IDENTITY THEFT & RELATED CONSUMER RIGHTS:
An Overview of the Issue, Responses and Resources

Originally compiled by Jack H. (Nick) McCall Jr. (2003)
Updated and revised by Norman G. Templeton (2004)
Updated and revised by Charles E. Young Jr. (2005-06)
Updated and revised by Kate E. Tucker (2007-08)

***Introductory Note**: This article provides a summary of various issues relating to identity theft. It is intended to be purely informational in nature and to provide an overview of the issues regarding identity theft; it does not constitute legal advice regarding any specific situations, nor does it necessarily cover all legal and practical aspects of identity theft. Please contact a lawyer for legal advice regarding any specific set of facts or circumstances.*

I. IDENTITY THEFT: THE BASICS

What is identity theft, and what's happening with it?

A pervasive new crime, "identity theft," is occurring with greater frequency, in part because of certain aspects of the Information Age. Think about all of the things we take care of online: shopping, making travel plans, paying bills, banking, filling prescriptions, personal emailing, business emailing, making appointments, applying for insurance or loans, etc. We put so much information "out there" that it would be naïve for us to think that all of it is safe. The problem has become so pervasive that we now have National Consumer Protection week dedicated to informing the public about what identity theft is, how to prevent it from occurring, and how to deal with the consequences if it does occur. This article addresses those issues.

Identity theft occurs when someone uses another person's personal information (such as a name, Social Security number, credit card number or bank account number) to engage in theft, conceal crimes, or obtain credit fraudulently. It can even be used to obtain illegal entry to, or employment in, the United States. Identity theft is a crime, and it can be a costly and devastating crime for its victims as well as for the credit grantors who are defrauded. Identity theft can, among other harms, mar a person's credit history and jeopardize a solid credit rating or result, if unchecked, in a denial of credit. Further, it can affect a person's federal tax history and Social Security earnings, if others use the stolen information for false employment or tax data.

Here are some of the most common ways that identity thieves can cause you serious trouble and inconvenience:

- The identity thieves open a new credit card account, using your name, date of birth, and Social Security number. When they use the credit card and don't pay the bills, the delinquent account appears on your credit report.

- The identity thief can call your credit card issuer and, pretending to be you, change the mailing address on your credit card account. Then, the identity thief runs up charges on your account. Because the bills are going to the new address and not to *your* address, you may not immediately realize you have a problem until after the thief has charged large amounts on your credit card.

- They may establish cellular phone service in your name and not pay for it.

- They could open a bank account in your name and write bad checks on it.

- In some cases, thieves have used Social Security numbers to help others fraudulently obtain jobs or new employment. They may also be used to forge immigration and travel documents. This can create confusion with your IRS tax records and Social Security Administration files, as your files might reflect earnings you have not received or jobs you have not held.

Many people attribute the rise in identity theft to the advent of the Internet, but that's something of a misconception. Studies have shown that only slightly more than 10 percent of the theft happens online; rather, the majority of identity theft occurs when someone steals your mail, checkbook, or wallet. Other ways thieves work include dumpster diving; facilitating inside jobs with temporaries, interns, and workers in your home or office (cleaning services, child-sitters, etc.); mailbox theft; and even false address changes at the Post Office.

Of course, none of those mundane means of identity theft has the media sizzle of widespread data security incidents involving millions of individuals at institutions like ChoicePoint, Bank of America, Marriott, CitiFinancial, Card System Solutions, and DSW Shoe Warehouse. The idea that someone has hacked into a company's computers and downloaded thousands of individuals' personal data is more sinister and cinematic than the vision of a drifter finding your wallet or stealing your mail.

But while those high-profile incidents are troubling, they ultimately will affect far fewer people than garden variety, everyday theft. For example, in 2006, ChoicePoint paid $5 million to the Federal Trade Commission ("FTC") and consumers for selling records of at least 163,000 individuals to a ring of identity thieves. But only 800 affected people actually suffered identity theft. On the other hand, we do still come across the large-scale data breach cases that cause the media stirs, such as the lawsuit against Certegy Check services, Inc. in 2007. The class action lawsuit was filed by 8.5 million people whose personal data was illegally accessed and sold by a former Certegy employee. Certegy offered to settle the matter earlier this year for up to $4 million. The court has not yet approved the settlement. Critics say the figure will be far too little given the number of potential victims. As part of the settlement, Certegy will also offer the victims credit monitoring services for one year.

An incident involving Providence Health System in Portland, Oregon, in late 2005 shows that old-school theft is still critical: 365,000 unencrypted patient records

were stolen from an employee's car, and the health-care provider notified affected patients and employees on its own. Providence became the subject of a nine (9) month investigation by the Oregon State Attorney General into whether it violated consumer protection laws by failing to take reasonable measures to protect medical records, and a patient filed a class action complaint alleging that Providence was negligent in failing to safeguard his health information. A settlement agreement was filed in September 2006.

There are conflicting reports regarding whether the crime of identity theft is increasing or decreasing. The Better Business Bureau reported approximately 9 million cases of identity theft in the United States last year; the Federal Trade Commission reported 9.9 million cases. According to the Federal Trade Commission, almost 4000 cases of identity theft were reported in Tennessee in 2007, up from 3500 in 2006. An additional 10,000 cases of consumer fraud were reported in Tennessee in 2007.

In contrast, the 2007 Identity Fraud Survey Report released by Javelin Strategy & Research reports a decline in identity theft of approximately 12% from the prior year. This translates to a fraud reduction of approximately $6.4 billion. The report cites various factors that have contributed to the decline including better consumer education and awareness, increased precautions taken by consumers, and increased usage of online banking enabling consumers to monitor their accounts. According to the survey, young adults are at the highest risk for identity theft because they are less likely to take routine safeguards such as shredding documents or regularly checking their bank accounts or credit reports.

The Better Business Bureau agrees that, generally, the Internet helps in reducing identity theft. Monitoring your checkbook and credit card status online is a huge deterrent to identity theft because people find problems quickly and can report them right away. And some companies, like E-Trade, are now offering free fraud protection to ease concerns. Sophisticated companies understand and appreciate that their customers want to feel secure when they do business, whether it's in person or online.

MasterCard and Visa USA officials have begun development of an independent standards-setting organization to certify that member banks and merchants meet minimum data security requirements. The entities set and monitor standards for the entire payment card industry. This not only improves security in that industry, but it has the indirect effect of contributing to the developing "standard of care" for data protection across industry sectors. The major credit card companies are instituting incentive programs to entice merchants to comply with the Payment Card Industry Data Security Standards (PCI-DSS) and other internal security programs.

Is identity theft a crime, and what laws apply to it?

Yes. The Identity Theft and Assumption Deterrence Act, enacted by Congress in October 1998, is the federal law making it a federal crime when someone "knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a

violation of federal law, or that constitutes a felony under any applicable state or local law." Under this law, a name or Social Security number is considered a "means of identification." So is a credit card number, cellular telephone electronic serial number, or any other piece of information that may be used alone or in conjunction with other information to identify a specific individual.

Violations of this law are investigated by various federal law enforcement agencies, and federal identity theft cases are prosecuted by the U.S. Department of Justice. In most instances, a conviction for identity theft carries a maximum penalty of fifteen (15) years imprisonment, a potential fine, and forfeiture of any personal property used or intended to be used to commit the crime. Schemes to commit identity theft or fraud also may involve violations of other federal laws, such as credit card fraud, computer fraud, mail fraud, wire fraud, immigration fraud, financial institution (i.e., bank) fraud, or Social Security fraud. Each of these federal offenses is a felony and carries substantial penalties – in some cases, as high as 30 years in prison as well as fines and criminal forfeiture.

Congress is also considering new laws to fight "phishing" attacks, a form of online fraud in which Internet users are tricked into providing financial account data and passwords to phony websites run by fraudsters. If you have received an e-mail that appears to have come from your bank, complete with trademarks and generally appropriate sounding language that ultimately requests your personal information, someone has tried to "phish" in your pond.

Lawmakers want to create new criminal sanctions and stricter penalties for those who send fake e-mails or use phony websites in these phishing scams. The Anti-Phishing Act of 2005, introduced by Sen. Patrick Leahy (D-VT) makes it a felony to use a computer to gather personally identifying information "through the use of material artifice, trickery or deception." One limitation of the Act is that it only covers phishing attacks within the United States; however, phishing is an international crime, making it difficult to stop.

Along those same lines, a couple of pieces of legislation have been introduced in the House of Representatives recently. The legislation is designed to protect internet users from the unknowing transmission of their personally identifiable information through spyware programs. And bills with slightly more specific language than the Virginia measure have been introduced in Arizona, New Mexico, and Washington. These bills would make it a felony to falsely represent a business or organization in an e-mail or website in order to obtain personally identifying information from an individual.

Many states have also passed laws related to identity theft. Tennessee's law making it a crime is found at Tennessee Code Annotated Section 39-14-150, which states that:

(a) A person commits identity theft who knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or

otherwise promote, carry on, or facilitate any unlawful activity.

(b) As used in this section, "means of identification" means any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including:

(1) Name, social security number, date of birth, official state or government issued driver license or identification number, alien registration number, passport number, employer or taxpayer identification number;

(2) Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;

(3) Unique electronic identification number, address, routing code or other personal identifying data which enables an individual to obtain merchandise or service or to otherwise financially encumber the legitimate possessor of the identifying data; or

(4) Telecommunication identifying information or access device.

(c) A violation of this section is a Class D felony.

Tennessee also has a statute that prohibits "criminal impersonation." This statute, found at Tennessee Code Annotated Section 39-16-301, states that:

(a) A person commits criminal impersonation who, with intent to injure or defraud another person:

(1) Assumes a false identity;

(2) Pretends to be a representative of some person or organization;

(3) Pretends to be an officer or employee of the government; or

(4) Pretends to have a handicap or disability.

(b) Criminal impersonation is a Class B misdemeanor; provided, that, upon conviction under subsection (a), the maximum fine of Five Hundred Dollars ($500) for such offense shall be imposed if the criminal impersonation was committed in order to falsely obtain a drivers license or other photo identification license.

In addition, Tennessee has the Tennessee Identity Theft Deterrence Act of 1999, Tenn. Code Ann. §§ 47-18-2101 to 47-18-2107, a civil law enforceable by private lawsuits. Echoing the criminal law, it prohibits directly or indirectly "obtaining, possessing, transferring, using or attempting to obtain, possess, transfer or use, for unlawful economic benefit, one or more" identification documents, financial documents,

or personal identification numbers of another person. If someone violates the criminal law, they probably violate this as well, and it would give a victim a chance to sue the perpetrator in court for damages. You could recover as one component of a damage award the greater of $10,000; $5,000 ***per day*** for each day that your identity has been assumed; or 10 times the amount obtained or attempted to be obtained by the thief.

You could ***also*** recover restitution for your actual losses, interest, and penalties under the Tennessee Consumer Protection Act ("TCPA"), which provides for triple damages; and your attorneys. fees and costs. The TCPA was enacted to protect consumers from those who engage in unfair or deceptive acts or practices in the conduct of any trade or commerce within Tennessee. Tenn. Code Ann. § 47-18-102(2). In the context of identity theft, this statute becomes more relevant when it is a business that has stolen a consumer's identity. In 2007, a Chancellor in Williamson County, Tennessee ordered two businesses, National Fulfillment, Inc. and Entertainment America, Inc. to place $300,000 in an escrow account pending the outcome of a trial. The lawsuit includes allegations that the businesses violated the Tennessee Identity Theft law and the TCPA when they billed consumers' credit cards for a product that never existed. As discussed previously, identity theft occurs not only when someone improperly uses your name or Social Security number, but also when they improperly use your financial information such as a credit card or bank account.

The Tennessee Legislature has passed some other laws to address related aspects of identity theft. One such law provides that your driver's license can no longer display your social security number unless you specifically request in writing that the number be displayed. Tenn. Code Ann. § 55-50-331(b)(2). As discussed elsewhere herein, you should not allow your Social Security number to appear on your license, and if it is there you should get it removed immediately, or at least when you renew.

In 2005, the legislature prohibited persons who accept credit cards or debit cards for business to print or cause to be printed more than five digits of the card number or the expiration date on either the receipt retained by the merchant or the receipt provided to the cardholder at the point of the sale or transaction. This law immediately applied to any cash register or other machine or device that electronically prints receipts for credit card or debit card transactions if the machine first went into use on or after January 1, 2005. Effective January 1, 2007, the bill applies to cash registers or other machines or devices that were in use before January 1, 2005. The law does not, however, apply to transactions in which the sole means of recording a credit card or debit card account number is by handwriting or by an imprint or copy of the card -- the "mom and pop" store exception. A violation constitutes an unfair and deceptive trade practice under the TCPA. Tenn. Code Ann. § 47-18-126.

Congress and several states are also considering ***data security*** as well, in an effort to force holders of data to handle it more carefully, protect it more vigorously, and notify consumers promptly of any breaches. According to Privacy Rights Clearinghouse, over one-third of Americans have had their personal information compromised and it is estimated that more than 94 million personal records were exposed in security breaches

between February 2005 and now. Congress is considering several new bills that would further enhance data security, require notice of security breaches and enhance criminal penalties, law enforcement assistance and other protections. In addition, companies are utilizing new technologies, such as data encryption and installation of central management systems, in order to better safeguard their sensitive data.

Tennessee passed a law in 2005 that added data security provisions to the Tennessee Identity Theft Deterrence Act of 1999. In sum, if someone holds or licenses computerized data that includes personal information in Tennessee, they have an affirmative obligation to report any breaches of their data security "to any resident of Tennessee whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person" and to do so "in the most expedient time possible and without unreasonable delay." If more than 1,000 people are affected, then notification must go to credit bureaus as well. Tenn. Code Ann. § 47-18-2107.

Most recently, Tennessee enacted the Credit Security Act of 2007, which went into effect on January 1, 2008. The Act allows consumers to put a freeze on their credit report and remove their Social Security number as a form of identification. Consumers can apply for the freeze by mail beginning September 1, 2008 or by electronic sign-up beginning January 31, 2009. There is a one-time set up fee of $7.50 for each of the three major credit bureaus the consumer places a security freeze with. The freeze can be temporarily lifted if the consumer wishes to make a major purchase requiring a credit check. The Social Security number protections began on January 1, 2008; and beginning in January 2009, violation of the provisions will be a Class B misdemeanor. The Act also provides additional protections for consumers and businesses when there has been a breach of data information. Note: TennCare contractors will be exempt from the Social Security number protection provisions because some of their practices in this area cannot be changed at the present time; this includes printing Social Security numbers on pharmacy cards.

What can you do to prevent identity theft?

There are several safeguards you can take to protect your personal information and decrease the chances that you will become a victim of identity theft. The following are some helpful hints for keeping your personal information from being stolen:

- In general, provide your personal information only when you receive an appropriate benefit in return for the disclosure. If you disclose personal data, consider using a post office box or business address and a business phone number. If you provide your residential address and phone number, ask how it will be used and how you can restrict any further use. You don't have to give every piece of information that you are asked for – only provide what is needed for the transaction.

- More specifically, on your checks do not use your home address and telephone number. Instead, use a post office box if you have one; if not, use your business

address and phone number. Never have your Social Security Number printed on your checks. You can handwrite it on your checks when necessary, but if you have it printed on them, then anyone can get it.

- Carefully check your bank statements, credit card statements and other financial statements regularly. If a statement does not arrive on time, notify the bank, credit card company or other financial provider that it has not arrived. A missing bill could indicate that someone has taken over your account and changed the address to his own.

- Request your free annual credit report (discussed in more detail in subsequent sections) to see if there are any debts that you do not recognize. If there is a debt you do not recognize, notify the creditor ***immediately*** to dispute the charge. Remember that errors on your credit report are not uncommon and do not automatically indicate that your identity has been stolen. A study released by the U.S. Public Interest Research Group in June 2004 found that 79% of the consumer credit reports surveyed contained some kind of mistake.

- Discard documents containing personal information by shredding them and until you discard them, keep such documents in a secure location.

- Put your vehicle registration in your trunk instead of your glove compartment. Car thieves now use the registration information to steal identities, and even if all you do is slow them down, that has some value.

- The next time you order checks, have only your initials (instead of first name) and last name put on them. That way, if your checkbook is stolen (or lost), others will not know if you sign your checks with just your initials or your first name, but you and your bank will know how you sign your checks. That will make fraudulent checks easier to spot. Also, consider arranging to pick your checks up at the bank, rather than have them mailed to your home address.

- When writing checks to pay your credit card accounts, do not put the complete account number on the "For" line of your checks. Instead, just put the last four (4) numbers. The credit card company knows the rest of your account (card) number, and anyone who might be handling your check as it passes through all of the check processing channels will not have access to it.

- Be aware of those around you in checkout lines when paying by check or credit card. Cellular phones with built-in cameras make it easy for someone to photograph your checks or credit cards and obtain your account numbers.

- Consider abandoning your "debit cards," or Visa and MasterCard clones that draw from your checking account. Typically, it is much more difficult to get a thief's charges resolved on these accounts than it is with a real credit card. Credit cards tend to offer more consumer protection and less consumer liability. For ATM

cards, if you report the identity theft within two days, you're only responsible for $50; wait longer, however, and your liability continues to increase. Most credit cards, on the other hand, have a "zero liability" policy.

- Do not disclose your e-mail address to commercial sites unless you are familiar with the site's privacy and use policies (which are required to be posted and available), how your e-mail address will be used and with whom the e-mail address with be shared. If a site requires an e-mail address merely to browse it, use *yourname*@privacy.net. If you want to access a website or other online forum that requires you to complete a registration form or give an e-mail address, consider using www.bugmenot.com to get a free password you can use instead. This website allows you to type in the address of the site you want to read (for example, the Knoxville News Sentinel site) and then it will give you a user ID and a password. Occasionally these do not work, but more often than not they do. It's also wise to have multiple e-mail addresses and to select one or two of them – ***not*** ones you use at work or for important or personal communications – these purposes. A good idea is to get a free G-mail or Hotmail address and use that for completing online registrations; you can also use sites such as www.mailinator.com and www.spamgourmet.com to obtain "dummy" or "disposable" e-mail addresses.

- Have a "non-published" residential telephone number – that is, one which is neither available in the printed directory nor from directory assistance – or a "non-listed" number that is not printed in the directory but available from directory assistance. (CD-ROMs containing nationwide listings of telephone directories are now readily and cheaply available from computer and discount stores. Nationwide telephone directories are also available on the Internet, and there is no charge for Internet users to search these directories.) If your address and phone number are in a directory, they are widely available. If your address is included in a local directory, it will also be in the nationwide directories.

- Do not complete street directory information forms (e.g., a request to complete street address information for a commercially published directory other than a telephone book). These directories include alumni directories, church directories, employer directories, etc.

- Avoid ordering products or services by telephone from companies if you don't know their data sharing practices. If you do, inform the merchant that you do not want your name, address and telephone number given to others. (Not only do the national catalog retailers "capture" and store your personal information, but many local retailers such as pizza delivery services capture your phone number and generally have your name and address displayed on their computer screen merely to be confirmed by you when you contact them to order their products.) You can also use "Caller ID" blocking services that are widely available from the phone companies to prevent your phone number from being displayed when you order products or services over the phone.

- Avoid completing product warranty or registration cards, consumer surveys, contest entries, preferred buyer promotions and the like. Also avoid using preferred shopper, store discount or check cashing cards. These cards generally permit the retailer to compile lifestyle information – number, ages and sex of people in the household, income level, and similar information, which is then used to compile targeted mailing lists, which are sold for marketing purposes. (However, *do* complete registration cards for products such as infant car seats or other products where it is very important for safety or health reasons that the manufacturer be able to contact you in the event of a product recall. If you have concerns about the company's privacy practices, please contact the company directly for more information.)

- Keep your computer's internal defenses up-to-date. Install all operating system patches as soon as you can, or better yet set up your computer to install them automatically when they are issued. Invest in a solid anti-virus program that updates itself automatically. Use a basic firewall. If your ISP (AOL, Earthlink, etc.) offers security software, accept it but consider supplementing it. Also, consider using a web browser other than Microsoft Internet Explorer, which is the most common avenue for hackers to exploit since it's the most popular browser. There are simple and free ways to tweak various web browsers to help prevent hidden code on web pages from invading your computer, and you can find them at http://www.cert.org/tech_tips/securing_browser/.

- Most importantly, understand the business practices of companies you patronize and only do business with companies that offer you appropriate choices with regard to your information. For example, limit your mail order shopping to companies who pledge not to resell your name and address to other companies. Complete credit applications and promotion entry forms only if the application has an "opt out" box for marketing information. If you're not sure whether a company will respect your wishes, either don't provide the information requested or provide non-personal data such as a business phone number instead of your home phone number – better yet, ask and shop elsewhere if you're not comfortable with the answer.

- Internet shopping has almost become standard practice for many of us. Pay for your order using a credit card; as discussed previously, it provides the most protection against identity theft. When providing credit card information over the internet, be aware of the site's security measures. Many web sites use Secure Sockets Layer (SSL) technology to encrypt your credit card information. They usually tell you they use this technology; however, you can check by making sure the address asking for your information begins with "https" instead of just "http." Another technology that ensures a secure connection is Secure Electronic Transaction (SET). Print all terms and conditions, receipts and confirmations. Read the privacy policy to find out what information the seller is gathering, how it

is to be used and how you can stop the process. Do not use the same password for ordering as you did to log into your computer.

- Finally, place the contents of your wallet or purse/billfold on a photocopy machine and copy both sides of each license, credit card, etc. Give the copy to a family member or friend, or store it in a safe place. That way, if your wallet is ever lost or stolen, you will know what you had in your wallet or purse/billfold, and all of the account numbers and phone numbers so that you can call and cancel those accounts and get replacements. It is also a great idea to carry a copy of your passport with you when you travel abroad, and to leave another copy with a family member or trusted friend while you are gone in case you have to get a replacement.

Protecting Your Social Security Number

Although many people think that their Social Security numbers are private, this is not true. Social Security numbers are, in fact, fairly readily available from many different sources. For example, Social Security numbers are often contained in public records, such as death certificates, driving records, court pleadings, and bankruptcy and lien filings and, as such, can be located by many persons. Additionally, Social Security numbers are widely available from credit reporting agencies and other professional information collectors and private investigators to qualified commercial, professional, and government users who use the numbers to check people's identities and to manage fraud risks.

To help protect yourself from fraud, never use your Social Security number as your "unique" identifying number unless you are required to so by law. For example, you will be required to provide your Social Security number for banking and tax purposes. You can legally refuse to provide your Social Security number to private businesses unless it is required for governmental purposes, such as tax withholding. However, some businesses, such as utilities, may require another form of identification or even a deposit if you do not give them your Social Security number and some businesses may refuse to extend credit unless you provide your Social Security number.

To prevent widespread disclosure of your Social Security number, *never* include it on your pre-printed checks or business cards. Similarly, do not use your Social Security number as your driver's license number or as a student identification number. In general, do not permit others to use your Social Security number for identification purposes. Instead, ask businesses to use a made-up number or pass code if they need to confirm your identity.

Often, an identity theft victim's first inclination is to try to get a new Social Security number if the victim's old one is stolen. For the following reasons, this may not necessarily be the best option.

- The vulnerability of the newly issued number is not significantly different from the compromised number, unless you scrupulously protect it. Seeking and receiving a new Social Security number provides no guarantee that the problems associated with the stolen number will be remedied any faster, if at all.

- In many cases, this may only lead to greater confusion. Your original number will remain assigned to you and linked through SSA computer systems to the new number. The new number will be cross-referenced to the old number for integrity reasons and so that earnings can be properly credited. The SSA does not void, delete or cancel Social Security numbers. When the SSA determines that the same number was accidentally assigned to two (2) different people and assigns a new number to one of these individuals, the numbers are not cross-referenced.

- A new Social Security number may not resolve the individual's problems because the SSA does not have the authority to control the use of Social Security numbers by other agencies, organizations and credit bureaus. These organizations (for instance, the IRS, Medicare/Medicaid, the military, the Veterans Administration, etc.) will have records and files organized under the original number. The SSA is neither responsible for, nor can the SSA control, how these organizations use your original Social Security number.

- Credit bureaus use the Social Security number in conjunction with other information (for example, the individual's name, year of birth, addresses, and spouse's name) to identify a record. When the individual uses a new number, he or she is not guaranteed a "fresh start," particularly if the other identifying pieces of information remain the same. Hence, getting a new Social Security number is no way for a person to try to hide from a poor credit history. A credit bureau may combine the credit records from the old Social Security number with those from the new number.

- In the case of identity theft, getting and using a new Social Security number may actually create a host of other, new problems. Even when the old credit information is not associated with the new number, the absence of any credit history under the new number actually may make it *more* difficult for an individual to get credit, continue college, rent an apartment, buy a big-ticket item like a car or home, open a bank account, get health insurance or get a job.

- Inquiries on a credit record do not always mean someone has used the victim's Social Security number or applied for credit. Up to 1/3 of all credit reports contain misinformation not attributed to identity theft. When misinformation or an apparent fraudulent account appears on an individual's credit record, that does not always mean that someone else misused that individual's number. Some credit bureau records are incorrect because of errors either caused by the reporting company when providing the information or by the credit bureau when adding the information (for instance, a Social Security number was incorrectly keyed or the records of two (2) individuals with similar names were combined).

If you can prove that you're harmed or being taken advantage of because someone has wrongfully used your Social Security number, and if you believe that getting a new Social Security number is absolutely essential, visit your local Social Security Administration office to request a new one. You can contact the local Social Security Office for Knox County at 8530 Kingston Pike, Knoxville, Tennessee 37919, phone: 865-692-0196, or toll-free: 1-800-772-1213.

If you've done all you can to fix the problem and someone is still using your number, under certain circumstances, the Social Security Administration may assign you a new number. However, the Social Security Administration will not assign you a new Social Security number if it believes that you:

- Intend to avoid the law or your legal responsibilities;
- Commit fraud or another crime;
- Intend to avoid or hide from a poor credit record or a criminal record;
- Have filed for bankruptcy; or
- Have lost your Social Security card or it was stolen, but there is no evidence that your number is being used by someone and that you're being harmed in some way by that use.

II. RESPONDING TO IDENTITY THEFT

What can you do to fight the effects of identity theft?

If you believe that you have been the victim of identity theft, you should take several important steps:

- First, immediately report the crime to the local law enforcement agency in the jurisdiction where the crime occurred and get a police report. You will need to send copies of the police report to the credit grantors and potentially to federal or state agencies. None of those entities will act without the police report.

- Next, contact the three main credit reporting agencies to get copies of your credit report – fraud victims are entitled to free copies over and above any other free copies you may have already obtained or received – and ask about the agencies. fraud alert services. The three main agencies are Experian, Equifax and TransUnion; contact information is provided below.

- Inform the credit grantors who have extended credit to the thief in writing about the situation and enclose copies of the police report.

- Contact the Social Security Administration if someone is using your Social Security number.

- Contact your bank and credit card companies if someone is using your bank account, checking account or credit card numbers.

- DOCUMENT EVERYTHING IN WRITING, and keep copies of the documents for at least ten (10) years, if not forever. You may solve ninety percent of the problem, but that last ten percent could keep cropping up, and you may need to be able to demonstrate the efforts you've made to correct things.

In addition, the Federal Trade Commission and the Tennessee Division of Consumer Affairs have some helpful resources regarding identity theft. You can find these resources by going to:

www.consumer.gov/idtheft
www.onguardonline.gov.
www.ftc.gov/bcp/edu/microsites/idtheft
www.state.tn.us/consumer

Here's how to contact the three (3) nationwide credit bureaus to notify them of the identity theft and obtain a copy of your credit reports:

Experian (formerly TRW): Dialing **1-888-397-3742** will connect you to a recording that has instructions for requesting copies of credit reports if you have been denied credit, employment or insurance. Requesting Consumer Assistance will connect you to a representative who can assist with more specific requests. You can also contact Experian via the Internet at **www.experian.com**, or you can write to P.O. Box 2002, Allen, TX 75013. However, the company seems to prefer handling identity theft issues by telephone.

Equifax: Dialing **1-800-685-1111** connects you to a recording that addresses requests for copies of your credit report, fraud incidents and what to do if you disagree with information on the report. You can also contact Equifax via the Internet at **www.equifax.com**, or write to Equifax Information Services, LLC, Disclosure Department at P.O. Box 740241, Atlanta, GA 30374. (With Equifax, be sure you ask for the phrase "fraud alert" to be placed at the top of your credit report.)

TransUnion: Calling Consumer Relations at **1-877-322-8228** connects you to a recording that addresses requests for copies of your credit report, and you may ask to speak to a representative. You can also contact Trans Union via the Internet at **www.transunion.com**. You can contact the TransUnion Fraud Victims Assistance Department at **1-800-680-7289**, or at P.O. Box 6790, Fullerton, California 92834.

What laws protect victims of identity theft?

The Fair Credit Reporting Act ("FCRA"), 15 U.S.C. § 1681, et. seq. is a federal law that regulates the collection, dissemination, and use of consumer credit information. Consumer Reporting Agencies ("CRAs") collect and disseminate information about

consumers to be compiled into a consumer's credit report and used for credit evaluation. CRAs have a number of responsibilities under FCRA, including the following:

- Provide a consumer with information about him or her in the agency's files and to take steps to verify the accuracy of information disputed by a consumer.
- If negative information is removed as a result of a consumer's dispute, it may not be reinserted without notifying the consumer within five (5) days, in writing.
- CRAs may not retain negative information for an excessive period of time. The FCRA spells out how long negative information, such as late payments, bankruptcies, tax liens or judgments may stay on a consumer's credit report - typically seven (7) years from the date of the delinquency. The exceptions: bankruptcies (10 years) and tax liens (7 years from the time they are paid).

An information furnisher, as defined by the FCRA, is a company that provides information to CRAs. Typically, these are creditors (credit card companies, mortgage banking institutions, etc.) with which a consumer has some sort of credit agreement. Information furnishers can also be collection agencies or courts reporting a judgment. Under the FCRA, these information furnishers may only report to a consumer's credit report under the following guidelines:

- They must provide complete and accurate information to CRAs.
- They have a duty to investigate disputed information from consumers.
- They must inform consumers about negative information which has been or is about to be placed on a consumer's credit report within 30 days.

Another law that identity theft victims can invoke is the Fair and Accurate Credit Transactions Act ("FACTA"), which was signed into law in December 2003 and which added certain significant provisions to the FCRA. FACTA was enacted to prevent identity theft, control the consequences of identity theft to victims. credit records, and help victims cleanse their credit records of identity-theft related information. FACTA also added provisions to enhance the accuracy and integrity of information reported to credit bureaus by businesses (furnishers). The FCRA, as amended by FACTA, establishes a communication link among consumers, agencies (credit bureaus) and furnishers (businesses who furnish consumer credit information to credit bureaus) which, if properly implemented, could synchronize consumer reports and purge theft-related information from agencies' and furnishers' files.

Fraud Alerts

- *Adding fraud alerts to consumers' files.* FACTA adds a new section to the FCRA which provides for two (2) varieties of fraud alerts that consumers may add to their files with nationwide credit bureaus. New Section 605A provides for "one call" fraud alerts that allow consumers who believe that they are or might be victimized by fraud or identity theft, to add a fraud alert to their files with the credit bureaus. The credit bureau must refer the alert to the other credit bureaus, and all of the bureaus must not only include the alert in the consumer's file, they

must also provide the alert each time they generate that consumer's credit score. The bureau must also notify the consumer of the right to a free credit report and must provide a requested report within three (3) business days of the consumer's request.

- *Limited time period for alerts.* But be warned: this type of fraud alert stays active only for ninety (90) days. To obtain an extended alert that lasts for seven (7) years, a consumer must provide the bureau with an identity theft report. The Federal Trade Commission must still define an "identity theft report" through the issuance of regulations, but under the Act, the report must at least include: (1) allegations of identity theft; and (2) a copy of an official, valid report filed by a consumer with a federal, state or local law enforcement agency. Further, the consumer will be subject to criminal penalties if the information is false.

- *Notification of the right to free credit reports.* For extended fraud alerts, the credit bureau must notify the consumer of the consumer's right to two (2) free credit reports within twelve (12) months of the request, and must provide the consumer's file to the consumer within three (3) business days of the consumer's request.

- *Additional alert for active military personnel.* Section 605A also allows consumers on active military duty to add an alert of their status to their files. Consumers on active duty include reservists who are on active duty, other than at their usual station. Once a military consumer requests the active duty alert, it will become part of his/her credit report for a twelve (12) month period. The intent of this type of alert is to deter identity theft from military personnel who are stationed away from old addresses. If you have a family member or friend about to go abroad in the military, urge them to use this to freeze their credit files before they depart.

- *Limits on credit transactions.* Under these alerts, users of credit reporting information may not proceed with a credit transaction unless the user "utilizes reasonable policies and procedures to form a reasonable belief that the user knows the identity of the person making the request." If the alert is an extended fraud alert, then the consumer may provide a telephone number in the alert that the user must use to verify the requester's identity, or the consumer may designate another reasonable method of contact.

Some consumer advocates have urged that customers ought to be able to direct companies to freeze their credit reports more easily than this. They point out that companies granting credit would benefit in the long run because of reduced write-offs. Credit-extenders respond that they fear an economic downturn from reduced sales because of needlessly frozen credit. Many states are legislating this now, although Tennessee has yet to act on it.

In addition to its fraud alert provisions, FACTA also added other provisions designed to assist with identity theft prevention, credit history restoration and information accuracy. Some of those provisions are:

Identity Theft Prevention

- *Creditors to implement red-flag guidelines and regulations.* The FTC, the National Credit Union Administration, and specified banking agencies to issue regulations that will require financial institutions and creditors to "establish reasonable policies and procedures" for implementing to-be-issued "red flag" guidelines regarding identity theft. A more concrete provision calls for regulations to prevent "account-takeover" identity theft by imposing special verification procedures when a card issuer receives a notification of a change of address from a cardholder and subsequently receives a request for an additional or replacement card.

- *Businesses must provide identity theft victims with business transaction information.* The revised FCRA gives requires businesses who have dealt with an identity thief to provide information about the transactions to the thief's victim and to law enforcement agencies. However, the provision imposes prerequisites that a victim must meet and allows a business to decline to provide the information if the business determines "in the exercise of good faith" that any of the following exceptions exists: the business does not have a "high degree of confidence in knowing the true identity of the individual" requesting the information, the request is based on a misrepresentation of fact, or the information requested is "Internet navigational data or similar information". The bottom line, though, is that you have a right to see copies of the paperwork that a thief used to open an account in your name. This gives you an advantage because you'll have something to compare and show people to prove it's not you.

- *Businesses must protect certain consumer information.* FACTA adds two provisions that seek to protect key consumer information. Section 605 will require merchants to truncate credit and debit card numbers on electronically printed receipts (though with delayed and staggered effective dates). Section 609 will now allow consumers requesting a report to order the agency to withhold the last five (5) digits of the consumer's social security number on the report. In addition, regulations now require users to dispose of the consumer information they acquire through consumer reports, including the erasing of electronic data.

Credit History Restoration

- *Agencies must block identity-theft-related information*. FACTA adds a new section, 605B, to the FCRA that requires agencies to block identity-theft related information within four (4) days of receiving specified information: proof of the consumer's identity, a copy of an identity theft report, the consumer's identification of the fraudulent information, and the consumer's statement that the

information does not relate to any transaction by the consumer. The agency must also notify the furnisher that a block is in place, and furnishers must implement procedures to prevent them from re-furnishing such information (to anyone, apparently, not just the notifying agency). Although the new provision allows an agency to rescind the block under certain circumstances, the agency must both notify the consumer of the rescission and the specific reason for the rescission within five (5) business days, just as an agency must notify a consumer that it is reinserting formerly deleted information. If the consumer notifies a reseller that a report contains identity-theft-caused information the reseller must block the report.

- *Furnishers must cease furnishing identity-theft-related information.* In turn, the FCRA now requires furnishers who have received notice of a block to have reasonable procedures to prevent them from refurnishing the information. The consumer can also trigger that responsibility by notifying the furnisher directly that the furnisher has furnished fraudulent information.

- *Furnishers may not sell or place for collection identity theft debt.* Once a furnisher has been notified that an agency has blocked a consumer's information as having resulted from identity theft, the furnisher may not sell or transfer the debt or place it for collection. This is not limited to third-party collectors.

- *Debt collectors must notify creditors of fraudulent debt.* FACTA imposes new notification responsibilities on debt collectors; once a consumer notifies a debt collector that a debt may be fraudulent or may have resulted from identity theft, the debt collector must notify the creditor of that allegation and must provide the consumer with all information about the debt to which the consumer would be entitled if the consumer were in fact the liable party.

Information Accuracy

- *Agencies to issue new accuracy and integrity regulations for furnishers.* The agencies that enforce the FCRA will establish guidelines for furnishers regarding the accuracy and integrity of furnished information and will issue regulations requiring furnishers to establish reasonable policies and procedures for implementing those guidelines.

- *Consumers may dispute furnished information directly with the furnisher.* The prior version of the FCRA had no provision by which a consumer could dispute an inaccurate item of information directly with the furnisher; rather, the consumer had to dispute the item with the agency which the FCRA then required to notify the furnisher. The FCRA, prior to amendment by FACTA, required the furnisher to reinvestigate the item only upon receiving the agency's notice, notice from the consumer was irrelevant and ineffective. Now a consumer may trigger a furnisher's responsibility to reinvestigate by disputing the item directly with the

furnisher where the circumstances of the dispute meet the conditions of set forth in the regulations.

- *Financial institution furnishers to notify customers of negative information.* The FCRA now requires a financial institution to notify a customer that it is furnishing negative information about that customer; however, financial institutions may take advantage of a safe harbor provision. The Federal Reserve Board is to provide a model notice not to exceed thirty (30) words.

- *Agencies must notify furnishers of reinvestigation results.* Now an agency that reinvestigates an item of information upon a consumer's dispute must notify the furnisher that furnished the information if the agency deletes or modifies it from the consumer's file because the agency found it to be inaccurate, incomplete or unverifiable.

- *Furnishers must block unverifiable information.* Under the prior version of the FCRA, once an agency notified a furnisher that a consumer disputed information that the furnisher had reported to the agency, the furnisher had to reinvestigate that item and report the results of the investigation back to the agency. Now the furnisher must also take steps to modify, delete or block that information to prevent it from re-reporting the inaccurate information. Consumers may enforce this provision.

Free Credit Reports

- *Agencies must provide consumers with a free annual credit report.* Consumers now have a right to a free annual credit report from nationwide and nationwide specialty consumer reporting agencies. On an annual basis, consumers may obtain a free credit report from each of the nationwide agencies within fifteen (15) days, after making the request by telephone, Internet or mail.

- Tennessee residents have been able to obtain their free credit reports since June 1, 2005. You can get yours through www.annualcreditreport.com, or you can call any of the credit bureaus' numbers listed above.

To whom should I report identity theft?

The Federal Trade Commission
http://www.ftc.gov/bcp/edu/microsites/idtheft

The Federal Trade Commission (the "FTC") is the federal clearinghouse for complaints by victims of identity theft. Although the FTC does not have the authority to bring criminal cases, the Commission assists victims of identity theft by providing them with information to help them resolve the financial and other problems that can result from identity theft. The FTC also may refer victim complaints to other appropriate government agencies and private organizations for further action.

As noted above, the FTC also runs the federal government's identity theft websites at http://www.ftc.gov/bcp/edu/microsites/idtheft and www.onguardonline.gov. These sites have abundant useful information (including form letters), and you can also file a complaint online. (See the attached **Exhibit A** for a sample of the form of complaint you can file with the FTC.) If you've been a victim of identity theft, you can file a complaint with the FTC by contacting the FTC's Identity Theft Hotline, as follows:

By phone:
Toll-free 1-877-ID-THEFT (438-4338)

By mail:
Identity Theft Clearinghouse
Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580

More identity theft resources can be found at the Privacy Rights Clearinghouse's website at **www.privacyrights.org** or the National Consumer Law Center's web site at **www.consumerlaw.org**. Note that each of these Internet sites also provide a form of "Identity Theft Affidavit," which can be downloaded and when completed, provides a very useful document to be provided to credit grantors, employers and federal and state agencies that make inquiries as to the identity theft. A copy of the Identity Theft Affidavit is attached as **Exhibit B**.

The Tennessee Division of Consumer Affairs
www.state.tn.us/consumer

The Tennessee Division of Consumer Affairs can also be contacted to file complaints regarding any consumer matter, including identity theft. The contact information for this organization is as follows:

By phone:
Toll-free 1-800-342-8385

By mail:
Consumer Affairs
500 James Robertson Parkway
Nashville, TN 37243-0600

ONE VERY IMPORTANT TIP: The importance of reporting an identity theft case to the police cannot be overemphasized. Your banks or credit card companies, and various agencies you may deal with – including the FTC, if you choose to file a complaint, or the IRS if you have tax-related issues arising from the identity theft – will probably want you to provide a copy of the police report. The Identity Theft Affidavit also calls for you to attach a copy of the police report to it – see Item 22 of the form

affidavit – if you have one available or can obtain a copy from the police or sheriff's department that investigated it.

III. SPECIALIZED ISSUES IN IDENTITY THEFT

Bankruptcy Fraud: U.S. Trustee
www.usdoj.gov/ust

If you believe someone has fraudulently filed for bankruptcy in your name, write to the U.S. Trustee in the region where the bankruptcy was filed. A list of the U.S. Trustee Program's Regional Offices is available on the U.S. Trustee's website or you may look in the telephone book under the Blue Pages under "US Government – Bankruptcy Administration." You may contact the nearest U.S. Trustee Program's office for Region 8 at 31 East 11th Street, 4th Floor, Chattanooga, TN 37402, phone: 423-752-5153, fax: 423-752-5161.

Your letter should describe the situation and provide proof of your identity. The U.S. Trustee, if appropriate, will make a criminal referral to law enforcement authorities if you provide appropriate documentation to substantiate your claim. You also may want to file a complaint with the U.S. Attorney or the FBI in the city where the bankruptcy was filed.

The U.S. Trustee does *not* provide legal representation, legal advice or referrals to lawyers. This means that you may need to hire an attorney to help convince the Bankruptcy Court that the filing is fraudulent. The U.S. Trustee also does *not* provide consumers with free copies of court documents. Those documents are available from the Bankruptcy Court clerk's office for a fee.

Criminal Violations

Although procedures to correct your record within the criminal justice databases vary from state to state, and even from county to county, the following information serves as a general guide.

If wrongful criminal violations are attributed to your name, contact the arresting or citing law enforcement agency – that is, the police or sheriff's department that originally arrested the person using your identity, or the court agency that issued the warrant for the arrest. File an impersonation report and have your identity confirmed. The police department takes a full set of your fingerprints and your photograph, and copies any photo identification documents like your driver's license, passport or visa. Ask the law enforcement agency to compare the prints and photographs with those of the imposter to establish your innocence. If the arrest warrant is from a state or county other than where you live, ask your local police department to send the impersonation report to the police department in the jurisdiction where the arrest warrant, traffic citation or criminal conviction originated.

The law enforcement agency should then recall any warrants and issue a "clearance letter" or certificate of release (if you were arrested/booked). You'll need to keep this document with you at all times in case you're wrongly arrested. Also, ask the law enforcement agency to file, with the district attorney's ("D.A.'s") office and/or court where the crime took place, the record of the follow-up investigation establishing your innocence. This will result in an amended complaint being issued. Once your name is recorded in a criminal database, it's unlikely that it will be completely removed from the official record. Ask that the "key name," or "primary name," be changed from your name to the imposter's name (or to "John Doe" if the imposter's true identity is not known), with your name noted only as an alias.

You'll also want to clear your name in the court records. Contact the D.A.'s office in the county where the case was originally prosecuted. Ask the D.A.'s office there for the appropriate court records needed to clear your name. Finally, contact the Tennessee Department of Safety (see the next section below) to find out if your driver's license is being used by the identity thief. Ask that your files be flagged for possible fraud.

You may need to hire a criminal defense attorney to help you clear your name. Contact the Knoxville Bar Association's Lawyer Referral and Information Service at 522-7501 for helpful assistance in finding an attorney.

Fake Driver's Licenses: Tennessee Department of Safety
www.state.tn.us/safety

If you think that your name or Social Security number is being used by an identity thief to get a driver's license or a non-driver's identity card, contact the Tennessee Department of Safety, which handles motor vehicle licensing in this state. You can reach the Safety Department's Driver License Station for Knox County by phone at 865-594-6399.

Investment Fraud: U.S. Securities and Exchange Commission (the "SEC")
www.sec.gov

The SEC's Office of Investor Education and Assistance serves investors who complain to the SEC about investment fraud or the mishandling of their investments by securities professionals. If you believe that an identity thief has tampered with your securities investments or a brokerage account, immediately report it to your broker or account manager and to the SEC.

You can file a complaint with the SEC using the online Complaint Center at **www.sec.gov/complaint.shtml**. Be sure to include as much detail as possible. If you don't have access to the Internet, you can write to the SEC at its Office of Investor Education and Assistance, 100 F Street, N.E., Washington DC, 20549-0213 or fax 202-942-8088

Mail Theft: U.S. Postal Inspection Service ("USPIS")
http://postalinspectors.uspis.gov

The USPIS is the law enforcement arm of the U.S. Postal Service and is responsible for investigating cases of identity theft involving the U.S. mail system. If an identity thief has stolen your mail to get new credit cards, bank or credit card statements, pre-screened credit offers or tax information, has falsified change-of-address forms, or obtained your personal information through a fraud conducted by mail, report it to your local postal inspector. You can locate the USPIS district office nearest you by calling your local post office for your particular ZIP code, or by checking the list at the website above.

Passport Fraud: United States Department of State ("USDS")
http://travel.state.gov/passport/passport_1738.html

If you've lost your passport or believe it was stolen or is being used fraudulently, contact the USDS through their website or call a local USDS field office. You can also contact the General Post Office for Knox County for any passport-related questions at the following address: 1237 E. Weisgarber Road, Knoxville, TN 37950-9616, phone: 865-558-4664.

Electronic Passports

All passports issued since August 2007 are electronic passports. An electronic passport is just like a traditional passport except it contains a micro-chip imbedded in the back cover. The chip stores all of the same visual data on the passport, a digital image of the passport photograph, a unique identification number and a digital signature. This electronic data protects the information from alteration. As well as ensuring data security, electronic passports facilitate identity verification of travelers, quicken immigration inspection and provide heightened border protection and security.

Phone Fraud

If an identity thief has established phone service in your name, is making unauthorized calls that seem to come from, and are billed to, your cellular phone, or is using your calling card and PIN, contact your service provider immediately to cancel the account and/or calling card. Open new accounts and choose new PINs. If you're having trouble getting fraudulent phone charges removed from your account or getting an unauthorized account closed, contact the appropriate agency from the list below.

- *For local service*: contact the Tennessee Regulatory Agency (.TRA.) **www.state.tn.us/tra/index.htm**. The TRA regulates local telephone service across this state. You can reach the TRA at 460 James Robertson Parkway, Nashville, TN 37243, or by phone at 1-800-342-8359.

- *For cellular phones and long distance*: contact the Federal Communications Commission ("FCC") – **www.fcc.gov**. The FCC regulates interstate and international communications by radio, television, wire, satellite and cable. You can contact the FCC's Consumer Information Bureau to find out about information, forms, applications and current issues before the FCC. Call: 1-888-CALL-FCC; TTY: 1-888-TELL-FCC; or write: Federal Communications Commission, Consumer Information Bureau, 445 12th Street, SW, Room 5A863, Washington, DC 20554. You can also file FCC complaints via the online complaint form at **www.fcc.gov**, or e-mail questions to **fccinfo@fcc.gov**.

Be aware that "pretexting," or procuring cell phone records for sale, is becoming a fast-growing strain of identity theft. For around $100, an online "people locator" or "information broker" can get you access to the records associated with a given cell phone number. They do this by getting your personal data from public records or commercial databases, then calling the phone company, pretending to be you, and authorizing the release of your records.

Social Security Number Misuse: Social Security Administration (the "SSA")
www.ssa.gov

One way to find out if someone is wrongfully using your Social Security number is to check your earnings record. If you are 25 or older and not already receiving Social Security benefits, you will automatically receive a Social Security Statement by mail each year. This Statement lists earnings posted to your Social Security record and provides an estimate of benefits you and your family may be eligible to receive now and in the future. You should get your Statement about three (3) months before your birth month. If you don't get a Statement, you can ask for one by submitting a Request for Social Security Statement (Form 7004). To get a Form 7004, download the form from the Internet at **www.socialsecurity.gov/online/ssa-7004.pdf.**

The SSA Office of the Inspector General investigates cases of identity theft. You can report allegations of a stolen or misused Social Security number to the SSA Fraud Hotline. Call: 1-800- 269-0271; fax: 410-597-0118; write: SSA Fraud Hotline, P.O. Box 17768, Baltimore, MD 21235; or e-mail: oig.hotline@ssa.gov. Also, call SSA at 1-800-772-1213 to verify the accuracy of your reported earnings and to ask for a copy of your Social Security Statement. You should follow this call up in writing.

Several useful SSA publications are as follows:

- SSA Fraud Hotline for Reporting Fraud – **www.ssa.gov/oig/guidelin.htm**

- Social Security: Your Number and Card (SSA Pub. No. 05-10002) . **www.ssa.gov/pubs/10002.html**

- When Someone Misuses Your Number (SSA Pub. No. 05-10064) . **www.ssa.gov/pubs/10064.html**

Tax Fraud: Internal Revenue Service (the "IRS")
www.treas.gov/irs/ci

The IRS administers and enforces the federal tax laws. If you believe someone has assumed your identity to file federal income tax returns or commit other tax-related fraud, call the IRS, toll-free, at 1-800-829-1040. Victims of identity theft who are having troubles filing their returns should call the IRS. Taxpayer Advocates Office, toll-free, at 1-877-777-4778.

IV. OTHER PRIVACY RESOURCES AND RELATED ISSUES

How to Get Off Marketing Lists.

You may write to the Direct Marketing Association (the "DMA") Mail Preference Service at P.O. Box 282, Carmel, New York 10512 to request deletion of names from mailing lists of participating catalog companies and from the telemarketing database of participating telemarketers. You may also fill out an online request form at www.the-dma.org/donotmail/

Visit the DMA online at **www.the-dma.org** for more information about the DMA Privacy Promise, direct marketing and the DMA Ethical Guidelines. You can also file a complaint against any DMA member who violates the DMA Guidelines or the Privacy Promise.

Please note that not all catalog companies and telemarketers belong to the Direct Marketing Association, so you may continue to receive some solicitations after you sign up for the DMA's preference services. Additionally, you will continue to receive solicitations and catalogues from companies that you have patronized in the past. To remove your name from these companies. mailing and telephone lists, you must contact each company directly.

Also, most telemarketers are required by federal law to maintain a list of individuals who do not want to receive telephone solicitations. Some states also have mandatory do not call lists. If you receive unwanted telephone solicitations, request that the caller place your phone number on its "DO NOT CALL" list. However, the law exempts charitable organizations, political organizations, and polling/survey organizations from maintaining a Do Not Call list, and these types of organizations may continue to contact you regardless of your requests.

You may also request removal of names from credit reporting companies. marketing lists by calling **1-888-5 OPT OUT** or by contacting the major credit reporting services at the following addresses:

Equifax: **www.equifax.com**
Experian: **www.experian.com**

TransUnion: **www.transunion.com**

How to Manage Credit Reports

If you're one of the 190 million people in the United States with a credit card, mortgage, or car loan, information about you probably is stored in the databases maintained by the three (3) main consumer credit reporting agencies. Your consumer credit report is a factual record of your credit payment history. This report can be provided by the credit reporting agency to others in accordance with federal and state laws. The information in your credit report is primarily used by businesses that are trying to decide whether to grant you credit. The information can also be used for other purposes, such as direct marketing.

Most of the information in your consumer credit report comes directly from the companies you do business with, but some information comes from public records. The typical consumer credit report includes four (4) types of information: Identifying Information, Credit Information, Public Records, and Inquiry Information.

Identifying information consists of your name, nicknames, current and previous addresses, Social Security number, and month and year of birth. Your telephone number may also be included. This information comes from credit applications that you complete, so its accuracy depends on your filling out the forms clearly, completely and consistently each time you apply for credit. *This is the only information that is distributed by companies who provide access to "credit header" data.*

Credit information includes specific information about your accounts, such as the date opened, credit limit or loan amount, balance, monthly payment and payment pattern during the past several years. The report also states whether anyone else besides you (your spouse or cosigner, for example) is responsible for paying the account. This information comes from companies that do business with you. *This information is provided to others only in accordance with the Fair Credit Reporting Act.*

Your credit report may also contain public record information (such as bankruptcy records; state and county court records, tax liens and monetary judgments; and, in some states, overdue child support). Finally, your credit report contains the names of those who obtained a copy of your credit report for any reason. This information comes from the consumer credit reporting agency, and it remains up to two (2) years, consistent with federal law.

It is a good idea to review your credit report each year, whether or not you think an identify theft has occurred. Reports can be ordered from Equifax, Trans Union and Experian using the contact information given above. Reports are free to anyone who has been a victim of identity theft as well as to anyone who has been denied credit or employment based on the contents of the report.

Children's Privacy Resources

For information on protecting kids online, visit:

The FTC: http://www.ftc.gov/privacy/privacyinitiatives/childrens.html

- The Children's Advertising Review Unit of the Better Business Bureau: **www.caru.org**

- The Direct Marketing Association – "Get Cybersavvy" Family Guide: **www.cybersavvy.org**

- Yahoo!'s Parent and Teacher Resources, including Safe Surfing Quiz: **www.yahooligans.com, www.netsmartz.org, http://kids.yahoo.com**

General Information about Online Privacy, Spam and Cookies

For information about protecting your privacy and security online, visit:

The Online Privacy Alliance: **www.privacyalliance.org**
TrustE: **www.truste.org**
Better Business Bureau Online: **www.bbbonline.org**
Privacy Rights Clearinghouse: **www.privacyrights.org**
Electronic Privacy Information Center: **www.epic.org**

For information about e-mail marketing and "cookies," which companies with an Internet presence use to track and monitor your visits to their and others' sites, and which companies often share with advertisers and others (and to learn how to opt out of compilation of personal and advertising/marketing data compiled from cookies), see:

DoubleClick: **www.doubleclick.com** - click on Privacy Policy
Network Advertising Initiative: **www.networkadvertising.org**

For help reporting "spam," which is any unsolicited advertisement received via the Internet, visit: **www.spamcop.net**. Almost all 50 states have anti-spamming laws; however, to date only one person, Jeremy Jaynes, has been convicted of violating the federal anti-spam law. He appealed his conviction, claiming that the law violates his First Amendment right to free speech. In February 2008, the Virginia Supreme Court affirmed Jaynes' felony conviction.

If you're interested in traveling the internet anonymously, consider downloading the free Tor software available at http://tor.eff.org/ or the commercial services offered by Anonymizer (www.anonymizer.com). These and other products are meant to make it harder for others to engage in "traffic analysis," that is, to trace your visits to web sites, your online posts or messages, and other communication forms. If you install one of these

products, use a site like www.showmyip.com to confirm that your Internet Protocol address has changed; if it has, then the software is working.

V. THE LAST WORD

Don't give in! Remember, do not allow yourself to be coerced into paying any bill or portion of a bill that is a result of identity theft. Do not cover any checks that were written or cashed fraudulently. Do not file for bankruptcy. Your credit rating should not be permanently affected. No legal action should be taken against you as the victim of an identity theft, but – using the tools and services outlined above – you need to take action to clear your name and record as soon as possible.

Identity theft may be a growing problem in the 21st Century, both nationally and in Tennessee; however, you can take many steps in advance to make identity theft more difficult and – if identity theft ever occurs to you – this outline's suggestions will hopefully give you various ways to better fight its effects.

INSTRUCTIONS FOR COMPLETING THE ID THEFT AFFIDAVIT

To make certain that you do not become responsible for any debts incurred by an identity thief, you must prove to each of the companies where accounts were opened in your name that you didn't create the debt. The ID Theft Affidavit was developed by a group of credit grantors, consumer advocates, and attorneys at the Federal Trade Commission (FTC) for this purpose. Importantly, this affidavit is only for use where a new account was opened in your name. If someone made unauthorized charges to an existing account, call the company for instructions.

While many companies accept this affidavit, others require that you submit more or different forms. Before you send the affidavit, contact each company to find out if they accept it. If they do not accept the ID Theft Affidavit, ask them what information and/or documentation they require.

You may not need the ID Theft Affidavit to absolve you of debt resulting from identity theft if you obtain an Identity Theft Report. We suggest you consider obtaining an Identity Theft Report where a new account was opened in your name. An Identity Theft Report can be used to (1) permanently block fraudulent information from appearing on your credit report; (2) ensure that debts do not reappear on your credit reports; (3) prevent a company from continuing to collect debts or selling the debt to others for collection; and (4) obtain an extended fraud alert.

The ID Theft Affidavit may be required by a company in order for you to obtain applications or other transaction records related to the theft of your identity. These records may help you prove that you are a victim. For example, you may be able to show that the signature on an application is not yours. These documents also may contain information about the identity thief that is valuable to law enforcement.

This affidavit has two parts:

- Part One — the ID Theft Affidavit — is where you report general information about yourself and the theft.
- Part Two — the Fraudulent Account Statement — is where you describe the fraudulent account(s) opened in your name. Use a separate Fraudulent Account Statement for each company you need to write to.

When you send the affidavit to the companies, attach copies (NOT originals) of any supporting documents (for example, driver's license or police report). Before submitting your affidavit, review the disputed account(s) with family members or friends who may have information about the account(s) or access to them.

Complete this affidavit as soon as possible. Many creditors ask that you send it within two weeks. Delays on your part could slow the investigation.

Be as accurate and complete as possible. You may choose not to provide some of the information requested. However, incorrect or incomplete information will slow the process of investigating your claim and absolving the debt. Print clearly.

When you have finished completing the affidavit, mail a copy to each creditor, bank, or company that provided the thief with the unauthorized credit, goods, or services you describe. Attach a copy of the Fraudulent Account Statement with information only on accounts opened at the institution to which you are sending the packet, as well as any other supporting documentation you are able to provide.

Send the appropriate documents to each company by certified mail, return receipt requested, so you can prove that it was received. The companies will review your claim and send you a written response telling you the outcome of their investigation. Keep a copy of everything you submit.

If you are unable to complete the affidavit, a legal guardian or someone with power of attorney may complete it for you. Except as noted, the information you provide will be used only by the company to process your affidavit, investigate the events you report, and help stop further fraud. If this affidavit is requested in a lawsuit, the company might have to provide it to the requesting party. Completing this affidavit does not guarantee that the identity thief will be prosecuted or that the debt will be cleared.

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

1. Any one of the nationwide consumer reporting companies to place a fraud alert on your credit report. Fraud alerts can help prevent an identity thief from opening any more accounts in your name. The company you call is required to contact the other two, which will place an alert on their versions of your report, too.

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

   In addition, once you have placed a fraud alert, you're entitled to order one free credit report from each of the three consumer reporting companies, and, if you ask, they will display only the last four digits of your Social Security number on your credit reports.

2. The security or fraud department of each company where you know, or believe, accounts have been tampered with or opened fraudulently. Close the accounts. Follow up in writing, and include copies (NOT originals) of supporting documents. It's important to notify credit card companies and banks in writing. Send your letters by certified mail, return receipt requested, so you can document what the company received and when. Keep a file of your correspondence and enclosures.

   When you open new accounts, use new Personal Identification Numbers (PINs) and passwords. Avoid using easily available information like your mother's maiden name, your birth date, the last four digits of your Social Security number, your phone number, or a series of consecutive numbers.

3. Your local police or the police in the community where the identity theft took place. Provide a copy of your ID Theft Complaint filed with the FTC (see below), to be incorporated into the police report. Get a copy of the police report or, at the very least, the number of the report. It can help you deal with creditors who need proof of the crime. If the police are reluctant to take your report, ask to file a "Miscellaneous Incidents" report, or try another jurisdiction, like your state police. You also can check with your state Attorney General's office to find out if state law requires the police to take reports for identity theft. Check the Blue Pages of your telephone directory for the phone number or check www.naag.org for a list of state Attorneys General.

4. The Federal Trade Commission. By sharing your identity theft complaint with the FTC, you will provide important information that can help law enforcement officials across the nation track down identity thieves and stop them. The FTC also can refer victims' complaints to other government agencies and companies for further action, as well as investigate companies for violations of laws that the FTC enforces.

   You can file a complaint online at www.consumer.gov/idtheft. If you don't have Internet access, call the FTC's Identity Theft Hotline, toll-free: 1-877-IDTHEFT (438-4338); TTY: 1-866-653-4261; or write: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580. When you file an ID Theft Complaint with the FTC online, you will be given the option to print a copy of your ID Theft Complaint. You should bring a copy of the printed ID Theft Complaint with you to the police to be incorporated into your police report. The ID Theft Complaint, in conjunction with the police report, can create an Identity Theft Report that will help you recover more quickly. The ID Theft Complaint provides the supporting details necessary for an Identity Theft Report, which go beyond the details of a typical police report.

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

ID Theft Affidavit

Victim Information

(1) My full legal name is _____
(First) (Middle) (Last) (Jr., Sr., III)

(2) (If different from above) When the events described in this affidavit took place, I was known as

_____
(First) (Middle) (Last) (Jr., Sr., III)

(3) My date of birth is _____
(day/month/year)

(4) My Social Security number is_____

(5) My driver's license or identification card state and number are_____

(6) My current address is _____

City _____ State _____ Zip Code _____

(7) I have lived at this address since _____
(month/year)

(8) (If different from above) When the events described in this affidavit took place, my address was

_____ _____

City _____ State _____ Zip Code _____

(9) I lived at the address in Item 8 from _____ until _____
(month/year) (month/year)

(10) My daytime telephone number is (_____)_____

My evening telephone number is (_____)_____

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

How the Fraud Occurred

Check all that apply for items 11 - 17:

(11) ❑ I did not authorize anyone to use my name or personal information to seek the money, credit, loans, goods or services described in this report.

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

(13) ❑ My identification documents (for example, credit cards; birth certificate; driver's license; Social Security card; etc.) were ❑ stolen ❑ lost on or about _____.
(day/month/year)

(14) ❑ To the best of my knowledge and belief, the following person(s) used my information (for example, my name, address, date of birth, existing account numbers, Social Security number, mother's maiden name, etc.) or identification documents to get money, credit, loans, goods or services without my knowledge or authorization:

_____ Name (if known)	_____ Name (if known)
_____ Address (if known)	_____ Address (if known)
_____ Phone number(s) (if known)	_____ Phone number(s) (if known)
_____ Additional information (if known)	_____ Additional information (if known)

(15) ❑ I do NOT know who used my information or identification documents to get money, credit, loans, goods or services without my knowledge or authorization.

(16) ❑ Additional comments: (For example, description of the fraud, which documents or information were used or how the identity thief gained access to your information.)

_____

_____

_____

_____

_____

(Attach additional pages as necessary.)

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

Victim's Law Enforcement Actions

(17) (check one) I ❑ am ❑ am not willing to assist in the prosecution of the person(s) who committed this fraud.

(18) (check one) I ❑ am ❑ am not authorizing the release of this information to law enforcement for the purpose of assisting them in the investigation and prosecution of the person(s) who committed this fraud.

(19) (check all that apply) I ❑ have ❑ have not reported the events described in this affidavit to the police or other law enforcement agency. The police ❑ did ❑ did not write a report. In the event you have contacted the police or other law enforcement agency, please complete the following:

_____	_____
(Agency #1)	(Officer/Agency personnel taking report)
_____	_____
(Date of report)	(Report number, if any)
_____	_____
(Phone number)	(email address, if any)
_____	_____
(Agency #2)	(Officer/Agency personnel taking report)
_____	_____
(Date of report)	(Report number, if any)
_____	_____
(Phone number)	(email address, if any)

Documentation Checklist

Please indicate the supporting documentation you are able to provide to the companies you plan to notify. Attach copies (NOT originals) to the affidavit before sending it to the companies.

(20) ❑ A copy of a valid government-issued photo-identification card (for example, your driver's license, state-issued ID card or your passport). If you are under 16 and don't have a photo-ID, you may submit a copy of your birth certificate or a copy of your official school records showing your enrollment and place of residence.

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

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

(22) ❑ A copy of the report you filed with the police or sheriff's department. If you are unable to obtain a report or report number from the police, please indicate that in Item 19. Some companies only need the report number, not a copy of the report. You may want to check with each company.

Signature

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

_____ _____
(signature) (date signed)

_____
(Notary)

[Check with each company. Creditors sometimes require notarization. If they do not, please have one witness (non-relative) sign below that you completed and signed this affidavit.]

Witness:

_____ _____
(signature) (printed name)

_____ _____
(date) (telephone number)

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

Fraudulent Account Statement

Completing this Statement

- Make as many copies of this page as you need. **Complete a separate page for each company you're notifying and only send it to that company**. Include a copy of your signed affidavit.
- List only the account(s) you're disputing with the company receiving this form. **See the example below**.
- If a collection agency sent you a statement, letter or notice about the fraudulent account, attach a copy of that document (**NOT** the original).

I declare (check all that apply):

❑ As a result of the event(s) described in the ID Theft Affidavit, the following account(s) was/were opened at your company in my name without my knowledge, permission or authorization using my personal information or identifying documents:

Creditor Name/Address (the company that opened the account or provided the goods or services)	Account Number	Type of unauthorized credit/goods/services provided by creditor (if known)	Date issued or opened (if known)	Amount/Value provided (the amount charged or the cost of the goods/services)
Example Example National Bank 22 Main Street Columbus, Ohio 22722	01234567-89	auto loan	01/05/2002	$25,500.00

❑ During the time of the accounts described above, I had the following account open with your company:

Billing name _____

Billing address_____

Account number _____

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

OMB #
3084-0047

Complaint Input Form

If you believe you have been the victim of identity theft, you may use the form below to send a complaint to the Federal Trade Commission (FTC). The information you provide is up to you. However, if you don't provide your name or other information, it may be impossible for us to refer, respond to, or investigate your complaint or request. To learn how we use the information you provide, please read our **Privacy Policy**.

The FTC serves as the federal clearinghouse for complaints by victims of identity theft. While the FTC does not resolve individual consumer problems, your complaint helps us investigate fraud, and can lead to law enforcement action. The FTC enters Internet, telemarketing, identity theft and other fraud-related complaints into Consumer Sentinel®, a secure, online database available to hundreds of civil and criminal law enforcement agencies worldwide.

We use secure socket layer (SSL) encryption to protect the transmission of the information you submit to us when you use our secure online forms. The information you provide to us is stored securely.

If you want to file a complaint with the FTC about a problem other than identity theft, please use the Federal Trade Commission online **complaint form**.

Printing This Complaint
After you have completed this online complaint form and have submitted the information to the FTC, you will have the opportunity to print out a completed ID Theft Complaint form that contains most of the information you filed in your complaint (very sensitive information, such as Social Security Numbers and Account Numbers, will not print). The printed ID Theft Complaint will be reformatted so that it can be used to support your local police report. Instructions on how to complete this online complaint form and information on how to use the printed ID Theft Complaint can be found here.

How Do We Reach You?

First Name:

Middle Name:

Last Name:

Suffix:

Street Address:

Apt. or Suite No.:

City:

State/Province:

Zip: -

Country:

Lived at this address since: **(MM/YY)**

Home Phone: ( ) *(Area Code)(Phone Number)*

Work Phone: **Ext.** *(Area Code)(Phone Number)(Extension)*

Cell Phone: ( ) *(Area Code)(Phone Number)*

Social Security Number: - -

Date Of Birth: **(MM/DD/YYYY)**

Drivers License State:

Drivers License Number:

Email Address: **(i.e., anyone@myisp.com)**

Complete if different from above when the events took place:

First Name:

Middle Name:

Last Name:

Suffix:

Street Address:

Apt. or Suite No.:

City:

State/Province:

Zip: -

Country:

Lived at this address from: (MM/YY) **until:** (MM/YY)

Tell Us About Your Problem

1. Types of Identity Theft You Have Experienced.

ID Theft occurs when someone uses your name or other identifying information for their personal gain. Please check the types of ID theft you were a victim of. (Check as many as apply)

- ☐ **Credit Cards**
- ☐ **Checking or Savings Accounts**
- ☐ **Loans**
- ☐ **Phone or Utilities**
- ☐ **Securities or Other Investments**
- ☐ **Internet or E-Mail**
- ☐ **Government Documents or Benefits**
- ☐ **Other**

Did suspect use the Internet to open the account or purchase the goods or services?

- ☐ Yes
- ☐ No
- ◉ Don't Know

2. Summary of Complaint

Please give us information about the identity theft, including, but not limited to, how the theft occurred, who may be responsible for the theft, and what actions you have taken since the theft. Please briefly describe problems you have had with companies where fraudulent accounts were established or your current accounts were affected. Please limit your summary to 2000 characters.

PLEASE DO NOT INCLUDE ANY SENSITIVE PERSONAL INFORMATION (e.g., Social Security number, date of birth, financial account or credit/debit card numbers, driver's license number, detailed health or medical history, or similarly sensitive information)

3. Details of the Identity Theft.

Did you authorize anyone to use your name or personal information to obtain the money, credit, loans, goods, or services, or for other purposes? Yes No

Did you receive any benefit, money, goods, or services as a result of the events described? Yes No

(Check one, if applicable) Your personal information or identification documents (for example, credit cards, birth certificate; driver's license; Social Security card; etc.) were: stolen lost on or about (MM/DD/YYYY)

(Check one) Are you willing not willing to assist in the prosecution of the person(s) who committed this fraud?

Do you know who used your information or identification documents to conduct financial transactions, cash checks, make withdrawals, or to obtain money, goods, or services without your knowledge or authorization as described? Yes No

When did you notice that you might be a victim of identity theft? **(MM/DD/YYYY)**

When did the identity theft first occur? (i.e., when was the first account opened?) **(MM/DD/YYYY)**

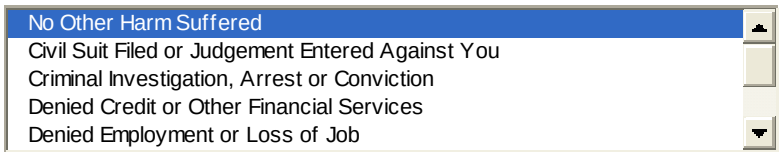
How many accounts (credit cards, loans, bank accounts, cellular phone accounts, etc.) were opened or accessed?

How much money, if any, have you had to pay? *(Numbers Only)*

How much money, if any, did the identity thief obtain from companies in your name? *(Numbers Only)*

How did the thief obtain the personal information?

What other problems, if any, have you experienced as a result of the identity theft? (Click on the down arrow. To select more than one, hold down the CTRL key while clicking your selection)



4. The Identity Thief.

Please provide any information you may have about the identity thief, including his or her name, and any addresses or phone numbers the identity thief may have used.

First Name:

Middle Name:

Last Name:

Suffix:

Street Address:

Apt. or Suite No.:

City:

State/Province:

Zip: -

Country:

Phone Number: **(** **)** *(Area Code)(Phone Number)*

Email Address:
(i.e., anyone@myisp.com)

Date Of Birth: **(MM/DD/YYYY)**

Additional information about this suspect (240 characters):

Your relationship to the identity thief:

5. Contacts.

Please indicate which of the following steps, if any, you have already taken to deal with the identity theft.
For which of the following credit bureaus, have you: (check all that apply)

Called to report the fraud?:	☐	**Equifax**	☐	**Experian**	☐	**Trans Union**	☐	**Other**	☐ **None**
Put a "fraud alert" on your report?:	☐	**Equifax**	☐	**Experian**	☐	**Trans Union**	☐	**Other**	☐ **None**
Ordered your credit report?:	☐	**Equifax**	☐	**Experian**	☐	**Trans Union**	☐	**Other**	☐ **None**
Problem with Credit Bureau?:	☐	**Equifax**	☐	**Experian**	☐	**Trans Union**	☐	**Other**	

Inaccurate Information on Credit Report

Personal information (Name, SSN, DOB, etc.):

(A)

(B)

(C)

(D)

Companies that requested your credit report without your knowledge:

Company Name:

Company Name:

Company Name:

Have you contacted the police? ☐ Yes ☐ No

If yes, please provide police department name:

Department State:

Report Number? ☐ Yes ☐ No

If yes, please provide report number:

6. Companies

Please identify companies or organizations where fraudulent accounts were established or your current accounts were affected. Please provide as much specific information about the fraudulent account or activity as possible.

Company 1

Company Name:

Type of Account:

New Account?

☐ Yes

☐ No

Date Issued or Misused: **(MM/DD/YYYY)**

Amount Thief Obtained ($):

(Numbers Only)

Credit Limit ($):

(Numbers Only)

Contact Person:

Contact Phone: **Ext.**

(Area Code)(Phone Number)(Extension)

Have you notified this company?

☐ Yes

☐ No

Have you sent written notifications to this company?

☐ Yes

☐ No

Company 2

Company Name:

Type of Account:

New Account?

☐ Yes

☐ No

Date Issued or Misused: **(MM/DD/YYYY)**

Amount Thief Obtained ($):

(Numbers Only)

Credit Limit ($):

(Numbers Only)

Contact Person:

Contact Phone: **Ext.**

(Area Code)(Phone Number)(Extension)

Have you notified this company? ☐ Yes ☐ No

Have you sent written notifications to this company? ☐ Yes ☐ No

Company 3

Company Name:

Type of Account:

New Account? ☐ Yes ☐ No

Date Issued or Misused: **(MM/DD/YYYY)**

Amount Thief Obtained ($):
(Numbers Only)

Credit Limit ($):
(Numbers Only)

Contact Person:

Contact Phone: **Ext.**
(Area Code)(Phone Number)(Extension)

Have you notified this company? ☐ Yes ☐ No

Have you sent written notifications to this company? ☐ Yes ☐ No

7. Documentation

Please indicate the supporting documentation you can provide to the law enforcement department or companies you notify. (Check either or both)

☐ **Government-issued identification information:**

☐ **Proof of residency during the time the event took place (for example, a rental/lease agreement in your name, a copy of a utility bill or a copy of an insurance bill)**

Reset

Paperwork Reduction Act Statement: This form is designed to improve public access to the FTC's Bureau of Consumer Protection's Consumer Response Center, and is voluntary. Through this form, consumers may electronically register a complaint with the FTC. We estimate that it will take, on average, 5 minutes to complete the form. Under the Paperwork Reduction Act, as amended, an agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a currently valid OMB control number. That number is 3084-0047, which also appears in the upper right-hand corner of the first page of this form.

Identity Theft IQ Test
Are You at Risk for Identity Theft? Test Your "Identity Quotient"

___ I receive several offers of pre-approved credit every week. **(5 points)**

___ **Add 5 points** if you do not shred them (cross-cut shredder preferred) before putting them in the trash.

___ I carry my Social Security card in my wallet. **(10 points)**

___ My state driver's license has my SSN printed on it, and I have not contacted the Department of Motor Vehicles to request a different number. **(10 points)**

___ I do not believe someone would break into my house to steal my personal information. **(10 points)**

___ I do not use a firewall on my personal computer. **(10 points)**

___ I have not ordered a copy of my credit reports for at least 2 years. **(20 points)**

___ I use an unlocked, open box at work or at my home to drop off my outgoing mail. **(10 points)**

___ I do not have a P.O. Box or a locked, secured mailbox. **(5 points)**

___ I carry my military ID in my wallet at all times. (It displays my SSN.) **(10 points)**

___ I do not shred (cross-cut shredder preferred) my banking and credit information when I throw it in the trash. **(10 points)**

___ I throw away old credit and debit cards without shredding or cutting them up. **(10 points)**

___ I provide my Social Security number (SSN) whenever asked, without asking why it is needed and how it will be safeguarded. **(10 points)**

___ **Add 5 points** if you provide it orally without checking to see who might be listening nearby.

___ I leave my purse or wallet in my car. **(10 points)**

___ I am required to use my SSN at work as an employee ID or at college as a student ID number. **(5 points)**

___ My SSN is printed on my employee badge that I wear at work or in public. Or it is posted on my time card in full view of others, or is on other documents frequently seen by many others at work. **(10 points)**

___ I have my SSN and/or driver's license number printed on my personal checks. **(10 points)**

___ I am listed in a "Who's Who" guide. **(5 points)**

___ I carry my insurance card (including Medicare) in my wallet **and** either my SSN or that of my spouse is the ID number. **(10 points)**

___ I do not believe that people would root around in my trash looking for credit or financial information or for documents containing my SSN. **(10 points)**

___ I do not verify that all financial (credit card, checking) statements are accurate monthly. **(10 points)**

Each one of these questions represents a possible avenue for an identity thief.

Understanding Your Score:

- **100 + points** - Recent surveys* indicate that 8-9 million people are victims of ID theft each year. You are at high risk. We recommend you purchase a cross-cut paper shredder, become more security-aware in document handling, and start to question why people need your personal data.
- **50-99 points** - Your odds of being victimized are about average.
- **0-49 points** - Congratulations. You have a high "IQ."
  Keep up the good work and don't let your guard down now.