to stay current and educated on these issues and voice your opinions regardless of where or how you feel about them.

To help you stay current, it is a good practice to review your credit reports from each of the main credit bureaus Experian, Equifax, and TransUnion. Under the Fair and Accurate Credit Transactions Act of 2003 (the FACT Act), you may obtain **one free credit** report from each main bureau, once-per year. Simply visit www.annualcreditreport.com or call 1-877-322-8228.

Review the following links or other links at www.identityfraud.com to help you stay current:

- Federal Trade Commission - http://www.consumer.gov/idtheft/ (View Laws, schemes, etc.)
- Consumer Privacy Guide.org - http://www.consumerprivacyguide.org/ (The site gives you useful tips for protecting your privacy and helps you take control of the way your information is used.)

For other useful information, search the web under: privacy rights; fraud; identity fraud, etc.

Section III.C. – Physical Risk Management

Section III.C. follows the risk management process of identifying exposures and taking steps to implement solutions. By now, you should be educated to the fact that identity fraud can happen to anyone, anywhere, at anytime. We provide additional educational points throughout this guide.

By referring to physical risk management and physical exposures, we mean items that are tangible, that we can touch, for example, shredders physically cut and destroy paper documents. Tangible physical items like our credit cards are contrasted from data on our computers or information in a hospital database that we do not touch. Data has value and we explore protection practices for data in the following Section III.D. under Technology Risk Management.

Following Section III.A., you should be able to identify all of your current financial relationships and accounts where you have a financial obligation, or where you have disclosed information to vendors and an account has been established. Protecting these accounts requires you to monitor and manage the accounts as each of these relationships presents an opportunity for fraud and abuse. However, monitoring existing account activity is easier than monitoring new accounts that can be opened in your name because you may not even be aware of new accounts that are opened fraudulently until creditors come collecting for past due funds.

Before we discuss the Physical Risk Management - Areas of Exposure and Solutions as described below, we need to uncover and help you manage an important area of exposure, **your credit**. Please take a moment to reflect on your need for credit, or *access to* new credit. If you have a very healthy credit position and do not foresee a need for new credit card accounts, you should consider 'closing the door' on credit grantors. In addition to opting out of marketing campaigns, one of the ways to help control new credit accounts from being opened in your name is to place a **fraud alert** and statement on your credit bureau records. A fraud alert and statement **should** reduce the opportunity of opening new accounts. We emphasize SHOULD. Often times credit grantors do not access information from the credit bureaus or the information goes unheeded. We describe the important fraud alert process as follows:

Area of Exposure
Credit grantors allowing new accounts to be open in your name without your explicit approval.

Problem
Obtaining new credit is too easy. Identity thieves may possess personal information and open accounts in your name which is referred to New Account Fraud or True Name Identity Fraud. You might not be aware of the new accounts as they usually have a mailing address different from your own. The fraudster uses your good credit to run up bills, sometimes making small payments to keep the accounts current, and eventually, they stop making payments. Creditors search their information records and catch up to you at your current address. The identity fraud nightmare begins as you attempt to clear your records.

Solutions
Perhaps the best way to monitor new account or fraudulent activity is to purchase a credit-monitoring product (like our credit report weekly alert or credit monitoring tool). These alerts will alert you to any changes in your credit reports, like a new account that opens.

Another solution is to place a "fraud alert" on your credit profiles with each of the three main credit bureaus. The alert should be followed with a statement similar to, "I may be a victim of identity fraud. Do not extend any credit without first contacting me personally to verify all applicant information. Contact me for verification at my home or work telephone numbers.

The fraud alert should reduce the chance of new accounts being opened without your explicit approval. *However, before placing a fraud alert on your bureau records, determine if you will need or want access to "instant" credit*. For example, credit grantors typically offer good incentives for people opening new accounts. They may offer instant "10%" discounts off purchases which dollar savings can be attractive. Having fraud alerts on your records may prevent you from getting instant credit even when you want it. If you need or like access to new instant credit, placing a fraud alert on your records may not be appropriate.

Action Steps

1. Purchase a weekly alert or credit-monitoring tool providing you with alerts to any changes in your credit records.

Initial Alert

2. Determine your desire or need for new credit opportunities. If new or instant credit opportunities are NOT desired, place an alert on your records by contacting each of the main bureaus by telephone and placing an initial fraud alert on your credit records. A fraud alert will reside on your records for 90 days.

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

It is not necessary to contact all three agencies, once you place an alert with one bureau, they will automatically notify the other two agencies and they will place an alert as well.

Seven Year Fraud Alert

3. Contact each bureau in writing and ask them to place a seven year alert on your credit files. They may require a copy of a law enforcement or other legal report of identity theft to honor your request.

Equifax	**P.O. Box 105314, Atlanta, GA 30348**
Experian	**P.O. Box 9701, Allen, TX 75013**
TransUnion	**P.O. Box 2000, Chester, PA 19022-2000**

Fraud alerts may only be removed in writing by mailing your request to each of the bureaus. Typically, some identifying information must be included like a bill or copy of your driver's license and a copy of your social security card.

Due to the increasing amounts of identity fraud, the three main credit bureaus are constantly updating how they address fraud. As laws dealing with fraud are changing quickly, their practices will also likely change. Be sure to follow their directions.

Areas of Exposure / Solutions

In addition to taking an appropriate course of action regarding credit monitoring and fraud alerts as mentioned above, the following information and practices should be integrated as best as possible:

	Area of Exposure	Potential Solutions	Action Taken
1.	Information Accuracy (Current Records)	Review your records for accuracy in the following areas: 1. Credit Bureaus – Obtain copies of your credit reports from the 3 main credit-reporting agencies (Experian, Equifax, and TransUnion). 2. Check your driving records and ID at your Department of Motor Vehicles. 3. If available, review your Social Security Administration earnings report (Traditionally sent out annually, however due to budget cuts this service is temporarily on hold) 4. Review your medical records at the Medical Information Bureau (www.mib.com). 5. Review your ChexSystems report for banking and checking history. (www.consumerdebit.com)	√
2.	Personal documents in the home	Thieves may enter your home and take your personal documents before they take your T.V. or DVD. Keep documents in a safe place and safe from prying eyes. This includes family and friends. Unfortunately, almost 14% of identity fraud victims know their assailant.	
3.	Personal documents in the mail	Mail theft is a major problem. Watch for your mail, monitor when bills or cards arrive. Consider buying a mailbox you can lock to secure incoming mail. Consider buying a Post Office box where mail can be received and better guarded. When mailing, drop mail at the post office. Also, consider paying bills on-line. With encryption, on-line bill payment is often more secure then mailing bills.	
4.	Discarding personal documents	Shred important personal papers. Dumpster diving frequently uncovers important details in the information or paper you discard.	
5.	Disclosing personal information	• Be cautious with whom you disclose information. Never give out personal information on the phone unless you are confident the people are legitimate and have a legitimate need. • Be careful when participating in surveys or promotions for "free giveaways". The information you disclose will be used somewhere, somehow. • All institutions, financial and healthcare especially, are under increasing pressure not to share your information. Consider "opting out" of allowing your information to be shared or sold. • Memorize your social security number and don't provide it to people who do not need it. Only companies needing to report income or revenue to the IRS should get your SSN. • Watch out for "shoulder surfing". Grand Central Station in NYC is one of the biggest crime scenes in America as thieves watch people entering sensitive information (like on calling cards). • Reduce the amount of information you place on all documents. Don't put your SSN, driver's license, or telephone number on checks and consider refusing to shop where these identifiers are requested.	-- --

6.	Securing personal information	Place passwords on all your accounts where you can. Passwords will increase the level of security on your accounts but they are not foolproof. Be sure to use passwords that are not easy to guess and change them frequently.	
7.	Solicitations by mail/phone	Consider opting out of receiving "pre-approved" credit offers. Call 1-888-5-OPTOUT to remove yourself from these offers. (There are about 5 **billion** credit card solicitations mailed out each year. Each presents an opportunity for fraud.) You can also write the Direct Marketing Association. See the Appendix section for contact information.	
8.	Correcting Inaccurate Information	Information at credit bureaus, your financial institutions, or your healthcare provider should be monitored for accuracy. Dispute incorrect information and follow through to make sure needed corrections are actually implemented. This includes monitoring all your bills and accounts for accuracy. Every time you use your ATM, see your bank statements, or view your bills, make sure your balance is correct. Do not pay for any fraudulent transactions.	
9.	Credit Cards	How many credit cards do you really need? Consider canceling (and cutting up) cards you do not use. Close accounts "at customer's request".	
10.	Other Magnetic Cards	When you visit a hotel, you are often given a plastic card key. The keys with magnetic stripes typically contain your personal information. When you leave these keys behind, turn them into the hotel counter, or fail to destroy them, you are leaving your personal information behind. Be careful with any card that has a magnetic stripe and destroy them personally when you done using them.	
11.	Personal Identification	Keep your passport, birth certificates, social security card, and other forms of ID you do not readily use in a safe place. Go thru your wallet or purse and clean out items you do not use and should not carry.	
12.	Personal checks	Pick up new checks from your branch. Checks are often stolen from the mail. They are very easy to identify.	
13.	Lost documents	If you have misplaced or lost cards, checks, your wallet, etc. cancel the accounts immediately "at customer's request". While you think you might find the lost items, a criminal will likely be making use of your lost items in the meantime. Time is of the essence. Early detection and notification of the lost item may also result in the criminal being caught in the act of a transaction and potentially save you from incurring losses.	
14.	Be Proactive	Take steps to limit and control your information wherever it may be. With new and existing relationships, determine how vendors use, share, or sell your information. Most companies now have privacy policies and practices that indicate their intended uses. If you are not satisfied with these, consider changing to new vendors.	
15.	Be Suspicious	Increase your attention to privacy related matters. Be suspicious of people asking for information and the ways you handle, store, and secure your information.	
16.	Remaining Risks	Recognize that information about you is already in circulation. You should take appropriate steps as indicated above and throughout this guide that will reduce your risks. Gaining better control over, monitoring, and managing your information should become part of your daily practices. By adopting good practices, you will lessen your chance of becoming a victim but realize you may still be victimized and therefore should maintain your membership that provides victim assistance and expense re-imbursement for certain costs you may incur.	

Section III.D. – Technology Risk Management

Section III.D. Technology Risk Management steps should be considered and implemented alongside the other risk management steps identified in this guide. By referring to technology risk management, we mean items, actions, or information that are influenced by computers or similar technical devices. Taking appropriate technical steps to reduce your exposures is highly recommended.

There are many information technology exposures that influence the use and abuse of your information. Many of the exposures are beyond your direct control. For example:

- Information stored in databases – Our information rests in many different databases and many of the databases can be accessed by hackers or by other fraudulent means. It is very difficult to control your exposures in a database that you do not manage.
- Access to your information – Whether at your healthcare provider or financial institution, individuals have access to your information. Your information may be obtained and used for illegal purposes by unscrupulous people who have access to your information
- Sharing or selling your information – Currently, the law allows for certain information to be shared and/or sold. The more your information is shared, the more the possibilities and opportunities for abuse increase.

The opportunity to control how your information is stored, accessed, or shared will change over time as privacy and security issues evolve and as companies face liability for the improper use of your information. There are also increasing amounts of legislation being adopted to further manage the exposures to your information.

The cyber world is expansive, always changing, and can be a risky place to share information. Therefore, as you venture into the cyber world, proceed with caution. Someone, somewhere, will likely record what you provide, say, or do. Whether it's accessing information in a database or using a cell phone or sending an email, information and communications can easily be found, heard, and read.

Before we describe the areas of exposures and solutions as described below, we encourage you to spend some time to learn about yourself on-line. You might be amazed at the type of information that exists about you or other people who have the same name. Much of the information accessible is public information. Depending on how much information you wish to uncover, you can access the web or web services that can uncover important details. Simply search your name, and/or variation of your name, phone number, address, etc. at www.google.com.

Areas of Exposure / Solutions – General Technology Related Protection Practices

Consider the following areas of exposure and steps to help increase your safety in our electronic age.

	Area of Exposure	Potential Solutions	Action Taken
1.	Passwords	Passwords do not qualify as strong security when compared to other strong authentication technology but they are a feasible and economical way to increase the level of security to your computer, account information, etc. Passwords increase security by requiring anyone seeking access to know the pass code. Don't share your passwords with anyone. Memorize your passwords and don't leave your passwords for easy viewing. The common practice of writing your password on a "post it" note and leaving this next to your computer is dangerous. Once a password is known, it provides easy access of your identity and becomes very difficult and burdensome to prove that it wasn't you who acted in some particular way.	√
2.	Secure Transactions	When transacting on the Internet, make sure that before you disclose any personal information that the site and page you are visiting is secured. Look for the web site address HTTPS (the "S" means the site is encrypted. Typically, your browser will also indicate when you are entering a secure site or portion of a site. A lock icon appearing in your lower navigation bar on your computer will indicate whether the site is secured. Most web sites utilize 128-bit encryption that protects your information. Do Not transact on sites that do not encrypt your information or do so at your own risk. Take the time to read a company's Security policy. It should discuss how they secure your information. Another form of security is to view whether the site has a digital certificate which authenticates the identity of the site (for example, a Verisign logo can be clicked into to confirm the site belongs to the company you are viewing) Sometimes, you might think you are transacting with a legitimate company when in fact, you might be transacting with a fraudulent imposter site.	
3.	Secure Web Surfing	Web surfing is neither private nor secure. Many firms can track your every move. Consider surfing anonymously. Below we comment on anonymous browsing.	
4.	Home Computer Security	Your home computer can be hacked. If you have a connection to the Internet, people on the Internet have access to your computer and all the information on it. This is especially important if you have "always on" DSL or cable connections. If your computer is always connected to the Internet, people on the Internet will always have access to your computer. In order to protect your information, you should: • Back up data frequently to avoid its loss whether by accident or an intentional malicious act (the newer computers that have CD read/write capabilities make this exercise very simple)	

		• Deploy "patches" to software to fix flaws • Incorporate a password to restrict access to your computer • Purchase virus software to detect and prevent against loss • Purchase a firewall and/or spyware • Consider encryption software that can encrypt your information while stored and e-mails while sending • For laptop computers, consider buying a physical lock to prevent people from walking away with your laptop • Biometric devices can be installed or attached to computers that restrict access • Be careful with business information on your personal computer	
5.	Information disclosure	Every time you complete information on-line, it will be used for a purpose. This includes surveys or on-line promotions for free products or a "chance to win". Another area to be cautious involves "chat rooms". By posting information or comments in a chat room, you are telling the world something about yourself. Can you trust people on the Internet who you do not know? Proceed with caution.	
6.	On-line Directories	Just as the credit bureaus have information on you that they sell to authorized people or firms, the Internet has directories that compile our information. For example, you might consider removing your name from public record websites such as www.intelius.com, www.publicrecords.com, www.ussearch.com. Unfortunately, removing your name from many on-line sources currently appears to be temporary only. After you remove your name, the next month or few months, the companies update their databases and obtain information about you. Most information the companies collect is public information. They access public databases at the state and federal level. Thus, to be effective, you would have to remove your name from the public domain by writing the various Departments of State. As privacy issues evolve, access to public information may become more restrictive. Keep current on laws that may effect change.	
7.	Social Networking	Use caution when setting up or visiting social networking websites (e.g., facebook, myspace, linkedin). Do not share personal information, such as social security number, DOB, maiden name, or your address where an identity thief can easily copy it and try to obtain credit in your name. It is also advisable not to announce an upcoming vacation or absence since that lets others know your whereabouts.	
8.	One Credit Card	Consider using only one credit card for on-line purchases. You will be able to better monitor card activity and should be able to detect fraudulent use.	
9.	Privacy Policies	Most web sites have privacy policies. If they don't, beware. Because privacy policies differ, you should read them carefully. Just because there is a link to a privacy policy doesn't mean it is	

		one you will agree with.	
10.	Too Good	Do you see an offer on the Internet that appears to be too good? Chances are that these offers *are* too good to be true. Exercise caution and consider avoiding the temptation in buying something or disclosing information on these offers.	
11.	Cookies	Cookies can help make your Internet activity more user friendly by storing information about you. However, they can also track your on-line activity. Consider deleting the cookies that are stored on your computer. (For AOL users, be careful which cookies you delete) With Windows, go to your Explorer directory. By going to your C drive under Windows, find the Cookies folder and see how many are stored. Delete these as appropriate. Also, look under the TEMP and Temporary Internet folders and consider deleting these items. This can also improve your computers operating efficiency. Similarly, you may want use your System Tools to perform Disk Cleanup or Disk Defragmenter.	
12.	Shred Data	When you delete information, you will likely not be deleting a permanent copy of the information that resides on your hard-drive. Specialized software can assist in permanently deleting or shredding unwanted stored information.	

Protection products you should invest in

In order to protect yourself and your computer from technology threats, there are some fundamental products you should consider purchasing. The following technology tools can increase your privacy and security. Currently, Identity Fraud, Inc. does not have any affiliation with the following companies. Also, we cannot pledge that any of the products we mention below will work as intended. We provide the information solely to support your own efforts in identifying technologies that may be appropriate.

	Protection Product	Description	Action Taken
1.	**Virus Software**	Virus software can save your computer. Computer viruses can destroy your hard drive, all your information, and generally render your computer useless. This can be expensive and difficult to remedy. Other potential threats like worms, Trojans, malicious active X controls and Java applets are equally destructive and should be protected against with virus software. Virus software works like a vaccine to detect known viruses. When you purchase virus software, you will be obtaining a defense against these known viruses. Should a known virus enter your system via e-mail or a diskette, the software should detect it and "quarantine" the file or code containing the virus. Unfortunately, new viruses are being created rapidly. It is estimated that there are 6-10 new viruses being created daily and that there are 100's of thousands of viruses. Thus, it is important to stay current on the latest viruses. If you buy a virus software	√

		license on a subscription basis, you can download current updates. You should make sure to update your software frequently (every few days) and scan your system once a week. Updates can be obtained by downloads from the internet. Popular anti-virus software venders can be reviewed at: http://antivirus.about.com/cs/antivirusvendors/	
2.	**Firewalls**	A firewall is a system that serves to manage access to your computer. On one hand, the firewall works to prevent access and block traffic, on the other hand, it works to allow access and traffic. It is important to realize that when you (your computer) are connected to the Internet, you have access to the Internet and people on the Internet have access to you. If you subscribe to "always on" DSL or Cable Internet connections, your computer is always available to outsiders. Hackers or identity thieves can rummage through your personal information on your computer, retrieve details, or destroy your system with malicious code. A firewall can help prevent unwelcome access and can serve as an important tool to help reduce your overall risk. Visit http://www.firewallguide.com/ or http://www.norton.com or http://www.mcafee.com/ to learn more or purchase products.	
3.	**Anonymous Web Browsing/email**	Sending e-mail over the Internet is similar to sending a postcard through the mail. The content of e-mail, its origin, and the intended recipient can be tracked and viewed by people or groups who have the ability and desire to monitor it. In fact, every unsecured move you make on the Internet can be monitored. Monitoring is helpful when we consider the need to assist law enforcement with the ability to seek out criminals or track down hackers, but depending on your viewpoint, it can also infringe upon rights to privacy, be abused by marketers, and represent the ability of "Big Brother" to watch over you. With encryption, you can protect and keep hidden 1) what you send, and 2) where you go. Click on www.anonymizer.com to view a popular site.	
4.	**Keyboard Encryption**	One way that criminals obtain sensitive information intended for fraudulent use is by facilitating the download of a virus or spyware application to your computer. A popular form of spyware is the keystroke logger, or “keylogger” virus. Keyloggers are capable of recording your every keystroke, whether online, offline, or both. This invasion of privacy gives criminals access to your usernames and passwords, credit card numbers, bank account numbers, and other confidential information that you may type for various purposes. A similar type of spyware can capture periodic images of your screen, thus accomplishing the same purpose as the keylogger. Avoid becoming of victim of these stealthy invaders by investing in keyboard encryption software and/or antispyware that will detect and remove keyloggers. Visit www.GuardedID.com to view proactive protection products against keylogger threats.	

Section III.E. – Credit Monitoring & Reviews

Section III.E. Credit Monitoring & Reviews address the reasons why monitoring and reviewing the information in your credit report is crucial. First, it is important to view your credit reports from each of the three main credit-reporting agencies (Experian, Equifax, and TransUnion) simply to make sure they are accurate. A June 2007 Consumer Reports study estimated Consumers find some 13 million inaccuracies on their credit reports each year. Second, you should review your reports in order to guard against fraudulent accounts being established in your name. Be sure to obtain your **free reports** as provided under the FACT Act.

Many people and firms access your credit report to evaluate whether you are a good risk. The reports contain your name and any name variations, your addresses, past and present, telephone number, social security number, date of birth, employment information and matters of public record such as civil judgments, tax liens and bankruptcies. The information in your report can be used to generate a "score" that forms a basis for evaluation and decisions on loans and insurance. A high score is considered good and a low score is bad.

Under the Fair Credit Reporting Act, people or firms that have a "legitimate business need" can access your credit reports. These include:

- Credit grantors
- Insurance companies
- Landlords
- Employers and potential employers (with your prior consent)
- Companies with which you have a credit account for account monitoring purposes
- Those considering your application for a government license or benefit
- A child support enforcement agency
- Any government agency

Reviewing your reports for accuracy is critical because decisions are made based on the information in your reports and the scores that are generated. If inaccurate information is part of your report, firms are not being provided with an accurate reflection of your true position. This can adversely affect your ability to obtain loans, credit, employment, etc. Unfortunately, bad information that is *accurate* cannot be removed from your reports. But *inaccurate* information can and should be corrected.

Inaccurate information may arise in your credit reports due to data entry errors, errors entering information on the wrong person (where two people may have the same name or similar SSN) or cases involving fraud wherein an imposter has co-opted your name and generates activity impacting your record. The law does allow inaccurate information to be removed or corrected.

Correcting Errors

In order to detect errors, you must first identify the errors by reviewing your credit reports. If errors are identified, you can initiate the correction and dispute process that includes the following:

1. Write to the Credit Reporting Agency (CRA) indicating details of your dispute. The CRA has up to 30 business days for an investigation to modify or remove inaccurate information. The bureau must consider all the relevant evidence you give it, and errors must be corrected. If the CRA cannot verify negative information, it must be deleted from your file. You are entitled to receive a free copy of your corrected report. You may ask the credit bureau to send a corrected report to

anyone who has requested your file in the past six months and to anyone that has requested it in the last year for employment.

2. If you disagree with the result of the CRAs investigation, you have the right to submit a 100-word explanation. The credit bureau must include the explanation in your file, although the negative information will not be removed.

Sometimes corrected errors reappear in credit reports at a later date. Federal law requires credit bureaus to notify the consumer within five days of reinserting information. Negative information cannot be reinserted into your file unless the credit bureau takes the added step of having the source of the information certify that it is complete and accurate. Credit bureaus must provide a toll-free number to dispute the reinsertion along with the opportunity to include a dispute statement. It is a good practice to periodically check your credit report to ensure that errors in your report are indeed corrected.

Credit Monitoring

Monitoring your credit statements with the bureaus is a prudent activity. In addition to reviewing your statements for accuracy, credit monitoring is one of the best ways to detect fraudulent account activity. Early detection of fraudulently created accounts is important to stop the situation from getting worse. It may even help in catching the criminal in the act when they attempt to use the fraudulent account.

Identity Fraud, Inc. recommends purchasing one of our credit monitoring tools. By purchasing the credit monitoring service from our web site, you are reducing your risk to loss.

Members having our Identity Protection Plan may obtain credit-monitoring tools as our preferred member discount prices. If you have questions, simply give us a call at 1-866-4-IDFRAUD (1-866-443-3728).

Section III.F. – Practices for Employees

Identity fraud arising from the workplace is increasing and this section will outline certain steps to consider for protecting you in the workplace environment.

Essentially, your workplace environment is similar to your home environment in many ways. You have personally identifiable information that can be uncovered, you probably utilize a computer or have access to computers, and you likely work closely with colleagues in the course of your employment. Thus, the physical and technology protection practices described in the previous sections should generally be mirrored when considering your workplace environment and employee practices.

In addition to the previous sections, prudent areas and activities to consider in the workplace environment include:

Areas of Exposure / Solutions

	Area of Exposure	Potential Solutions	Action Taken
1.	Personal information in the workplace	Your individual personnel files contain sensitive information. Is your SSN used as an employee identifier? Speak to your human resources manager and confirm their information handling and protection practices. Recommend changes. Your employee information should be secured in locked cabinets and available only to authorized persons. Similarly, the computer system that stores your employee information should be adequately protected. Either thieves or unscrupulous workmates can uncover information in your office, from HR, via the garbage, or from you if they pretend they are somebody they are not.	√
2.	Discarding documents	Shred important documents. Both HR and you should shred appropriate documents that contain private information. This includes paper and computer data. This practice should be extended to shred important corporate documents before throwing in the trash.	
3.	Disclosing information	Be cautious with whom you disclose information. Never give out personal information unless you are confident the people are legitimate and have a legitimate need. Keep your passwords private. If you share your password, someone can masquerade as you and this can lead to trouble. Don't keep your passwords on post-it notes. Memorize them and make sure to change them frequently.	
4.	Business Credit Cards	You should monitor account activity like you would your own. There is no reason thieves can't abuse your business credit cards.	
5.	Employer Web and e-Mail Monitoring	Check your employer's computer usage and monitoring policy. If one does not exist, ask that one be created. This will help establish what the rules of employment are. Certainly, an employer has the right to monitor your web-surfing and email activities if they communicate their practices to you. Remember that where you visit on the web or what you send in an email can be stored and referred to for many years. If your practices are inappropriate, this could lead to termination.	
6.	Be Suspicious	As with any of your personal or business dealings, consider the sensitivity and protections that should be given to information.	

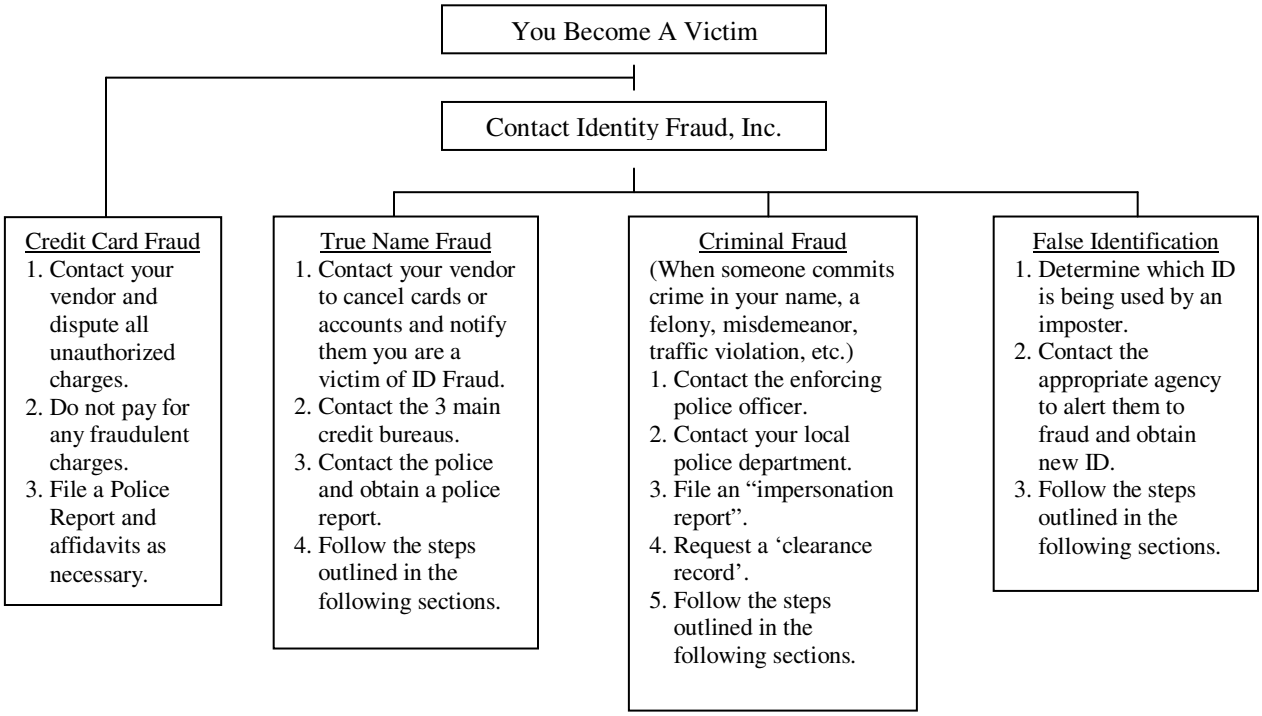
Section IV – Victim Action Items

If you are a victim or believe you may be a victim of identity fraud, you should take immediate steps to halt the destruction being done to your good name. This section is broken down into the following four main categories:

1. Immediate Action Items – Steps to follow including contacts to be made and letters to be mailed.
2. File Creation & Case Organization – You will be compiling important records of communications via the telephone, letters, reports, and affidavits. Keeping good documentation is needed to save you time, help keep your sanity, give you confidence, and prepare your case.
3. Claim Kit - We describe the elements of the Claim Kit that you will receive following your notice of a loss to Identity Fraud, Inc. The Claim Kit will comprise letters that can be used in contacting appropriate parties to clear up your records.
4. Filing a Claim – We outline specific action steps and items needed to present a claim in order to be reimbursed for certain expenses you incur as a result of being victimized.

It is important to realize that different types of identity fraud exist that will affect your specific course of action. For example, credit card fraud is a common occurrence but does not require the same action as if you are a victim of True Name Identity Fraud. Similarly, if an imposter commits a crime in your name, like theft or drunk driving, you are a victim of Criminal Identity Fraud and will need to take appropriate steps to clear your name. In all cases contact Identity Fraud, Inc. toll-free at 1-866-4-IDFRAUD (1-866-443-3728). We can evaluate your specific situation and escalate your case to our Victim Assistance Counselors to help you through the process.

We provide the following outline as a brief overview of the process that may be needed to rectify your situation. This outline is supported in the following sections with more detailed action steps.



Section IV.A. – Immediate Action Items

When you become a victim of identity fraud, it is important to take immediate action. Emphasis is placed on **URGENT** items in steps 1-6 below and is followed by additional steps on the following page.

First, if you are a victim of the most common type of fraud, credit card fraud, contact your vendor(s) and alert them to the unauthorized charges. Remember that the law states you are not liable for more than $50 of unauthorized fraudulent charges (they may waive this). Simply removing the fraudulent charge may properly address the problem.

IMMEDIATE / URGENT ACTION ITEMS – TRUE NAME IDENTITY FRAUD

1. Contact Identity Fraud, Inc. toll-free at 1-866-4-IDFRAUD (1-866-443-3728). We will evaluate your situation and likely escalate your call to our VRS Elite™ Victim Assistance Counselors.

2. Gather your personal Identity Fraud binder, a pen and paper, and record pertinent communication details including with whom you speak, their position or title, location, time, telephone, address, and conversation summary. This documentation will be supportive as you proceed.

3. Contact the vendors of your lost or stolen cards, or accounts that are being used fraudulently. Close the accounts (at customer's request), request new accounts to be established with new passwords if this is appropriate. Stop payment on any lost, outstanding or recently issued checks. Also, contact the Check Verification companies.

4. Contact the fraud departments at the 3 main credit reporting agencies (CRA's), Experian, Equifax, and TransUnion, and place a verbal fraud alert and victim statement on your file. Do this via their automated voice systems or while speaking with a live person. Request the CRA's to notify all parties who received your reports in the last 6 months (1 year for employers) and request their phone numbers to contact them and ask they issue no credit to fraudulent imposters.

5. Obtain copies of your credit report from the 3 main CRA's. Your reports will automatically be issued to you following your contact to the CRA's above. Although the reports ordered directly from the CRAs following an identity fraud incident are free, you should seriously consider purchasing a "3-in-1" on-line credit report from our site. (This is an important time-saver and is secured with encryption). This will give you your report from each of the 3 main CRA's very quickly (about 60 seconds). You can then print out the report to analyze and bring it to the local police to help compile your police report. Alternatively, the credit reports from each of the CRA's will be mailed to you free of charge and typically arrive in 7-10 days. In 7-10 days however, a fraudster may be using accounts in your name and you will not realize which accounts are being used until you review your credit reports.

    a. Review your reports for accuracy and fraud. If you identify any fraudulent accounts, immediately call the vendors and close the accounts at "customer's request" and obtain details on the accounts, like the original false application, billing statements, and contact details on where the cards were sent.

6. Contact or visit your local police department and obtain a police report. In completing a police report, you should provide sufficient documentation including a list of fraudulent accounts. The report will be used in later correspondence. For safety, let the police pursue the criminal but be sure to request or even demand copies of any evidence they uncover that involves you.

ADDITIONAL ITEMS

After you have taken the immediate and urgent items described above, the process for recovering your good name becomes very administrative. As you will need to communicate with a variety of people and companies, support your case in a professional manner with good documentation (including a written summary or your situation), and follow up with each entity to ensure the steps you have taken are actually implemented. The process may take months and requires your patience. With proper pursuit and diligence, you will be able to recover from the nightmare that has been forced upon you.

The following steps may or may not apply in your particular case. The action steps below provide a guide that indicates where appropriate action may need to be taken. They include:

1. Completing a Fraud Affidavit. In many cases, the credit grantors where fraudulent accounts have been established will require you to complete a fraud affidavit. This document lists the accounts in question and is a legal statement from you evidencing fraud. Thanks to Federal Trade Commission efforts, a generic fraud affidavit has been created that can be submitted to many financial institutions / credit grantors. However, not all companies will accept this affidavit. Some companies will require that you complete their own type of affidavit. Although this is cumbersome, you will need to follow the rules established by each different company. Thus, upon contacting a financial institution, ask if they accept the FTC's affidavit. To download the affidavit, visit: http://www.ftc.gov/bcp/edu/resources/forms/affidavit.pdf or visit our Members Section for a download. Firms may request that the affidavit be notarized. Try to resist or seek alternatives but if necessary, notary expenses will be reimbursed as part of a claim made to Identity Fraud, Inc. under the benefits provided in the membership plan. A copy of the affidavit may be downloaded at our site in the Members section or the FTC site.

2. In addition to notifying your credit grantors or financial institutions where fraud may be occurring, contact your other vendors where you have a relationship. This includes your utilities, stockbroker, IRA's, health provider, etc. You should review Worksheet #1 where you have completed a list of your existing relationships. Contact each party and/or monitor the accounts closely.

3. Confirm the accuracy of your records and whether they are being used fraudulently.

    a. Contact your Department of Motor Vehicles – A fraudster will often obtain false ID to help them cash checks and open accounts. In contacting your DMV, you should see if a new drivers license was issued, place a fraud alert (or similar) on your driving record to make sure they do not issue a new ID without verifying your request, and obtain a copy of your driving record to see if any fraudulent activity is associated with your record. If a new license was issued, find out the details including the address and whether a photo and fingerprints were taken. This can help you and the police track down the imposter. The DMV may request that a complaint form be submitted. Complete the complaint form and include relevant information like a copy of your police report and identifying documents. An investigation should be instigated but discuss the exact steps with the DMV. You may need to obtain a new license.

    b. Contact the Post Office - Check with your local Postmaster and the Postmaster of the geographic area where you suspect fraudulent activity is occurring to ensure your correct address. Notify the Postal Inspector that you are a victim of identity theft and determine the appropriate steps to ensure that mail is not delivered to a fraudulent address. Uncover

details that will help identify the imposter. See if an investigation will be instigated and what other specific steps you should take. You may need to complete a complaint form to get the process underway.

c. Contact the Social Security Administration – Report SSN fraud to the SSA. If you are unsure of SSN fraud, review your credit reports and, if possible, obtain an earnings report from the SSA. (Visit www.ssa.gov to see if the Social Security Administration has lifted the temporary hold on sending out benefits statements.) Your earnings report may uncover the fraudulent use of your SSN. Determine appropriate steps you should take with the SSA for your specific case. You should **not** try to obtain a new SSN because it can introduce complications into the vast number of records that already are associated with your number. Also, the SSA will not issue a new SSN unless you can satisfy their requirements and prove that you are being disadvantaged through no fault of your own. In extreme cases, a new SSN may be appropriate.

d. Obtain Your Medical Records - Find out if fraudulent claims or activity have affected your medical history and records. This information is stored in the insurance industry's database at the Medical Information Bureau (MIB). Similar to credit reports, you may obtain a copy for $9 or for free if an insurance company has accessed your MIB report to make a decision. You may also want to contact your health insurer or Doctor for records.

e. Contact the local US Passport Office – Determine if a new passport has been issued, if so, to what address. Advise them of your situation and place a fraud alert on your records advising them that no passport should be issued unless they receive written verification from you first. Follow their procedures. You may want to obtain a new passport if you do not have one. The passport is a primary form of identification, meaning, having just a passport is considered verification of your identity. They are also difficult to counterfeit or falsify.

4. Alert Your Employer – Your human resources professional should learn that you are a victim. Certain employment or benefit records may be affected by fraudulent means and they may help detect or explain errors. Similarly, you may need to take time away from work to help rectify identity fraud problems. Under the Identity Fraud, Inc. membership, certain benefits include reimbursement for lost wages or time taken from work (up to the applicable sub limit). You will need certain documents from HR when submitting a claim and this is discussed more fully in the following sections below. If you are seeking a new job, the prospective employer may perform a background check on you. You may want to advise them you are a victim of identity fraud and that your background may contain inaccurate information. If you are denied employment due to information in your credit report, the employer is supposed to advise you.

5. Contact Appropriate Government Offices – Located in the Appendix is a list of contact numbers and addresses. Consider contacting the Secret Service, FBI, and FTC in addition to your local authorities. The enforcement divisions of the government typically allocate their resources to crime rings or large fraud cases. However, by submitting your case and requesting an investigation, you may achieve some results. The information you submit will likely be entered into a database that law enforcement can access. The more communication and information available to law enforcement should help efforts in arresting fraudsters.

6. Keep organized and diligent in making sure the actions you are taking produce results. Keep good records of your situation and communications, send letters via certified mail with return receipts,

keep track of your time and expenses and keep in touch with Identity Fraud, Inc.'s support counselors. Escalation and attorney involvement may be applicable.

ACTION ITEMS – CRIMINAL IDENTITY FRAUD

The goal for cases involving Criminal Identity Fraud is to clear your good name and records by obtaining a Determination of Factual Innocence, a Certificate of Clearance, cleansing of the criminal databases, and capturing the assailant. Depending on your state, there may be different terms and laws applicable to clearing your name and therefore, it is important to discuss your specific case with the authorities.

The following steps will direct you through the process that you will most likely encounter. You should:

1. Contact Identity Fraud, Inc. toll-free at 1-866-4-IDFRAUD (1-866-443-3728). We will evaluate your situation and likely direct you to our VRS Elite™ Victim Assistance Counselors.

2. Contact the enforcing authority, police officer, sheriff, or court that issued the citation, arrest, or warrant and alert them to the fact that you are a victim of identity fraud and that you would like to file an impersonation report and obtain a determination of your factual innocence resulting in a certificate of clearance. It is best if you can speak with the specific person who issued the citation etc. If the authority is located far away, confirm that they will accept a "Courtesy Report" from your local enforcement authority. Often times the issuing authority may be in a different jurisdiction than your local police. A crime may have been committed in a different city, county, or state. Thus, you may need to work with both your local authority and the authority that issued the original citation, warrant, etc.

3. Visit or make an appointment to visit your local police or sheriffs department to advise them of your situation and to discuss the appropriate remedies. You should request an impersonation report and/or a courtesy report to be completed. You may need to take fingerprints and provide copies of identifying documents like your driver's license, passport, SSN, and current address to confirm your identity. The combined documents will comprise a report you can deliver to the appropriate authorities. You may also need to sign and provide a notarized affidavit to accompany your report.

    a. Ask your local law enforcement officer to run a database check on your name to uncover if any charges exist. They may or may not be allowed to share this information with you, but they may confirm that such records do indeed exist.

4. Mail the report (via certified mail, return receipt requested) to the originating authority and follow up to confirm their receipt and what action steps will be taken next. If possible, include details on the impersonator as best as you can.

5. Contact the Department of Motor Vehicles and request a copy of your records. Typically, an imposter that has committed a crime in your name has your identification and has shown this ID to the issuing officer. Because the information is valid, the officer will not necessarily know that they are dealing with an imposter. By obtaining your DMV record, you may detect a different photograph or address associated with your name. Place a fraud or similar alert on your record and ask what specific steps should be taken. In many circumstances, you should be issued a new drivers license. If you uncover factual details that are pertinent, share these with the police.

6. Upon receiving a Certificate of Clearance, which may require you to appear in court and have an "identity hearing" to substantiate your innocence, begin the process to clear your name in the various criminal databases. Most likely, the fraudulent violation has been recorded at the local county, state, and federal databases. Clearing your name entirely may be impossible, as law enforcement will keep a trail of facts. More likely is to remove your name from the "primary name" on the criminal record. Regardless of the imposters name being known or not, request that a "key name" switch be entered. This will switch your name with that of the imposters name or a 'John Doe'. In any event, your name will likely appear on the record as an alias. For example, John Doe, alias Your Name, has committed felony drunk driving, Section 502…etc.

    a. Keep several copies of any clearance or release letter / certificate. Always carry one with you in case you are confronted by the police for a fraudulent crime.
    b. Enter your name in your state's 'victims of identity fraud' database if one exists. If you are ever confronted by police, you can refer to this database to support your innocence.
    c. Perform a criminal search on your name to determine if your records have been cleansed.

7. Alert Your Employer – Your human resources professional should learn that you are a victim. Bringing attention to your employer will help ensure they do not collect inaccurate information on you. Similarly, you may need to take time away from work to help rectify identity fraud problems. Under the Identity Fraud, Inc. membership, certain benefits include reimbursement for lost wages or time from work up to the applicable coverage limit. You will need certain documents from HR when submitting a claim and this is discussed more fully in the following sections. If you are seeking a new job, the prospective employer may perform a background check on you. You may want to advise them you are a victim of identity fraud and that your background may contain inaccurate information. If you are denied employment due to information in your credit report, the employer is supposed to advise you.

8. You may also need to testify or appear in court in order to prosecute the imposter if they are located and apprehended.

9. In the event of serious offenses or complications in clearing your records, you may need to hire a criminal defense attorney for proper legal representation. Consult Identity Fraud, Inc.'s advisors via the toll-free hotline.

10. Stay organized by keeping records of who, where, and when you have conversations, send letters, or reports. Record your time and expenses. You can recover certain expense under the Identity Fraud, Inc. membership plan or through legal channels if the criminal is apprehended and convicted and the courts grant restitution.

Section IV.B. – File Creation & Case Organization

When you become a victim of identity fraud, you will need to take charge of your own situation, become your own detective, and build a case that is presentable to creditors and the courts. The Identity Fraud Claim Kit will provide pre-drafted attorney letters to help convey professional and legal messages. Quality conduct, evidence, and presentation will go a long way in helping you communicate your problems and optimize your results.

Consider the following steps when creating your files, organizing, and communicating your case:

1. From the date you first become aware of the fraud, begin to catalogue your activities in a summary sheet or journal that can always be referred to. This includes listing the date, the people you speak with, their titles and contact details, length of the call, a summary of the conversations, and diary dates for follow up action. It is a good idea to document conversations by writing follow up letters outlining the facts and action items agreed to in the conversations. When sending letters, faxes or emails, make copies and file them in an organized fashion. Send letters or emails with return receipt requested to evidence delivery. See the Appendix section for a sample Activity Log to enter details into for easy reference and a documented trail on when communications are made or received.

2. Prepare a brief written summary of the pertinent facts surrounding your situation. This summary can be provided to the police, to credit grantors, or other parties to help them understand your facts and should save you time from recreating new letters each time you want to communicate your situation. Items should include:
    a. How and when you first became aware of the fraud.
    b. Identifying specific financial accounts or violations that are mistaken
    c. A brief description of the burdens it has created for you
    d. A brief request for action and support

3. Utilize your personal Identity Fraud (3-ring) Binder to file letters and written summaries of communications by the entity you are working with. For example, a specific bank credit card should have its own location for pertinent communication that can be easily accessed.

4. Get organized from day one and stay current. Don't let letters you send or receive pile up until a later day. You need to be able to access information quickly to save you time and to respond professionally when someone calls on you. Consider creating a new file folder on your computer called My Identity Fraud to store letters, but be sure to make hard copies as well and store them in your identity binder.

5. After obtaining a police report or compiling affidavits, send copies keeping the originals in your files. Regarding affidavits send only the details needed for each specific company. For example, there is no reason why your credit card company should have details on your bank accounts if they are not the same firm.

6. Begin your detective work and record evidence you learn from each of the entities you deal with. Record your suspicions on who, where, or when your fraud was instigated. These thoughts can always be referred to if you write them down. If you are the primary account holder on an account, you have a right to receive copies of original applications, records of purchases and payments, and the contact details on the account. Gathering evidence includes information from the police where you should attempt to learn details from them. Compiling information from different sources may start to help narrow the scope on who the imposter is. You can share your findings with the police when you follow up with them to check on their efforts and progress in resolving your case.

7. Don't hesitate to professionally escalate your case to the next supervisor or manager if you are not getting any results. This could include the District Attorney or president of a firm. But avoid threats and emotional outbursts as this unprofessional behavior could actually create an adversarial relationship when in fact you should be trying to build a team that supports you.

8. Add the contacts you make to the Contact Sheet located in the Appendix for easy reference.

9. Keep a record of all expenses, time, and emotional impact. Certain expenses are recoverable under the benefits provided in the Identity Fraud membership. These or other items may also be recovered via the courts if the imposter is caught and convicted and the court agrees to grant you restitution for your losses.

10. Keep in communication with the police on a periodic basis. Remember that identity fraud cases take a significant amount of time. If your case actually receives some dedicated effort and resources to pursue it, police need to gather evidence, locate the impersonator, build a solid case, and prosecute. They must do this while combating murders, thefts, and other crimes that tend to take priority over identity fraud cases. However, in time, your impersonator may be caught and you will want to keep abreast of any legal proceedings in order to at least provide a victims statement and request for restitution.

    a. Consider contacting the District Attorney and identify who may be handling your case. You might send them your summary statement and see how you can help. You can also ask questions on how the process will proceed, whether you should attend any court proceedings etc.

    b. Prepare a letter or seek support from our Victim Assistance Counselors to help prepare a victims statement letter including a request for restitution from the courts. Any letter should be short and to the point providing credible evidence of expenses incurred, projected future expenses (like the continued need to monitor your credit reports) and a reasonable request for emotional injury. By law, during the prosecution process, the Judge is required to read the victims statement and take it into account when reviewing the case. However, there is no requirement that restitution be paid. (This is another reason why our member benefits are important because many times, the victims have no money to pay you back) The victim's statement and request for restitution is a good opportunity to professionally summarize and state your case. It may also help bring an emotional close to the dreadful burdens you have endured.

11. Monitor your records. Continue to monitor your credit reports every 2-3 months until the level of activity subsides and then at least twice a year. Reviewing your reports or monitoring them with weekly alerts is a good way to stay current. Many identity fraudsters re-engage their criminal activity and begin with the information they already possess.

Remember to build a team that helps you resolve your case. Being organized, acting and presenting information in an accurate and professional manner will help your efforts.

Section IV.D. – Filing a Claim

One of the primary benefits of the Identity Fraud, Inc. membership is the ability to recover certain lost expenses that you incur as a result of rectifying your identity fraud case. In many situations, the criminal fraudsters using your name are 1) not caught, and 2) do not have enough money to reimburse you, thus leaving you to pay for necessary items. Similarly, the government is not in a position to pay you for lost time and expenses associated with identity fraud.

There may be situations where you can pursue legal action against the credit bureaus or credit grantors if they are negligent in their practices, violate laws, or generally contribute to your injuries, however, this process can be extremely difficult to pursue and expensive to have proper legal representation. Your specific case may justify a lawsuit but the troubles inherent with litigation will have to be weighed against the benefits you hope to achieve.

The general lack of financial remedies available to victims was a primary factor in our efforts to develop identity fraud insurance benefits and expense reimbursement coverages. Our benefits are not intended to provide coverage where you already have limitations of liability under law, e.g. you are not liable for more than $50 of unauthorized credit card charges. Rather, they are designed to pay you for expenses you incur, lost wages, miscellaneous expenses and important legal fees if your situation demands legal representation.

The Claim Process

a. Notice of an Incident – The claim process begins by establishing that an Incident has occurred. You will need to contact Identity Fraud, Inc. toll free at 1-866-4-IDFRAUD (1-866-443-3728) to provide us notice. We will likely escalate your incident and call to our VRS Elite™ claims staff.

b. VRS Elite™ Fraud Victim Assistance – We, or our insurer, will help you through the process of gaining back your identity and clearing your records. You will obtain relevant portions of the Claim Kit that apply to your particular situation. We will also advise on what documentation you will need to provide in submitting a claim.

c. Submitting a Claim – Follow our specific directions for submitting a claim. Generally, you will need to supply documentation (e.g. receipts for expenses) of your losses.

d. Your Responsibilities – In addition to following directions for your specific circumstances, you will have to adhere to the terms and conditions of our master insurance policy. These include:

   i. Promptly file a report with the police if an Incident has occurred and you reasonably believe that a violation of the law may have occurred.
   ii. Promptly notify the appropriate governmental or business entity in the event of an incident.
   iii. Take all reasonable steps to mitigate possible losses regarding the incident including requests to waive any applicable fees.
   iv. Not admit to any liability whatsoever or do so at your own expense.
   v. Cooperate with our insurer including:

      - Submitting receipts of expenses incurred and other documentation that may be requested relating to an Incident;

- Submitting a signed, sworn proof of loss, or affidavit containing information requested within sixty (60) days of the request;
- Submitting to questions under oath at such times as may be reasonably required about any matter relating to an Incident;
- Cooperating to enforce any legal rights you, us, or our insurer may have against anyone who may have liability to you;
- Providing authorization to obtain records or other information;
- Immediately sending copies of any demands, notices, summonses, or legal papers received in connection with an incident;
- Attending depositions, hearings and trials, secure and give evidence, and obtain the attendance of witnesses with regard to any legal matter relating to an incident.
- Provide sufficient evidence of lost wages including sufficient proof of the activities that necessitated the lost wages and providing any other reasonable information or documentation we may request regarding Lost Wages.
- Transfer any rights or recovery against others to our insurer or us to the extent of any payment made under the plan benefits and do everything necessary to secure these rights and do nothing after an incident to impair these rights. You may however, waive your rights of recovery in writing before an incident occurs.

Our insurer is a leading insurance company. We will work with you to submit your legitimate claims for prompt payment. If you experience any problems while working with us or our insurer to resolve your claim, you may escalate your problems by sending an email to memberservices@identityfraud.com. We will endeavor to correct any problems you may experience and/or clarify questions you may have.

Closing Remarks

Identity Fraud, Inc. is committed to providing valued solutions to you and your family. While the IFI Loss Prevention Guide & Resource Guide is a valuable tool that can help reduce your exposures to identity fraud, it represents only one aspect of our protection strategy. Together with our education, credit solutions, identity insurance and VRS Elite™ Fraud Victim Assistance, the Loss Prevention Guide supports the need to approach identity fraud protection in a comprehensive, holistic fashion.

By participating in our Identity Protection Plan(s) and renewing your membership annually, you will always have access to the most current version of our Loss Prevention Guide as well as being updated on new laws, risk management techniques and new products.

We will continually look to add products and services to our site from partners that will enable you to increase your security. By being an active member in our protection plans, you will be able to receive these products at a discount.

We value your input and encourage you to provide us with any suggestions you may have that might help us improve the services we provide to our members. If you have a suggestion or comment, please email us at memberservices@identityfraud.com.

Although no one can guarantee you complete protection against identity fraud, our mission is to significantly reduce your risks by keeping you educated on the fight against fraud and by providing you with valued products and services that reduce your chances of loss.

We thank you for your participation.

Sincerely,

Thomas A Widman

Thomas A. Widman
President

Section V – Appendix Items

Section V.A. - Identification of Accounts

Worksheet 1 should be utilized for listing all of your existing accounts and account relationships. Monitor your account activity, passwords, and keep this worksheet in a safe place away from prying eyes.

Section V.B. - Contact Sheet

We have provided many names and numbers you may need to contact if you become a victim. Also, use this sheet to record the contacts you make.

Section V.C. - Activity Log

Use the Activity Log to record the contacts you make and as a diary of when follow up activity should be pursued.

Section V.D. - Expense Records

Compiling a record of your expenses will be needed to support any claim made under the benefits provided by Identity Fraud, Inc. You should be sure to keep receipts of all expenses.

Section V.E. - Rights Under the FCRA

The Fair Credit Reporting Act is the primary legislation that governs your financial information held with the bureaus. Knowing what your rights are will allow you to monitor corrective action and make demands to the bureaus or credit grantors when clearing your records.

Section V.F. - Summary of Relevant Laws

Following the laws indicated in *Section II*, we provide a more detailed review of certain relevant laws.

Worksheet 1 – Identification of Accounts

To be amended according to your specific account relationships

Type / Firm	Account #	Password	New Password	Mail Date	Monthly	Contact
Financial						
Credit Cards						
Example: Citibank	4000-1111-2222-3333	XYZ12ab	Change 10/1	4th	$500	1-800-123-4567
1.						
2.						
3.						
ATM/Debit						
1.						
2.						
Checking						
1.						
2.						
Investment						
1.						
2.						
IRA/401k						
1.						
2.						
Money Market						
1.						
2.						
Credit Union						
Mortgage						
1.						
2.						
Auto Loan						
1.						
2.						

Type / Firm	Account #	Password	New Password	Mail Date	Monthly	Contact
Other Loans						
1.						
2.						
3.						
4.						
Insurance						
Life / Accident						
1.						
2.						
Disability						
Health						
Dental						
Home						
Auto						
Utilities						
Telephone/Fax						
1.						
2.						
3.						
Cell Phone						
PDA						
Internet						
Cable TV						
Gas/Electricity						

Water						
Garbage						
Leisure						
Health Club						
Country Club						
Other						
Subscriptions						
1.						
2.						
3.						
Associations						
1.						
2.						
3.						
Other						
1.						
2.						
3.						
4.						

As you can see, there are a variety of accounts and financial relationships that you may have. Information may be stolen or fraudulent charges may appear on your existing accounts. REMEMBER - DO NOT PAY FOR FRAUDULENT CHARGES. If your existing accounts have been accessed fraudulently, make contact with the fraud department to clear your record. You may need to take additional steps as outlined in *Section IV*. Ask your vendor what specific steps are needed to correct the error and fraud.

In addition to existing accounts, an identity thief may open up totally new accounts in your name. If so, take action quickly and review the steps outlined in *Section IV*.

Contact Sheet

Company/Gov't Agency	Division	Address	City	State	Zip	Telephone
1. Identity Fraud, Inc	Call Center					1-866-4-IDFRAUD
2. Equifax	Fraud Assistance					1-888-766-0008
3. *Equifax*	Customer Service	P.O. Box 740241	Atlanta	GA	30374	1-866-673-3740
4. Experian	Fraud Assistance					1-888-397-3742
5. *Experian*	Customer Service	P.O. Box 2002	Allen	TX	75013	1-800-493-1058
6. TransUnion	Fraud Assistance					1-800-680-7289
7. *TransUnion*	Customer Service	P.O. Box 1000	Chester	PA	19022	1-866-744-8221
8. Global Payments						1-800-638-4600
9. ChexSystems						1-800-428-9623
10. Cross Check						1-707-586-0551
11. Certegy						1-800-237-2997
12. National Processing						1-800-526-5380
13. SCAN						1-800-262-7771
14. TeleCheck						1-800-710-9898
15. Federal Trade Commission	ID Theft Clearinghouse	CRC-240	Washington	D.C.	20580	1-877-IDTHEFT
16. Social Security Administration	Data Operations Center	P.O. Box 7004	Wilkes-Barre	PA	18767	1-800-269-0271
17. Federal Bureau of Investigations	Criminal Justice Information Services	935 Pennsylvania Ave., NW	Washington	D.C	20535	1-202-324-4444
18. US Secret Service	Public Affairs	950 H Street, N.W. , Suite 8400	Washington	D.C.	20223	1-202-406-5708
19. National Fraud Information Center	Consumer Assistance	P.O. Box 65865	Washington	D.C.	20035	1-800-876-7060
20. Internal Revenue Service		1111 Constitution Ave, N.W.	Washington	D.C.	20224	1-202-927-5170
21. US Department of Justice		950 Pennsylvania Ave, N.W.	Washington	D.C.	20530	1-202-353-1555
22. Nat'l Assoc. of Attorneys General	Consumer Protection	750 First Street, N.E.	Washington	D.C.	20002	1-202-326-6000
23. Federal Government Info. Center						1-800-688-9889

IDENTITY FRAUD INC.

Contact Sheet
Con't

Company/Gov't Agency	Division	Address	City	State	Zip	Telephone
22. Direct Marketing Association	Mail Preference	P.O. Box 9008	Farmington	NY	11735	
23. Direct Marketing Association	Telephone Preference	P.O. Box 9014	Farmington	NY	11735	
24. National 'Opt-Out" Center						1-888-5-OPTOUT
25. Lexis Nexis						1-800-227-9597
26. Medical Information Bureau		P.O. Box 105, Essex Station	Boston	MA	02112	1-617-426-3660
27. California Pubic Interest Research Group (CALPIRG)		11965 Venice Blvd., #408	Los Angeles	CA	90066	1-213-251-3680
28. US PIRG		218 D Street, S.E.	Washington	D.C.	20003	1-202-546-9707
29. Consumers Union		1666 Connecticut Ave, N.W.	Washington	D.C.	20009	1-202-462-6262
30. Electronic Privacy Information Center		666 Pennsylvania Ave, S.E.	Washington	D.C.	20003	1-202-483-1140
31. Office of Privacy Protection				CA		1-800-952-5210
32. Privacy Rights Clearinghouse		1717 Kettner Avenue	San Diego	CA		1-619-298-3396
XX. Your Other Contacts						

IDENTITY FRAUD INC.

Activity Log

Date / Time	Contact Person	Company / Gov't Agency	Address	Telephone/ Fax / email	Time Spent	Expenses Incurred	Action	Follow-up Date

IDENTITY FRAUD INC.

Expense Records

Date / Time	Contact Person	Company / Gov't Agency	Type of Expense (Miscellaneous - phone, postage, travel, notaries, etc.)	Cost	Lost Wages / Time Off	Legal Costs

Appendix Section V.E.

Summary of Your Rights Under the Fair Credit Reporting Act

The Federal Fair Credit Reporting Act went into effect in 1971. The original FCRA protected your rights as a credit-active consumer by placing limits on who could see a copy of your credit report. It mandated that no one, but you, may legally review your report unless they have a legitimate business need involving the following:

- Conducting a credit transaction.
- Making an employment decision.
- Underwriting insurance.
- Conducting a legitimate business transaction.
- Reviewing an account to see whether the terms are still being met.
- Completing a business transaction initiated by the consumer.
- Determining eligibility for a governmental license or benefit.
- Assessing credit or prepayment risks in insuring, investing in or servicing an existing credit obligation.
- Responding to a court order or federal grand jury subpoena.

Anyone who knowingly and willfully obtains a credit report under false pretenses may be fined up to $5,000 and imprisoned for up to one year.

The original 1971 law was significantly amended which changes went into effect September 30, 1997. The new changes further protect consumers by giving them more control over their credit information. Currently, your rights under the FCRA include:

1. **You must be told if information in your file has been used against you.** Anyone who uses information from a Consumer Reporting Agency (CRA) to take action against you -- such as denying an application for credit, insurance, or employment -- must tell you, and give you the name, address, and phone number of the CRA that provided the consumer report.
2. **You can find out what is in your file.** At your request, a CRA must give you the information in your file, and a list of everyone who has requested it recently. There is no charge for the report if a person has taken action against you because of information supplied by the CRA, if you request the report within 60 days of receiving notice of the action. You also are entitled to one free report every twelve months upon request if you certify that (1) you are unemployed and plan to seek employment within 60 days, (2) you are on welfare, or (3) your report is inaccurate due to fraud. Otherwise, a CRA may charge you up to eight dollars.
3. **You can dispute inaccurate information with the CRA.** If you tell the CRA that your file contains inaccurate information, the CRA must investigate your claim (usually within 30 days) (unless your dispute is frivolous). The source of the disputed information must review your evidence and report its findings to the CRA. (The source also must advise national CRA's -- to which it has provided data -- of any findings that support your claim of fraud.) The CRA must give you a written report of the investigation and a copy of your report if the investigation results in any change. If the CRAs investigation does not resolve the dispute, you may add a brief statement to your file. The CRA must normally include a summary of your statement in future reports. If an item is deleted or a dispute statement is filed, you may ask that anyone who has recently received your report be notified of the change.
4. **Inaccurate information must be corrected or deleted.** A CRA must remove or correct inaccurate or unverified information from its files, usually within 30 days after you file a dispute.

5. **CRA is not required to remove accurate data from your file unless it is outdated or cannot be verified.** If your dispute results in any change to your report, the CRA cannot reinsert into your file a disputed item unless the information source verifies its accuracy and completeness. In addition, the CRA must give you a written notice telling you it has reinserted the item. The notice must include the name, address and phone number of the information source.
6. **You can dispute inaccurate items with the source of the information.** If you tell anyone -- such as a creditor who reports to a CRA -- that you dispute an item, they may not then report the information to a CRA without including a notice of your dispute. In addition, once you've notified the source of the error in writing, it may not continue to report the information if it is, in fact, an error.

In addition, employers must now obtain an applicant's written permission before obtaining a credit report. Employers, who deny employment because of something in the applicant's report, must now provide the applicant with a copy of the credit report used before making the adverse decision.

Another area granting consumers greater control is the ability to "opt out" of unsolicited credit and insurance offers. Each bureau must establish a tool-free telephone number to contact (they have established 1-888-5-OPTOUT as single number to call to effect your requests). Your name is required to be removed from marketing lists for two years and if you request permanent deletion from the marketing lists, you will need to complete a form that will allow you to have your name permanently removed.

To review the full text of the FCRA, search the Internet or go to www.ftc.gov.

Appendix Section V.F.

Summary of Relevant Laws

This section elaborates on laws indicated in *Section II*. However, the following are not organized alphabetically as in Section II. For additional information, search the Internet to review the complete laws or helpful interpretations.

THE IDENTITY THEFT ASSUMPTION AND DETERRANCE ACT (ID Theft Act)

The ID Theft Act addresses "Fraud and Related Activity in Connection with Identification Documents and Information". The Act, which became effective October 30, 1998, makes identity theft a Federal crime with penalties up to 15 years imprisonment and a maximum fine of $250,000. It establishes that the person whose identity was stolen is a *true* victim. Previously, only the credit grantors who suffered monetary losses were considered victims. This legislation enables the Secret Service, the Federal Bureau of Investigation, and other law enforcement agencies to combat this crime. It allows for the identity theft victim to seek restitution if there is a conviction. It also establishes the Federal Trade Commission as a central agency to act as a clearinghouse for complaints, (against credit reporting agencies and credit grantors) referrals, and resources for assistance for victims of identity theft.

Text from the Act includes:

CENTRALIZED COMPLAINT AND CONSUMER EDUCATION SERVICE FOR VICTIMS OF IDENTITY THEFT.

a. IN GENERAL – Not later than 1 year after the date of enactment of this Act, (October 30, 1998) the Federal Trade Commission shall establish procedures to –
    1. log and acknowledge the receipt of complaints by individuals who certify that they have a reasonable belief that 1 or more of their means of identification (as defined in section 1028 of title 18, United States Code, as amended by this Act) have been assumed, stolen, or otherwise unlawfully acquired in violation of section 1028 of title 18, United States Code, as amended by this Act:
    2. provide informational materials to individuals described in paragraph (1); and
    3. refer complaints described in paragraph (1) to appropriate entities, which may include referral to –
        A. the 3 major national consumer reporting agencies; and
        B. appropriate law enforcement agencies for potential law enforcement action.
b. AUTHORIZATION OF APPROPRIATIONS – There are authorized to be appropriated such sums as may be necessary to carry out this section.

THE USA PATRIOT ACT

The Patriot Act was passed on October 24, 2001 as a result of and following the terrorist acts on September 11, 2001. The full name of the Act is "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism", i.e. USA PATRIOT. The Act was established "To deter and punish terrorist acts in the United States and around the world, to enhance law enforcement investigatory tools, and for other purposes".

The bill changes many existing statutes and generally expands the authority of the US Government to fight terrorism. In the effort to combat terrorism, many definitions and procedures have been altered to bring criminal activity into the terrorist realm. Whether crimes fall into the terrorist realm or not, the potential of certain acts having national security implications grant authorities increased powers with acts having increased penalties.

The bill is very young and passed with exceptional speed due to pressing needs of national security. But the bill also has received considerable criticism from privacy advocates who believe the power granted to government is exceptional and misguided. Certain critical emphasis is placed on the powers of surveillance. Under the Act, surveillance (or spying) is allowed if information could be deemed relevant to an ongoing criminal investigation.

There appears to be a lack of a necessary connection between the individual being spied on and terrorist activity. The person spied on does not have to be the target of the investigation. This application must be granted and the government is not obligated to report to the court or tell the person spied upon what it has done. Privacy advocates are alarmed at the lack of checks and balances traditionally found in legislation dealing with national security. Privacy advocates feel the Act allows the government to monitor, spy, and obtain information (now legally) on every ordinary citizen and therefore represents a loss of our privacy counteracting other existing legislation that maintains checks and balances.

GRAMM-LEACH-BLILEY ACT (GLBA)

The Gramm-Leach-Bliley Act, which passed in 1999, removed barriers traditionally held between banks, investment banks, and insurance companies changing laws that have been in effect for over 60 years. It also began to address information sharing practices among financial institutions having control over non-public personal information.

Title V of the GLBA addresses financial institution information privacy practices. Subtitle A requires financial institutions to make certain disclosures regarding their privacy policies and to give certain individuals the opportunity to prevent the institution from releasing information about them to certain third parties. Subtitle B criminalizes actions by certain data collection services and other parties of obtaining personal financial information from financial institutions by misrepresenting their right to such information.

Under Subtitle A, a framework is established to protect nonpublic personal information. Two primary provisions include Section 502 and Section 503. Section 502 generally requires that a financial institution may not, directly or indirectly, or through any affiliate, disclose to a nonaffiliated third party any nonpublic personal information, unless (i) the institution has provided the consumer with a notice complying with the privacy policy requirements under section 503 and the institution discloses to a consumer that such information may be disclosed to a third party, (ii) the consumer is given the opportunity before the information is disclosed to direct that such information not be disclosed to such third party, and (iii) the consumer is given an explanation of how the consumer can exercise the nondisclosure option.

In general terms, Section 503 basically requires that at the time a customer relationship is established and at least annually thereafter during the continuation of such relationship, a financial institution must provide a notice to consumers that describes the financial institution's policies and practices with respect to (i) disclosing nonpublic information to affiliates and nonaffiliated parties, including the categories of information that may be disclosed; (ii) disclosing nonpublic personal information of persons who are no

longer customers of the financial institution, and (iii) protecting the nonpublic personal information of consumers.

The GLBA instituted important privacy protections for consumers by incorporating its 'opt out' provisions. These first steps toward giving consumers greater control over their information is being followed by various state efforts for 'opt out' legislation. In California, for example, efforts are underway that permit personal information disclosure only if the consumer first allows it. This 'opt in' places the burden on the financial institution to not disclose information verses GLBA that requires the consumer to make the effort to contact the financial institution.

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)

HIPAA provisions address a multitude of healthcare practices and issues. For the purposes of this protocol, we focus on the sections addressing privacy of information. In enacting the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Congress mandated the establishment of standards for the privacy of individually identifiable health information.

Under current laws, personal health information can be distributed - without either notice or consent - for reasons that have nothing to do with a patient's medical treatment or health care reimbursement. Patient information held by a health plan may be passed on to a lender who may then deny the patient's application for a home mortgage or a credit card - or to an employer who may use it in personnel decisions. The Privacy Rule establishes a federal floor of safeguards to protect the confidentiality of medical information. State laws that provide stronger privacy protections will continue to apply over and above the new federal privacy standards.

The Privacy Rule generally requires activities that include:

- Providing information to patients about their privacy rights and how their information can be used.
- Adopting clear privacy procedures for its practice, hospital, or plan.
- Training employees so that they understand the privacy procedures.
- Designating an individual to be responsible for seeing that the privacy procedures are adopted and followed.
- Securing patient records containing individually identifiable health information so that they are not readily available to those who do not need them.

As required by Congress in HIPAA, the Privacy Rule covers health plans, health care clearinghouses, and those health care providers who conduct certain financial and administrative transactions electronically. These electronic transactions are those for which standards are required to be adopted by the Secretary under HIPAA, such as electronic billing and fund transfers. These entities (collectively called "covered entities") are bound by the new privacy standards even if they contract with others (called "business associates") to perform some of their essential functions.

As Congress required in HIPAA, most covered entities have two full years from the date that the regulation took effect - or, until April 14, 2003 - to come into compliance with these standards. Under the law, small health plans will have three full years - or, until April 14, 2004 - to come into compliance. (http://aspe.hhs.gov/admnsimp/final/pvcguide1.htm)

COMPUTER FRAUD AND ABUSE ACT

Section 1030 of the Act addresses fraud and related activity in connection with computers. This section was also amended by the USA Patriot Act to increase the scope of abuse and severity of the penalties. The Act essentially criminalizes persons who engage in the following:

- having knowingly accessed a computer without authorization or exceeding authorized access …with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation…
- intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains-
    - information contained in a financial record of a financial institution, or of a card issuer…or contained in a file of a consumer reporting agency on a consumer…
    - information from any department or agency of the United States; or
    - information from any protected computer if the conduct involved an interstate or foreign communication;
- intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States;
- knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period;
- knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;
- intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or
- intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage;
- knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, …
- with intent to extort from any person, firm, association, educational institution, financial institution, government entity, or other legal entity, any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to cause damage to a protected computer;

The penalties for the above offenses range from fines and/or imprisonment for up to 1 year, 5 years, 10 years, and/or 20 years depending on the offense.

ELECTRONIC FUNDS TRANSFER ACT

The EFT Act was established primarily because existing consumer protection legislation was unclear when considering the use of electronic funds transfer systems. The purpose of the Act is to provide a basic framework establishing the rights, liabilities, and responsibilities of participants in electronic fund transfer systems.

Perhaps the most important areas to consider are the liabilities that consumers face when using EFT's. EFT's include ATM's, direct deposits, pay-by-phone systems, personal computer banking, and point of sale transfers. Consumer liability is based on the time you first notice and report an error or loss and is summarized as follows:

- If the loss is reported within two business days, consumer liability is limited to $50.
- If the loss is reported after 2 days but within 60 days, liability is limited to $500
- **If you fail to notify the institution of the error within 60 days, you may have little recourse. Under federal law, the institution has no obligation to conduct an investigation if you have missed the 60-day deadline. Consumer liability may be unlimited.**

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

An error also may occur in connection with a point-of-sale purchase with an EFT card. An oil company, for example, might give you an EFT card that lets you pay for gasoline purchases directly from your bank account. These purchases will be shown on your periodic statement from the bank. In case of an error on your account, however, you should contact the issuer of the card (for example, the oil company) at the address or phone number the company has provided. After you've notified the company about a point-of-sale purchase error, the company has 20 business days to investigate and tell you the results. It has up to 90 days to complete an investigation, if it returns the money to your account and notifies you promptly of the credit. If no error is found at the end of the investigation, the institution may take back the money if it sends you a written explanation. (www.ftc.gov) (http://www4.law.cornell.edu/uscode/15/1693.html)

FAIR AND ACCURATE CREDIT TRANSACTIONS ACT

The FACT Act was signed into law by President Bush on December 4, 2003 to better ensure that all citizens are treated fairly when applying for a mortgage or other type of credit. The Act also provided important provisions to help fight identity theft. One of the provisions gives every consumer the right to obtain their credit report, free of charge, every year.

Consumers may request their free credit report(s) as follows:

Request via the Internet:
www.annualcreditreport.com (Reports provided on-line)

Request via Telephone:
1-877-322-8228 (Reports provided via mail)

Request via Mail: (form required)
Annual Credit Report Request Service
P.O. Box 105281
Atlanta, GA30348-5281

Additional Information

The FACT Act is intended to help ensure that all Americans, of every income level and background, are able to build good credit and better confront the problem of identify theft by incorporating the following:

- Ensuring that lenders make decisions on loans based on full and fair credit histories, and not on discriminatory stereotypes.
- Improving the quality of credit information, and protecting consumers against identity theft by:
    - Giving every consumer the right to his or her credit report free of charge every year.
    - Helping prevent identity theft before it occurs by requiring merchants to leave all but the last five digits of a credit card number off store receipts.
    - Establishing a nationwide system of fraud alerts for consumers to place on their credit files. Credit reporting agencies that receive such alerts from customers will now be obliged to follow procedures to ensure that any future requests are by the true consumer, not an identity thief posing as the consumer. The law also will enable active duty military personnel to place special alerts on their files when they are deployed overseas.
    - Requiring credit-reporting agencies to stop reporting allegedly fraudulent account information when a consumer establishes that he or she has been the victim of identity theft.
    - Requiring creditors or businesses to provide copies of business records of fraudulent accounts or transactions related to them.
    - Allowing consumers to report accounts affected by identity theft directly to creditors - in addition to credit reporting agencies.

The FACT Act provides consumers new tools to better fight identity theft. We encourage you to obtain your free credit report each year and to understand that identity theft is serious business that will continue to evolve as thieves become more sophisticated and as thieves react to new defenses like the FACT Act.

FAIR CREDIT BILLING ACT

The Fair Credit Billing Act attempts to address errors and disputes in billing where the law applies to "open end" credit accounts, such as credit cards, and revolving charge accounts - such as department store accounts. It does not cover installment contracts - loans or extensions of credit you repay on a fixed schedule. The FCBA settlement procedures apply only to disputes about "billing errors." For example:

- unauthorized charges. Federal law limits your responsibility for unauthorized charges to $50;
- charges that list the wrong date or amount;
- charges for goods and services you didn't accept or weren't delivered as agreed;
- math errors;
- failure to post payments and other credits, such as returns;
- failure to send bills to your current address - provided the creditor receives your change of address, in writing, at least 20 days before the billing period ends; and
- charges for which you ask for an explanation or written proof of purchase along with a claimed error or request for clarification.

Disputes about the quality of goods and services are not "billing errors," so the dispute procedure does not apply. However, if you buy unsatisfactory goods or services with a credit or charge card, you can take the same legal actions against the card issuer as you can take under state law against the seller. To take advantage of this protection regarding the quality of goods or services, you must:

- have made the purchase (it must be for more than $50) in your home state or within 100 miles of your current billing address;
- make a good faith effort to resolve the dispute with the seller first.

The FCBA indicates your rights, the action steps needed to rectify your billing error, and the requirements of credit issuers in resolving the disputes. (www.ftc.gov)

FAIR DEBT COLLECTION PRACTICES ACT

Congress recognized that the collection practices of debt collectors is often abusive, deceptive, and unfair. Abusive debt collection practices contribute to the number of personal bankruptcies, to marital instability, to the loss of jobs, and to invasions of individual privacy. Because existing laws and procedures for redressing these injuries were seen as inadequate to protect consumers, it was the purpose of this title to eliminate abusive debt collection practices by debt collectors, to insure that those debt collectors who refrain from using abusive debt collection practices are not competitively disadvantaged, and to promote consistent State action to protect consumers against debt collection abuses. (www.ftc.gov)

CHILDRENS ONLINE PRIVACY PROTECTION ACT of 1998 (COPPA)

With the rise of the Internet, legislation was created to protect children's on-line activities and the information they disclose. Section 1303 of the act addresses the **REGULATION OF UNFAIR AND DECEPTIVE ACTS AND PRACTICES IN CONNECTION WITH THE COLLECTION AND USE OF PERSONAL INFORMATION FROM AND ABOUT CHILDREN ON THE INTERNET.**

Generally, it is deemed unlawful for an operator of a website or online service directed to children, or any operator that has actual knowledge that it is collecting personal information from a child, to collect personal information from a child in a manner that violates the regulations prescribed under subsection (b). Elements of the regulation include the requirement:

- to provide notice on the website of what information is collected from children by the operator, how the operator uses such information, and the operator's disclosure practices for such information; and
- to obtain verifiable parental consent for the collection, use, or disclosure of personal information from children;
- require the operator to provide, upon request of a parent under this subparagraph whose child has provided personal information to that website or online service, upon proper identification of that parent, to such parent
    - a description of the specific types of personal information collected from the child by that operator;
    - the opportunity at any time to refuse to permit the operator's further use or maintenance in retrievable form, or future online collection, of personal information from that child; and
    - notwithstanding any other provision of law, a means that is reasonable under the circumstances for the parent to obtain any personal information collected from that child;
- prohibit conditioning a child's participation in a game, the offering of a prize, or another activity on the child disclosing more personal information than is reasonably necessary to participate in such activity; and

- require the operator of such a website or online service to establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children.

A more complete description of the Act can be found at www.ftc.gov/ogc/coppa1.htm

FREEDOM OF INFORMATION ACT

The Freedom of Information Act (FOIA) establishes a presumption that records in the possession of agencies and departments of the Executive Branch of the United States government are accessible to the people. This was not always the approach to federal information disclosure policy. Before enactment of the FOIA in 1966, the burden was on the individual to establish a right to examine these government records. There were no statutory guidelines or procedures to help a person seeking information. There were no judicial remedies for those denied access.

With the passage of the FOIA, the burden of proof shifted from the individual to the government. Those seeking information are no longer required to show a need for information. Instead, the "need to know" standard has been replaced by a "right to know" doctrine. The government now has to justify the need for secrecy.

The FOIA sets standards for determining which records must be disclosed and which records can be withheld. The law also provides administrative and judicial remedies for those denied access to records. Above all, the statute requires federal agencies to provide the fullest possible disclosure of information to the public.

THE PRIVACY ACT OF 1974

The Privacy Act of 1974 is a companion to the FOIA. The Privacy Act regulates federal government agency record keeping and disclosure practices. The Act allows most individuals to seek access to federal agency records about themselves. The Act requires that personal information in agency files be accurate, complete, relevant, and timely. The subject of a record may challenge the accuracy of information. The Act requires that agencies obtain information directly from the subject of the record and that information gathered for one purpose not be used for another purpose. As with the FOIA, the Privacy Act provides civil remedies for individuals whose rights have been violated.

Another important feature of the Privacy Act is the requirement that each federal agency publish a description of each system of records maintained by the agency that contains personal information. This prevents agencies from keeping secret records.

The Privacy Act also restricts the disclosure of personally identifiable information by federal agencies. Together with the FOIA, the Privacy Act permits disclosure of most personal files to the individual who is the subject of the files. The two laws restrict disclosure of personal information to others when disclosure would violate privacy interests.

While both the FOIA and the Privacy Act support the disclosure of agency records, both laws also recognize the legitimate need to restrict disclosure of some information. For example, agencies may withhold information properly classified in the interest of national defense or foreign policy, trade secrets, and criminal investigatory files. Other specifically defined categories of confidential information may also be withheld.

The essential feature of both laws is that they make federal agencies accountable for information disclosure policies and practices. While neither law grants an absolute right to examine government documents, both laws establish the right to request records and to receive a response to the request. If a record cannot be released, the requester is entitled to be told the reason for the denial. The requester also has a right to appeal the denial and, if necessary, to challenge it in court.

These procedural rights granted by the FOIA and the Privacy Act make the laws valuable and workable. As a result, the disclosure of federal government information cannot be controlled by arbitrary or unreviewable actions. (http://www.ftc.gov/foia/privacy_act.shtm)

END