Identity Theft: The Silent Thief

Dina Nesheiwat, St. Thomas University
Introduction

You have an appointment with a new doctor in town and you arrive a few minutes early to fill out all the necessary paperwork that requests the usual information of your name, address, Social Security number, driver’s license number and insurance information. Six months later you apply for a school loan where a credit check is run. Surprisingly, you discover you were declined because there are several credit card accounts listed that you never opened.1 What’s going on? How did this happen? This is how the chaos of identity theft begins.

The visit at the doctor’s office seems harmless and simple but it is actually an example of identity theft at work. It is no longer necessary for burglars to break into a person’s home to accomplish theft. Identity theft is a very serious crime that occurs almost anytime your personal information is used without your knowledge to commit fraud and other crimes.2 Identity thieves can access the personal information of another in quite a few ways. Almost any action where an individual’s identity information is shared or made available to others creates an opportunity for identity theft to occur.

This life changing and often traumatic and heinous crime can take place in the comfort of one’s own home or in a public place, and has no boundaries. It hits the young and the old, the rich, the poor, and even the deceased. Sunday night garbage that is left on the street, the un-shredded credit card statements tossed in the trash, the “pre-approved credit applications” or liberally disclosing credit card numbers over the telephone while booking a flight, hotel reservation or car rental are havens for identity thieves. People are even vulnerable just sitting at a local Starbucks where it is easy for criminals to “shoulder surf” behind customers as they type in their credit card information to access the “hotspot Wi-Fi internet.” At the end, Starbucks

---

becomes an easy “hot spot” for criminals to steal personal information and the identities of unsuspecting customers who unknowingly fall prey to one of the fastest growing crimes of the century.

The identification information most commonly needed by a criminal is basically a person’s name, birth date, Social Security or driver’s license number. All of this information can be easily obtained from stealing one’s mail, going through one’s trash, or by a hacker accessing credit or bank accounts on the Internet.³ Other ways criminals access personal information is often through data companies and even the Department of Motor Vehicles who have been reported to sell personal information for marketing purposes.⁴ Moreover, in some ways it is satirical in how simple it is for a criminal to gather enough personal information through public records, such as property deeds or court records. These documents were once difficult to access but today, are easily retrievable on the Internet.

The two major Federal statutes that apply to identity theft are The Fair and Accurate Credit Transactions Act (the “FACT Act”), and the Identity Theft and Assumption Deterrence Act of 1998. (“ITADA”).⁵ In addition to these regulations, each state sets forth their own statute governing the crime of identity theft. For example, Florida passed the Florida Crimes Code Section 817.568 – Fraudulent Practices – Criminal Use of Personal Identification Information.⁶ Nevertheless, the Executive Orders, United States Code, several Acts passed by Congress and state and local laws, alongside the regulations placed by the Department of Justice (the “DOJ”), Social Security Administration (the “SSA”) Federal Trade Commission (the “FTC) and several

⁴ Id.
others are only a few of the efforts and attempts put forth by the government and its agencies in regulating and preventing the continuance of identity theft.

**Executive Order 13402**

On May 10, 2006, Former President George W. Bush established the President’s Identity Theft Task Force (the “Task Force”) by Executive Order. The former President launched a new era in the fight against identity theft and called for a coordinated approach among government agencies to combat the crime. The Task Force was led by an exhaustive list including former Attorney General Alberto R. Gonzales, and Deborah Platt Majoras, the Chairman of the Federal Trade Commission. The Task Force worked with many of the Federal agencies to determine how the government can increase safeguards to better secure an individual’s personal data that the businesses and the individuals hold.

The Task Force proposed a strategic plan (the “Strategy Plan”) to combat identity theft and attempted to organize government resources to crack down on criminals, strengthen efforts to protect the personal information of individuals, help law enforcement officials investigate, and prosecute the thieves. Moreover, a goal to help to educate consumers and businesses about protecting themselves and increasing protection on the personal data entrusted to them. The strategic plan set out ways to further improve the effectiveness and efficiency of the Federal Government’s activities in the areas of identity theft awareness, prevention, detection, and prosecution.

---

8 Id. at viii.
9 Id. at 3
The plan acknowledged that identity theft had at least three stages in its “life cycle,” and it is best attacked at those stages. The first stage provided ways in which the thief attempts to acquire a victim’s personal information. The described “low-tech” method included stealing mail or workplace records, or even to the extent of “dumpster diving.” Moreover, the illustrated “high tech” schemes include frauds such as hacking and the use of malicious computer codes. Astonishingly, even though the thief obtains the personal information, it does not inevitably lead to identity theft. A report showed the personal records of nearly seventy-three (73) million people that were lost or stolen, but there was no evidence of a surge in identity theft or financial fraud as a result.

The second stage is the thief’s attempt to abuse the illegally obtained information. In most situations, the thief either attempts to greedily use the information for personal gains or to sell the information. The misuse of stolen personal data was classified into two (2) categories by the Task Force; Existing Account Fraud and New Account Fraud. The former type of fraud was typically considered less costly; however, it was a more common form of identity theft that occurred when the criminal obtained account information involving credit, banking, or utility accounts that are already open. The rationale of suggesting this type of fraud was less costly, but the most common was based on the notion that although the thief may have incurred thousands of dollars in fraudulent charges, he typically would not have enough information to ultimately steal your identity. Conversely, one could argue this rationale as absurd for the reason

---

10 Id. at 2
11 Id.
12 Id. at 2-3
13 Id. at 3
14 Id.
15 Id. at 18
that not all financial institutions protect an individual’s account against fraudulent charges. Therefore, to declare any type of fraud less costly seems somewhat outlandish.

The second category encompasses the thieves’ use of one’s personal data. Particularly a Social Security number, birth date, and home address to open new accounts in the victim’s name. The types of new accounts that can be opened with this information include phone services, credit cards, and loans. Fraud has even gone to the extent of criminals obtaining government, medical or other benefits. Although this New Account Fraud is less likely to occur, it imposes much greater costs and hardships on victims.\footnote{Id. at 19}

Finally, the third stage of the identity theft “life cycle” is the point when the identity thief has completed the crime and is enjoying the benefits while the victims are first realizing the harm.\footnote{Id.} The usual scenarios in which the victims first become aware of the identity theft is when they are denied a loan, denied employment, or receive a phone call from a debt collector for a debt they did not incur. Despite the consumer’s confidence in securing their personal information, identity theft can still occur. Unfortunately, security systems are imperfect and identity thieves have become more resourceful, making identity theft inevitable and thus crime on the rise.

The Strategy Plan emphasizes the importance of keeping sensitive consumer data out of the hands of identity thieves by achieving better data security, therefore, making it more difficult for the thieves to steal identities. The proposed plan recommends that Federal agencies reduce the unnecessary use of Social Security numbers, which is probably considered the most valuable commodity for an identity thief.\footnote{Id. at 4} The accessibility of information, education, and awareness for consumers is crucial. When the consumer is vigilant and attentive in understanding the...
importance of securing and protecting their personal data, the number of cases of identity theft reported each year will most likely be reduced. When consumers lack sufficient knowledge and awareness on how to protect themselves, they unfortunately become an easy target for identity thieves. As pretentious as it may seem, there are some individuals who remain ignorant and susceptible, thus the Strategic Plan’s suggestion of implementing “awareness campaigns” is vital and will help to deter, detect, and defend against identity theft.\footnote{Id.}

**The Fair and Accurate Credit Transaction Act of 2003**

The FACT Act was signed by former President George W. Bush in 2003 as an amendment to the Fair Credit Reporting Act (the “FCRA”). Not only does the FACT Act allow consumers to obtain a free copy of their credit report each year, and in some cases, victims of identity theft twice a year; it also added provisions that are primarily intended to help consumers fight the growing crime of identity theft, including accuracy, privacy, limits on information sharing, and new consumer rights to disclosure.\footnote{The Fair and Accurate Credit Transactions Act: Consumers Win Some, Lose Some. http://www.privacyrights.org/fs/fs6a-facta.htm (last visited March 3, 2009).}

The FACT Act defines identity theft as “fraud committed using the identifying information of another person.” However, it is not inconceivable that a victim of identity theft might have their own definition including moments of heartache, confusion, misplaced hope, and distress. Today, too many people encompass the “it won’t happen to me” naïve attitude. However, those targeted range from the most cautious at one end of the spectrum to the most naïve. As Colorado Senator Wayne Allard pointed out, “identity theft is something that [people] believe will never happen to them . . . [h]owever, according to the Federal Trade Commission, in
[the year] 2004, [there were] 246,570 people [who] suffered from a stolen identity.”

Once a criminal obtains a copy of your credit card or bank statements or any other record that has your name, address, and even a phone number on it, the criminal’s job becomes much easier. The failure to properly discard identification documents is merely helping the criminal succeed in becoming, in essence, you.

The FACT Act sets out provisions in its seven major titles: Identity Theft Prevention and Credit History Restoration, Improvements in Use of and Consumer Access to Credit Information, Enhancing the Accuracy of Consumer Report Information, Limiting the Use and Sharing of Medical Information in the Financial System, Financial Literacy and Education Improvement, Protecting Employee Misconduct Investigations, and Relation to State Laws. These Titles added extra protection and precautionary measures to try and deter the possibility of identity theft and securing personal information.

The first Title of the FACTA Act contains terms that primarily deals with the prevention of identity theft. In part, the Act launched new regulations relating to fraud alerts and active duty alerts, requiring the credit bureaus, obviously, upon the request of the consumer, to place a fraud alert on their profile for at least ninety (90) days. If a consumer suspects they have been a victim of identity theft, they can place an alert on their credit file, which essentially alerts potential creditors as well. Once the consumer places the alert on their file, the credit reporting agency shares the information with the other two nationwide credit reporting agencies. Recognizably, Equifax, Experian and TransUnion are the three (3) major credit reporting agencies.

---

Furthermore, in the effort of protecting personal information, this Title created new restrictions that prohibit companies from printing more than five (5) digits of any customer’s credit card number on receipts. Also, it recommends new regulations to be established by certain government agencies regarding the detection of identity theft by financial institutions and creditors.\footnote{Id.}

The second Title lays out provisions dealing with improvements in use and consumer rights of accessing their credit information. Until recently, consumers did not have access to their credit scores and had to pay about ten (10) dollars to get a copy of their credit report. With the FACT Act provisions now in effect, consumers may request a credit score including an explanation of the factors that went into computing the score. Moreover, credit reporting agencies have an obligation to give identity theft victims a notice of their rights. This includes notice of: (1) the right to file a fraud alert, (2) the right to block information in a report that resulted from fraud, and (3) the right to obtain copies of documents used to commit fraud.\footnote{The Fair and Accurate Credit Transactions Act: Consumers Win Some, Lose Some. \url{http://www.privacyrights.org/fs/fs6a-facta.htm} (last visited March 3, 2009).}

Additionally, because identity thieves are not afraid to get their hands dirty and are privy to the practice of “dumpster diving” which ultimately gives them a goldmine of personal data, the FACT Act requires any consumer reporting agency or business that uses a credit report must implement procedures for proper document disposal. This requirement will help to ensure that sensitive personal data is not simply left in a trash dumpster once a business no longer needs the information. We have seen several instances of companies improperly and recklessly disposing of or losing records they no longer need. For example, just last year a security breach, occurred at the Bank of New York Mellon where it was reported twelve (12) million customers had their
personal information, including their names, addresses, Social Security numbers and possibly bank account information stolen, lost or displayed.25

The third Title encompasses the concept of consumers being able to dispute inaccurate information detailed on their credit report. Normally, when creditors and other businesses access a person’s credit report, that company believes the data is generally accurate. Despite the fact that the successful stockbroker is at the car dealership, intensely and irresolutely deciding between the black or silver SUV in celebration of his daughter’s 16th birthday, someone with impeccable credit history is not expected to be turned down for a loan. However, one in four credit reports contain errors serious enough to cause consumers to be denied credit, a loan, an apartment, or even a job.26

The fourth Title focuses on limiting the use and sharing of medical information in the financial system and the confidentiality of an individual’s medical contact information. Because the privacy of medical information is a top priority among people today, the FACT Act set out standards that forbid consumer reporting agencies to disclose the name, address, or phone number of any medical creditor unless the information is in codes that are not identifiable. This provision was enacted because it was found that over half of the collection debts reported are for medical debt. When an individual’s credit report is being reviewed, the medical facility who reported the debt also appears and could inadvertently reveal the consumer’s medical condition.27

Title fifth Title of the FACT Act works to improve the financial literacy and educational improvement of consumers. It simply states that a commission will meet once every four (4) months for the purpose of improving the financial literacy and education of consumers. The provision suggests that certain members be involved in the commission, such as the Secretary of Treasury and heads of the Federal Banking agencies. It also described the individual duties of each and goal of taking any necessary actions to streamline and improve the financial literacy education programs or materials of the Federal Government.  

Recently, in February of this year, folders with personal information for numerous clients of a California mortgage broker were overflowing in a bin for days at a public recycling site. The files contained bank account statements, completed tax forms, credit reports, and Social Security numbers. California law clearly states: “A business shall take all reasonable steps to destroy, or arrange for the destruction of a customer’s records within its custody or control containing personal information which is no longer to be retained by the business.” The irresponsible behavior should be addressed by prosecuting the business owner to the fullest extent with the maximum fines and penalties, in the hopes of getting the message across to other business owners. The message relaying that, essentially, people’s lives and identities are in these businesses’ control; therefore, they must secure and protect it as if it were their own.

Finally, the last two (2) Titles, Protecting Employee Misconduct Investigations and Relation to State Law deal with making it understandable that employers do not have to get permission to perform a misconduct investigation. This provision is extremely significant to employers because it liberates them from following the FCRA’s exacting consent and disclosure

requirement when they take on third parties to investigate workplace conduct. Before this provision came into effect, if it was an in-house investigation, employers had to give the employee notice. The same was true when employers hired outside entities to investigate. Employers risked violating the FCRA’s requirements if they failed to inform the employee and obtain their consent. Protecting Employee Misconduct Investigations essentially translates into your employer is not required to give notice or get permission to conduct an in-house misconduct investigation.

However, nowadays this does not apply if a third party is sought to conduct the investigation. For the most part, an employer’s disclosure of an employee’s consumer report could compromise their privacy rights and even their safety interests. After all, the employee already consented to a credit or background check when they were initially hired. The scope of their consent did not extend to the employer disclosing their personal information to outsiders, especially behind their back. Therefore, adding this regulation makes it safer for the individual and their interests.

Conversely, this provision could make it more difficult for employers to conduct investigations and crack down on misconduct because not all companies have the resources to carry out an in-house investigation and are not as skilled as third party investigation companies. Also, if an employer were to approach a miscreant employee and alert them that they are about to be the center of a misconduct investigation, the employee is most likely going to shape up before he potentially gets shipped out.

31 Id.
32 Id.
Finally, the last Title, Relation to State Law, put forward the notion that this provision does not annul, alter, affect, or exempt any person subject to the provisions of this Title from complying with the laws of any State . . . except to the extent that those laws are inconsistent with any provision of this Title, and then only to the extent of the inconsistency.” 33 This language strongly suggests states may enact other identity theft laws, so long as they are not inconsistent with other provisions of the FCRA. 34

**Identity Theft and Assumption Deterrence Act**

The other major Act governing identity theft is The Identity Theft and Assumption Deterrence Act of 1998 (“ITADA”), is an amendment of title 18, United States Code. ITADA went into effect on October 30, 1998 and established identity theft as a federal crime. It also added identity theft as an offense carrying a punishment of a fine or imprisonment with a maximum sentence dependent on certain factors. 35 Additionally, this Act recognized and selected the Federal Trade Commission (the “FTC”) as a clearinghouse for complaints and consumer information. 36

Procedurally, any violations of ITADA are inspected by several agencies ranging from the Federal Bureau of Investigations (the “FBI”), the U.S. Secret Service, the U.S. Postal Inspection Service, the Social Security Administration’s Office of the Inspector General, and the Treasury Inspector General for Tax Administration. In the end, The Department of Justice prosecutes the cases. 37 ITADA reads in part as follows,

---

33 Id.
36 Id. at 11
37 Id. at 12
Whoever... 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; shall be punished as provided in subsection (b) of this section.\textsuperscript{38}

ITADA addresses identity theft in two significant ways. First, the Act strengthens the criminal laws that are governing identity theft. Second, the Act addresses the problem of identity theft by focusing on consumers as victims.\textsuperscript{39} The latter way is mostly handled by the FTC, who not only plays the role of facilitator between the victims and the government agencies, they also must adopt procedures to (1) log the receipt of complaints by victims of identity theft; (2) provide identity theft victims with informational materials; and (3) refer complaints to appropriate entities, including the major national consumer reporting and law enforcement agencies.\textsuperscript{40}

As previously mentioned, the FTC plays this role because they are considered the clearinghouse for the complaints that trickle in by the consumers. Accordingly, their role is primarily one of facilitating information sharing among public and private entities.\textsuperscript{41} When a victim of identity theft becomes aware of what has happened to them, if any comfort is involved, it would seemingly stem from the victim not having to deal directly with the entities that may have put them in this situation to begin with. Therefore, the comfort of being slightly relieved of this stress and anxiety is placed on the shoulders of the FTC.

\textbf{Florida Law}

Each state contains their individual identity theft laws to regulate this crime. For example, Florida \textit{Fla. Stat. Ann. § 817.568} states,

\footnotesize{\begin{itemize}
\item \textsuperscript{38} Id.
\item \textsuperscript{40} Id.
\item \textsuperscript{41} Id.
\end{itemize}}
Any person who willfully and without authorization fraudulently uses, or possesses with intent to fraudulently use, personal identification information concerning an individual without first obtaining that individual’s consent, commits the offense of fraudulent use of personal identification information, which is a felony of the third degree . . .

Some of the infamy of identity theft rose with media coverage of the hazards of buying and selling on the Internet. However, the most common ways that offenders steal identities are primarily low-tech methods, with some more popular than others. Identity thieves will steal wallets or purses from shopping bags, cars, or by pick pocketing. It’s amazing how fast it can happen to anyone. On a personal note, recently I was shopping in Target in Miami Lakes when suddenly police officers rushed through the front door in response to a woman’s purse stolen from her shopping cart. After much questioning and review of video surveillance tapes, the police found the purse in the back of the store with all of the contents of the purse still there, except the driver’s license and credit cards were missing. Who knows what the thieves’ intentions were in this unfortunate situation, but this is just a mere instance of how fast and unexpected identity theft can potentially occur.

Another facet of thievery is stealing mail. Thieves may simply take it from insecure mailboxes, submit a false change-of-address form to the post office to direct someone’s mail to themselves, or collude with a postal employee to steal mail that contains personal information. Mail that is valuable to a crook includes pre-approved credit card applications, energy or telephone bills, bank or credit card statements, and convenience checks. They obtain these items by rummaging through trash cans or through business dumpsters.

---


"Supported by our tougher identity theft laws, we will continue to prosecute those who commit this form of unarmed robbery." This statement was made by Florida Governor, Charlie Crist in response to the discovery of two (2) brothers from Hillsborough County, Florida who participated in an identity theft scheme to defraud gas stations in two (2) counties. The men used counterfeit credit cards that contained stolen personal identification information from ten (10) victims. The brothers used the credit cards to steal gas from commercial gas stations by pumping diesel fuel into fuel bladders concealed in modified pick-up trucks.\footnote{General of Florida Bill McCollum: News Release (2006) \url{http://myfloridalegal.com/newsrl.nsf/newsreleases/72D8EBAB2FD8C5D4852571D900665C31} (last visited March 16, 2009).}

In March of 2009, the Miami Police publicly recognized identity theft as “becoming a huge problem.” They also reported they have recently confiscated over fifty (50) stolen credit cards. This statement was made after an incident involving a sixty-three (63) year old woman who placed her pocketbook under her car seat and ran inside a gas station. During those few minutes, thugs smashed her car windows and stole her personal belongings. Within twenty-four (24) hours, thieves attempted to withdraw $2000 dollars from the victim’s personal bank account. Luckily, the thieves were caught and during the arrest, the suspect had in his possession, fifty-five (55) credit cards and a couple of different check books.\footnote{WSVN Channel 7 News Miami/Ft. Lauderdale: Police Warn Public of Identity Theft: (2009) \url{http://www.wsvn.com/news/articles/local/M1114864/} (last visited March 16, 2009)}

Furthermore, the Identity Theft Data Clearinghouse issued a report in 2003 ranking the major metropolitan areas for identity theft. Miami, Florida was ranked number four (4) with 2,871 reported victims.\footnote{Identity Theft Data Clearinghouse: Major Metropolitan Areas Ranking for Identity Theft (2003) \url{http://www.consumer.gov/sentinel/pubs/IDT%20Reports%20for%20Top%2026%20MSA.pdf} (last visited March 16, 2009).} Just within Miami itself the number one (1) ranked type of identity theft was credit card fraud with a reported 1,001 victims.\footnote{Id.} Coming in at the number two (2) spot
was bank fraud with 508 victims.\textsuperscript{48} Phone and utilities fraud fell into the third ranking category with 497 victims.\textsuperscript{49} These are only a few of the types of identity theft reported by the victims.

\textbf{Thieves At Work}

Thieves can obtain people’s credit reports by posing as someone who is legally permitted to do so, such as a landlord or an employer. Some thieves have the audacity to conspire with or bribe employees of businesses, government agencies, or service organizations, such as hospitals and HMOs, to obtain personnel or client records. If the thieves are themselves employees, they can access the information at work.\textsuperscript{50} Thieves can also hack into corporate computers and steal customer and employee databases, then sell them on the black market.\textsuperscript{51} Some thieves even buy identities on the street for the going rate of about twenty-five ($25) dollars, or buy credit cards that may be either counterfeit or stolen.\textsuperscript{52} Other items up for sale are birth certificates, visas, and passports.\textsuperscript{53} In 2001, the U.S. Immigration and Naturalization Service intercepted over 100,000 fraudulent passports, visas, alien registration cards, and entry permits. Thieves buy these fake and counterfeit IDs on the Internet for as little as fifty dollars ($50) dollars.\textsuperscript{54} All the technology for reproducing plastic cards, including their holograms and magnetic strips, can easily be

\textsuperscript{48} Id.
\textsuperscript{49} Id.
\textsuperscript{51} Id.
\textsuperscript{52} Id.
\textsuperscript{53} Id.
\textsuperscript{54} Id.
purchased on the Internet. There is even special software for criminals to purchase and steal pin numbers or user ID login information.

Furthermore, thieves trick individuals using the Internet into giving their passwords and other personal information, which is known as phishing. Another method thieves are using is to watch users punch in their pin numbers on telephones or at ATM’s. With the use of one single stolen ID, thieves can obtain legitimate IDs that can be used for a wide variety of additional fraudulent activity. They gain entry into ID-issuing agencies, such as motor vehicle departments, by using bribery or extortion, or posing as employees.

In this cyber age, people enjoy surfing the internet and benefiting from the information highway, especially when responding to advertisements or solicitations. However, during this email interaction, they unknowingly become victims to the identity theft process. Their acquiescence to the criminal’s request provides the criminal with their personal information. Moreover, even if the evil persuasion and inducement by the criminal can be lacking, the criminal may continue his prowl by using programs that allows them to track and record the information a person keys into a computer. The criminal can ultimately obtain personal data just by another person’s mere click onto a website link. It is then tracked and recorded and eventually aids the criminal in securing the personal information and obtaining the password or banking information that person has entered. This type of information has become most appealing to the criminal, and victims who are computer illiterate or who nonchalantly explore the internet without any concern or awareness of this potential crime happening to them are especially vulnerable.

55 Id.
56 Id.
57 Id.
The latter are only a few ways one can strip the credit history, dignity, and identity of another. However, the following is a summary of ways listed by the FTC on how a thief can steal your identity.

**Dumpster Diving.** They rummage through trash looking for bills or other paper with your personal information on it.

**Skimming.** They steal credit/debit card numbers by using a special storage device when processing your card.

**Phishing.** They pretend to be financial institutions or companies and send spam or pop-up messages to get you to reveal your personal information.

**Changing Your Address.** They divert your billing statements to another location by completing a change of address form.

**Old-Fashioned Stealing.** They steal wallets and purses; mail, including bank and credit card statements; pre-approved credit offers; and new checks or tax information. They steal personnel records, or bribe employees who have access.

**Pre-texting.** They use false pretenses to obtain your personal information from financial institutions, telephone companies, and other sources.\(^5\)

As noted by the FTC, identity theft starts with the misuse of your personal information such as your name and Social Security number, credit card numbers, or other financial account information. For identity thieves, this information is as good as gold. Skilled identity thieves can use the aforementioned methods to obtain your information. Once it is in their hands, this is where the chaos begins, the chaos that one may be oblivious to until they receive a collection notice in the mail, or the continued denial of school loans or mortgage approvals. Once the information falls into the hands of a criminal, they have several options of taking advantage of being “you.”

**Making a Comeback**

Once an individual has become victim of identity theft, the time effort and patience it takes to rebuild their life is priceless. The FTC estimates that as many as nine (9) million

---

\(^5\) Federal Trade Commission: Fighting Back Against Identity Theft
Americans have their identities stolen each year. The Identity Theft Resource Center noted that identity theft victims spend on average about $1500 and expend 600 hours of time to restore their credit histories after they realize what has happened to them. To assist with some precautionary and preventative measures, Congress enacted The Gramm-Leach-Bliley Act which requires any company defined under the law as a “financial institution” to implement policies and procedures to maintain the security and confidentiality of “nonpublic personal information.” This was known as the Safeguards Rule. The “nonpublic personal information” was considered to be any stored personal information of customers, employees or vendors including driver license numbers, Social Security numbers, Federal Tax ID numbers, medical information, dates of birth, addresses and more.

The country’s current recession, high unemployment rates, and overall economic state gives rapid rise to identity theft, which means it is important for one to learn how to protect themselves by adopting simple preventative habits. The DOJ recommends being “stingy” on giving out your personal information. When a company asks you for your Social Security number for security or verification purposes, it is sufficient for you to provide them with only the last four (4) or even six (6) numbers rather than the entire number.

If a stranger calls and offers you the chance to receive a major credit card, a prize, or other valuable item, but asks you for personal data, such as your Social Security number, credit card number, expiration date, or mother's maiden name, ask them to send you a written

59 Id.
62 Id.
application form. If they won't do it, tell them you're not interested and hang up. Keeping track of your account statements is imperative in monitoring and maintaining your credit and identity. If a bank or credit card statement has not come in the mail as is normally expected, this in itself should prompt an inquiry to the financial institutions to resolve the matter. Receiving a copy of your credit report on a regular basis is another important factor in helping to maintain one’s reputation, credit and identity.

The Better Business Bureau also offers several safety tips that can protect consumers from identity theft. Individuals can safeguard their identity by not releasing their social security or account numbers in response to any e-mail, phone, or in-person requests. Keep all sensitive documents, checkbooks and credit cards securely locked away at home, only carry the credit cards you frequently use and never carry your social security card in your wallet.

Furthermore, it is important to shred all documents containing your personal data. Another important safety measure is enrolling in payroll direct deposit and e-mail notifications of any changes to your accounts. Also, steer away from receiving paper statements. In essence, some may find this much more convenient than sorting through collections of mail. Moreover, keeping passwords hidden, even in your home and changing them periodically is important. Discard, erase and completely destroy all of your personal data before deciding to throw away your old desktop for a new laptop.

Reviewing bank and credit card statements weekly, accessing and managing accounts online, and reviewing credit reports regularly are some safeguards and extra precautionary measures which should be taken. When traveling, call your financial institution’s fraud

---

65 Id.
66 Id.
department and let them know you will be away in those certain areas, therefore, if there is any suspicious activity occurring while you are on travel, the financial institution will be on alert.

Victims of identity theft have had emotional, social, and financial impacts that often resulted in a loss of job opportunities, denial of loans for school, housing, or cars because of poor credit scores and negative information on their credit reports from the identity theft. It is important to be aware and follow the safeguards to help prevent, protect, and prepare one for the potential of this fast growing crime of happening not only to the man on the news, or the lady next door, but that it can happen to anyone.

On An “Entertaining” Note

Thieves do not discriminate. Steven Spielberg, Oprah Winfrey, Paris Hilton, Ted Turner and Martha Stewart are some of several Hollywood entertainers that have fallen victims to identity theft. In March of 2001, police called it one of the most ambitious identity theft scheme they have seen when Abraham Abdullah, a busboy at a restaurant posing as his victims, obtained Social Security numbers, credit card numbers and all vital financial records to contact their banks and brokerage firms. Abdallah obtained this information from a dog-eared copy of a Forbes "400 Richest" article, with notations of Social Security numbers, home addresses and birth dates of 200 chief executives, celebrities and tycoons. They say he also had more than 400 stolen credit card numbers, one of them belonging to a Federal Prosecutor. Abdallah used computers at a library, web-enabled cell phones, virtual voicemail and hired couriers, duping credit reporting companies such as Equifax into providing detailed credit reports on his victims.

---

68 Id.
69 Id.
70 Id.
Actor Will Smith was a victim of identity theft when Carlos Lomax opened fourteen credit accounts using Will Smith’s legal name, Willard C. Smith. The thief charged over $30,000 dollars to the fake accounts. Lomax was previously convicted of using the identity of Atlanta Hawks basketball player Steve Smith to rack up $81,000 worth of charges on a credit card account.\textsuperscript{71}

New York Mayor Michael Bloomberg found himself the victim of identity theft when Odalis Bostic and Charles Nelson made off with $10,000 dollars using phony checks.\textsuperscript{72} The two were nabbed after attempting to cash a $400,000 dollar check. American Idol’s Rubin Studdard’s ex-manager and Public Relations director, Ronald Edwards racked up $275,000 dollars using the singer’s personal information to take out credit cards, deposit checks and purchase goods and services.\textsuperscript{73} Other celebrity victims include Mel Gibson, Barry Bonds, Tiger Woods, Christina Aguilera, Lindsey Lohan, and Ross Perot. Unfortunately, because of their high profiles and continuous presence in the spotlight and media, celebrities may be more vulnerable to identity theft.\textsuperscript{74}

\textbf{Conclusion}

Identity theft it is a silent crime that has become an increasingly common occurrence for numerous individuals and families. Victims of identity theft experience countless days of frustration and helplessness in efforts to fix and repair their identity, yet it only takes a few steps to thwart this turmoil from the beginning. Sadly, there are still some families who ignore or do not know how to guard themselves from identity fraud. Some people are insensible that it can

\textsuperscript{72} Id.
\textsuperscript{73} Id.
\textsuperscript{74} Celebrity ID Theft Common Traits To You. (2005). \url{http://idtheftsecrets.blogspot.com/2005/12/celebrity-id-theft-common-traits-to.html} (last visited April 8, 2009).
and may happen to them. Unfortunately, while pieces of their life, years of hard work and dignity can suddenly be stripped away from them, somewhere there is a criminal profiting at their expense.

Congress must continue to enact legislation and be involved in protecting individuals from this horrific experience. Legislation to effectively scrutinize and manage this white collar crime may at least make it more difficult for a thief to illegally obtain another’s personal information. In the event thieves get hold of the information, the legislation enacted will help rectify the problem more quickly and efficiently. Furthermore, enacting legislation to force companies to be more careful with one’s personal information and implementing fines or penalties, will provide more safeguards and protection for the privacy of an individual’s information. Moreover, increasing the amount of free access to an individual’s credit report will empower them to monitor their credit more frequently to deter or halt identity theft from the start.

In the hearing before the Committee on Banking, Housing and Urban Affairs of the United States Senate, Senator Jack Reed of Rhode Island stated, “we live in a time when proliferation of information through various electronic modes of exchange offers extraordinary opportunities to reshape our culture and our economy, but the down side, of course, is we open ourselves up to the exploitation of that information by criminals and by others.” However, with today’s laws and advanced technology designed to protect identity theft, it is making the thief work a little harder for their . . . well . . . your money.

So, as you get ready to give your personal information to the meek receptionist at the doctor's office, or your check to the mousy cashier at the mall, or your credit card and tip to your

favorite waiter, be conscious that identity theft is always lurking in any size shape or form. It is imperative that we operate under a heightened sense of awareness and proactively take not only precautionary measures, but extraordinary precautionary measures every day, anytime, and everywhere.