IDENTITY THEFT: FACTS, FICTIONS, AND FORECASTS

DAN DAVIDSON*
WAYNE SAUBERT**

I. INTRODUCTION

Identity theft is, allegedly, a major problem that is getting much worse annually. While there can be little doubt that the problem exists or that the number of occurrences has increased over the past decade, there is considerable doubt that the situation is as dire as it is so often portrayed.[270] However, there is also little doubt that the problem can be minimized, if not totally avoided, assuming the potential victims address it in a reasonable and rational manner.

This paper will address the issue of identity theft, including the estimated number of victims and the annual losses caused by such conduct. It will also address some of the more important legislative actions designed to reduce the risk posed, and several of the cases that have involved identity theft. Finally, it will include a discussion of some recommendations for preventing or minimizing the risk of becoming a victim of this crime.

II. THE FEAR FACTOR

The concern about identity theft has become serious enough that the Solicitor General of Canada and the Justice Department of the United States have issued a joint Special Report to advise the public of the seriousness of the problem, along with current trends and developments in the law dealing with the issue.[271] This Special Report begins by defining the issue, stating that: "Identity theft refers to all types of crimes in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain."[272] (This is a *very* broad definition that encompasses a myriad of torts and crimes. A narrower definition that focuses on *identity* theft rather than *data* theft is included later in this paper.) The report then goes into some detail about the number of cases that have been reported in each of the two countries. According to this report, the PhoneBusters National Call Center in Canada received 7,629 complaints about identity theft in 2002, with total reported losses of more than $8.5 million, and an additional 2,250 complaints in the first quarter of 2003, with reported

* J.D., Professor of Business Law, Radford University.
** J.D., M.Acty, Associate Professor of Accounting, Radford University.
[270] *See, e.g.*, Associated Press, *Identity Theft May Be Hyped*, THE ROANOKE TIMES, Nov. 11, 2005.
[271] *Public Advisory: Special Report for Consumers on IDENTITY THEFT*, SPECIAL REPORT FROM THE DEPARTMENT OF SOLICITOR GENERAL OF CANADA AND THE UNITED STATES DEPARTMENT OF JUSTICE, www.specp-sppcc.gc.ca/pulbications/policing/Identity_Theft_Consumers. (last visited March 2, 2006).
[272] *Id.*

losses of more than $5.3 million.[273] Meanwhile, the Federal Trade Commission reported a 500% increase in identity theft reports from 2000 through 2002, with complaints increasing from 31,117 in 2000 to 161,819 in 2002.[274]

The Better Business Bureau, in conjunction with Javelin Strategy and Research, conducted a follow-up survey[275] updating the FTC's 2003 Identity Theft Survey Report.[276] The results of the Javelin/Better Business Bureau survey were released January 26, 2005. The survey showed that:

- Within the previous twelve months some 9.3 million Americans were victims of some form of identity theft;
- The total cost to the U.S. economy due to identity theft fraud was $52.6 billion for the year, virtually unchanged from the $51.4 billion reported by the FTC in 2003 (adjusted for inflation);
- Most identity thieves obtain personal information on their victims by "traditional" methods such as finding or stealing a wallet or checkbook, theft of mail, and "dumpster diving" rather than through electronic channels.

The FTC report from 2003 had previously reported that:

- 27.3 million Americans had been victims of identity theft over the previous five years, with 9.9 million people (4.6% of the population) being victims in the previous year;
- 3.23 million consumers (1.5% of the population) discovered that new accounts had been opened, or some other fraud (e.g. renting an apartment, obtaining medical treatment, or obtaining a job) had been committed in their names, while 6.6 million had existing accounts compromised by an identity thief;
- 15% of victims reported that their personal information had been misused in non-financial ways, such as obtaining government documents or in the completion of tax forms;
- 52% of all identity theft victims discovered that they had been victimized through monitoring their accounts.

The number of victims reported and the costs associated with identity theft are obviously causes for concern, and steps need to be taken to reduce the risks and losses occasioned by the crime. However, while it is apparent that there is a reason for concern, the media and the credit industry have significantly contributed to the public perception that identity theft is a matter of *grave* concern. For example, the lead paragraph in a story originating in *The Miami Herald* reports that:

> A growing outcry over security breaches at giant information brokers – coupled with the growing sophistication of scammers – is jolting consumers with a grim threat: They're more vulnerable than ever to identity theft.[277]

[273] *Id.* (The report did not state whether these losses were in Canadian dollars or U.S. dollars. Since the Canadian dollar is worth approximately $.85 U.S., this could be a significant difference in the total amount lost.)
[274] *Id.*
[275] *2005 Identity Fraud Survey Report*, JAVELIN STRATEGY & RESEARCH AND BETTER BUSINESS BUREAU, http://www.javelinstrategy.com/reports/2005IdentityFraudSurveyReport (last visited March 2, 2006).
[276] *Federal Trade Commission –Identity Theft Survey Report*, Sept. 03, www.ftc.gov/os/2003/09/synova tereport.pdf (last visited March 2, 2006).
[277] *Congress Examines Identity Theft Threat*, THE ROANOKE TIMES, March 10, 2005, p. A5.

In a similar vein, *Credentials*, a newsletter from a credit monitoring service, reports that "the incidence of identity theft is increasing. The number of identity theft victims who reported the misuse of their personal information has almost doubled over the past 2 years. In the past year alone approximately 10 million Americans discovered they have been victims of identity theft."[278] American Express claims that "identity theft is a rapidly escalating crime that can potentially damage your credit and good name."[279] This American Express release goes on to cite the Federal Trade Commission's statement that "referred to identity theft as the fastest-growing white-collar crime in America" in a notice sent to its cardholders.[280] Even *Parade*, the Sunday supplement newspaper insert/magazine has addressed the issue, and in an alarming manner, asserting that "[d]ue to stunningly widespread corporate carelessness, the records of more than 46 million Americans were lost or stolen in the first half of 2005 alone."[281]

One source asserts that the total cost of identity theft is approaching fifty billion dollars a year in the United States, with the average victim losing $4,800 and needing to spend an average of 240 hours repairing the damage to his or her credit.[282] American Express issued a newsletter to its customers in which it cited the FTC's statement that identity theft is the fastest-growing white-collar crime in America, with more than 27 million Americans being victims of such theft in the past five years, and 9.9 million of those being victims in the previous year.[283] These shocking numbers in the newsletter immediately preceded an offer from American Express to provide *Identity Protection* for cardholders who signed up for this new program, at a cost of $5.95 per month or $59.95 per year, conveniently charged to the customer's American Express account.

There have been numerous reports of computer hackers who have gained access to customer data, and of the potential havoc that such access might cause for those consumers whose identity is subsequently stolen as a result of these hackings. For example, ChoicePoint, the largest information broker, issued a warning to 145,000 people in February 2005 that criminals posing as small businesses had gained access to the personal data of these people. At least 750 people were, in fact, defrauded due to this breach, and the state of California estimated that as many as 400,000 were potentially at risk due to the compromise of their data.[284] LexisNexis announced March 9, 2005, that intruders had managed to gain access to information on as many as 32,000 U.S. citizens by improperly accessing the databases of Seisnet, a subsidiary of LexisNexis.[285] The stolen data included Social Security numbers of the victims.

Because of these and similar occurrences, Congress is considering legislation that would increase the authority of the Federal Trade Commission to enact regulations mandating minimum security standards and improved privacy protection, especially by the various data-collection companies and agencies.[286]

---

[278] *Identity Theft Protection*, CREDENTIALS, YOUR CREDIT MONITORING SERVICE, Volume 3, Issue 2 (citing data from the 2003 Identity Theft Survey Report sponsored by the Federal Trade Commission and prepared by Synovate *at* www.synovate.com).

[279] *When Identity Theft Strikes, Protect Your Good Name*, IDENTITY PROTECTION, American Express (citing data from a 2002 "FTC 'Consumer Alert'" and the FTC Identity Theft Survey Report of 2003).

[280] *Id.*

[281] *How to Guard Your Identity*, PARADE, July 31, 2005, p. 4.

[282] *Supra* note 4.

[283] *Supra* note 5.

[284] *Congress Examines Identity Theft Threat*, ROANOKE TIMES, Mar. 10, 2005, at A5.

[285] *Id.*

[286] *Id.*

III. PHISHING AND PHARMING

One of the most common methods of acquiring confidential information from a person involves "phishing." According to Webopedia,[287] "'phishing' (also known as *carding* and *spoofing*) is "the act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft."[288] Phishing often involves an apparently valid email from a person's bank or credit card issuer. The email often alleges that the bank or credit card issuer is verifying certain data in the course of a routine audit or computer upgrade, and asks the recipient to verify certain data. The data to be "verified" normally includes the recipient's PIN and password, as well as the accuracy of the account number and the name on the card. The request will also, on occasion, request the person's city of birth and/or mother's maiden name, again for purposes of verification. The unsuspecting "phish" clicks on the reply button and provides the requested information. Unfortunately for the "phish," the email originated with a person or person who have no connection with the bank or the credit card issuer; rather, the person who placed the request in the original email is an identity thief and the "phish" has just provided him or her with enough information to access the account about which the information was requested, or to open new accounts in the name of the "phish," obviously for fraudulent purposes.

If a phisher obtains credit card information, he or she can use the information to make credit card purchases online or by telephone. This carries some risk to the victim, but the statutory limitations on credit card liability for unauthorized use offer a shield to the victim, provided that he or she properly monitor the account and notify the credit card issuer as soon as the unauthorized use of the card is reflected on a monthly statement. However, phishers also gather information on debit cards, and in this circumstance the accessing of the victim's account may be more direct. Once the phisher acquires the account number and the PIN, he or she can simply reproduce this information on a *white card*, a blank white plastic card that looks like a credit card, and then use this card to access the account of the victim via ATM, as well as online or by telephone. Encoding machines that will implant the information on the back of such white cards are readily available on the Internet, selling for as little as $50.[289]

One thing that has been of tremendous help to white card users is the lax ATM security approach taken by the banking industry, at least until recently. Every ATM card has a hidden three-digit code, known as either a CVV (Card Verification Value) or a CVC (Card Verification Code), which identifies the card issued by the bank. Unless the ATM can read and verify this three-digit code, the ATM should not allow access to the account with the card. However, until recently many, if not most, banks did not bother to activate or use this feature of their ATMs, assuming that when a debit card was inserted into an ATM and the correct PIN was entered that the person using the card was an authorized user.[290] As a result of this oversight, it is estimated that as much as $2.75 billion was stolen from banks (via improper access to some three million accounts) by means of ATM and debit card fraud from mid-2004 to mid-2005.[291]

Phishers also use "Trojan horses" in emails as a means of accessing a person's information. A Trojan horse, in computing terms, is "a destructive program that masquerades as a benign

[287] Webopedia is an online encyclopedia dedicated to computer technology. It can be accessed at http://www.webopedia.com.

[288] Webopedia Computer Dictionary, *What Is Phishing?* Jupitermedia Corp., ¶ 1 (2006), http://www.webopedia.com/TERM/p/phishing (last visited March 2, 2006).

[289] B. Sullivan, *ATMs May be an Easy Target for Thieves*, MSNBC.com, Aug. 10, 2005, http://www.msnbc.msn.com/id/8743446/&&CE=3032091 (last visited March 2, 2006).

[290] *Id.*

[291] A. Litan, *Gartner Says ATM/Debit Card Fraud Resulted in $2.76 Billion Loss in Past Year*, THE GARTNER REPORT, Aug. 2, 2005, http://www.gartner.com/press_releases/asset_133138_11 (last visited March 2, 2006).

application."[292] Some Trojan horses are malicious, designed to delete programs or otherwise disrupt the computer owner's ability to use his or her computer. But more recently a number of Trojan horses have included spyware ("any software that covertly gathers user information through the user's Internet connection without his or her knowledge, usually for advertising purposes"[293]) which may include the ability to monitor the targeted computer and relay any information gathered to another party. The spyware may monitor keystrokes, allowing the other party to obtain passwords or encryption codes from the targeted computer, thus bypassing its security system. Spyware may also provide a backdoor that allows the person sending the Trojan horse to access the recipient's computer and use it as his or her own from a remote location. Such usage can result in the theft of hundreds of identities. For example, in March 2005, Brazilian police arrested an alleged "phishing kingpin" who reportedly had stolen between $18 and $37 million over the previous two years by using a Trojan horse hidden in emails to access confidential information from recipients of the emails. Police estimated that the "kingpin" and his gang sent more than three million emails containing the Trojan horse each day.[294] With more than three million emails sent daily, even a small percentage of successful installations of the software would result in a very large pool of potential victims of this Trojan horse plan.

A similar means of stealing an identity involves "pharming," in which the thief redirects Internet traffic to fake websites with the intention of garnering confidential information from the victims. As defined by Webopedia, "pharming seeks to obtain personal or private (usually financial related) information through domain spoofing."[295] The phony (*spoofed*) website to which the victim was directed normally looks like the intended website, and the unsuspecting customer places an order, providing his or her personal information to the pharmer, who is then able to use the information for his or her own illegal purposes. While less prevalent than phishing, the results can be just as devastating to the victim. There is a growing concern that the increase in phishing and pharming activities may lead to a reduction in public trust of the Internet, with a resulting decrease in e-commerce.[296]

While the number of complaints received and the dollar value of the losses reported sounds impressive, do these figures provide evidence of a pervasive crime wave or a system in dire straits? If so, what is being done about the problem? If not, why has this crime received so much media attention when other crimes, unless they are particularly heinous, do not attract as much attention and concern? These are a few of the questions to be addressed below.

IV. HOW WIDESPREAD IS THE PROBLEM?

Despite all the attention paid to online fraud and identity theft, it appears that the problem does not quite live up to the hype. While there is, admittedly, a problem with identity theft, the number of victims reported is probably misleading. One reason for this is the very broad definition of identity theft: "Identity theft refers to all types of crimes in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain."[297] This definition would include, for example, a person who found a gas

[292] Webopedia Computer Dictionary, *What Is Trojan Horse?* Jupitermedia Corp., ¶ 1 (2006), http://www.webopedia.com/TERM/T/Trojan_horse.html (last visited March 2, 2006).

[293] Webopedia Computer Dictionary, *What Is Spyware?* Jupitermedia Corp., ¶ 1 (2006), http://www.webopedia.com/TERM/S/spyware.html (last visited March 2, 2006).

[294] J. Leyden, *Brazilian Cops Net "Phishing Kingpin*," CHANNEL REGISTER, Mar. 21, 2005, http://www.channelregister.co.uk/2005/03/21/brazil_phishing_arrest (last visited March 2, 2006).

[295] Webopedia Computer Dictionary, *What Is Pharming?* Jupitermedia Corp., ¶ 1 (2006), http://www.webopedia. com/TERM/P/pharming.html (last visited March 2, 2006).

[296] B. Sullivan, *Data Leaks Stunt e-Commerce, Survey Suggests*, MSNBC.com, June 15, 2005, http://www.msnbc.msn.com/id/8219161 (last visited March 2, 2006).

[297] *Supra* note 1.

company credit card and used that card to get a single tank of gas as an identity thief. A better, and narrower, definition of identity theft can be found in Wikipedia[298], which defines identity theft as "the deliberate assumption of another person's identity, usually to gain access to their finances or frame them for a crime."[299]

Despite the fear of high-tech thieves, often believed to be operating out of Russia, China, or Romania, most victims are likely to know the identity of the person who stole their identity, and to know the method used by the criminal in gaining access to the information. The 2005 Identity Fraud Survey, released by the Better Business Bureau and Javelin Strategy & Research, reports that these crimes are more likely to be committed offline than online.[300] This survey, a follow-up to the FTC's 2003 Identity Theft Survey, also reports that Internet-related fraud is generally less severe, less costly, and, most importantly, less common that is generally thought. As a result, this survey implies that careful and thoughtful protections in day-to-day activities will do a great deal to reduce the risk of losses due to identity theft, and that the emphasis on developing new and better protections for online activities, while worthwhile and valuable, will not eliminate the problem and may not significantly reduce its occurrence.

For those times when careful and thoughtful protections will not suffice there are already some statutory protections available, and others are pending. In addition, safeguards that were already in place but not being used are now becoming standard. For example, the CVC and CVV hidden codes on bank-issued debit cards are designed to notify the ATM that a card is, in fact, a valid card issued by the bank. If neither code is present on the card, the ATM should refuse to honor the card or to allow any transactions, a very strong protection against ATM fraud and theft. However, until recently most banks did not have this feature of the ATM activated, believing that the PIN was sufficient protection. Given the increased use of white cards to access customer accounts (an estimated three million accounts were subject to such unauthorized access from late 2004 through August 2005, at a cost to the banks of approximately $2.75 billion), most of the major banks in the U.S. have now activated this security, with the other banks either already following suit or being expected to in the near future.[301]

In September 2005, the three major credit reporting agencies, Equifax, Experian, and TransUnion announced new standards for their customers to follow in transmitting data. These new standards will require the banks, credit unions, and other financial service firms to use standardized encryption systems or formats when sending consumer data to any of the three agencies. The new encryption standard will be a minimum128-bit rate of encryption, using either the Advanced Encryption Standard or the Triple Data Encryption Standard.[302]

MasterCard and Visa have instituted requirements for the truncation of credit card numbers on customer receipts. Merchants accepting either type of card for payment must truncate the account number, and may not show the expiration date of the card on customer receipts. Visa's requirement went into effect immediately for any credit card terminals deployed after July 1, 2003, with an absolute deadline for compliance of July 1, 2006, for any terminals already in use July 1, 2003. MasterCard required all terminals, new or existing, be in compliance by April 1, 2005.[303] These requirements from Visa and MasterCard satisfy federal and state statutes requiring truncation for

[298] Wikipedia, the Free Encyclopedia is a multilingual free content online user-edited encyclopedia. It can be accessed at http://www.wikipedia.com.

[299] Wikipedia.org, Identity Theft, Wikimedia Foundation, Inc. (2006), http://en.wikipedia.org/wiki/identify_theft (last visited March 2, 2006).

[300] BBB Online, *Identity Theft*, Council of Better Business Bureau, Inc. (2003), www.bbbonline.org/IDtheft (last visited March 2, 2006).

[301] *Supra* note 17.

[302] M. Bosworth, *Credit Bureaus Adopt Unified 'Data Protection' Standard*, Consumer Affairs.com, Oct. 7, 2005, http://www.consumeraffairs.com/news04/2005/data_protection.html (last visited March 2, 2006).

[303] *Credit Card Account Number Truncation*, The Graduate, Inc. (2006), http://www.thegraduate.net/credit-card-account-number-truncation.php (last visited March 2, 2006).

all credit card receipts, but reflect the credit card industry's concern regarding the perception of problems with identity theft.

There are statutory provisions designed to prosecute those persons who commit identity theft, but there does not seem to be much protection provided for the victims, except for traditional legal remedies applied to this new, and occasionally high-tech, crime. In the cases discussed below the courts did not seem to be overly concerned with providing any protection to parties who complained about the release of their confidential information unless and until there was an actual loss due to the theft of an identity. This is an area that may need to be addressed by the legislature in the future as a means of assuaging the concerns of the public, especially if the alternative is a decline in public acceptance and use of e-commerce. In the interim, individuals should exercise as much care with their personal and confidential information as they should exercise with their wallets, purses, and cash.

V. THE GOVERNMENTAL RESPONSE TO THE PROBLEM

The U.S. government obviously recognizes the threat posed to its citizens by identity theft. It has empowered the Federal Trade Commission with the authority to establish a special program to protect people from identify theft. Congress had previously enacted the Privacy Act of 1974 and the Fair and Accurate Credit Transactions Act of 2003 (FACTA), amendments to the Fair Credit Reporting Act intended to help consumers fight identity theft.

In an effort to combat phishing and pharming activities, Senator Patrick Leahy introduced the Anti-Phishing Act of 2005.[304] This bill is intended to complement the identity theft and wire fraud statutes already in effect by providing criminal penalties for either of two acts, 1) knowingly sending "spoofed" email that links to sham websites with the intent to commit a crime, or 2) creating or operating a sham website. Persons convicted of either of these offenses would face criminal penalties of up to five years incarceration and fines of up to $25,000 per offense. The bill also specifically excludes from its coverage parodies and political speech, neither of which would fall within the definition of phishing. Darlene Hooley, a member of the House of Representatives, sponsored the bill (H.R. 1099) in the House.[305] The bill has been read twice on the Senate floor and forwarded to committee for further consideration.

VI. IDENTITY THEFT AND THE COURTS

A search of LexisNexis for cases involving identity theft revealed a total of eleven cases in the past ten years in which the term *identity theft* appears in the court's opinion. From this list, five cases were relevant to the topics discussed herein, and none of the opinions provided much protection to the person claiming that his or her identity had been, or could be, stolen unless the court intervened.

In re Crawford[306]established the foundation for some of these cases. The Crawford court addressed the issue of whether the mandatory inclusion of a person's social security number on court records and documents that would be open to the public was permissible. Jack Ferm, a non-attorney bankruptcy petition preparer did not include his social security number on several documents submitted to the bankruptcy court by two of his clients as required by 11 U.S.C. § 110(c). The court fined Ferm $800 for his failure to include his social security number on the documents, and Ferm appealed, alleging that the imposition of this fine violated his constitutional

[304] Senate bill S.472, introduced Feb. 28, 2005.

[305] Wikipedia.org, Anti-Phishing Act of 2005, Wikimedia Foundation, Inc. (2006), http://en.wikipedia.org/wiki/Anti-Phishing_Act_of_2005 (last visited March 2, 2006).

[306] 194 F.3d 954 (9th Cir. 1999), cert. denied, 528 U.S. 1189 (2000).

rights to privacy and equal protection, and also his statutory rights under section 7 of the Privacy Act of 1974.

The controversy originated when Ferm petitioned the bankruptcy court to allow him to substitute an identification number of some sort in place of his social security number on any bankruptcy petitions he prepared for his clients. Ferm's request was based on his fear of becoming the victim of credit card fraud or some similar crime if his social security number was included on documents that are a matter of public record, and thus available to any miscreants who happened to come across the number. He did admit that he had no problem with furnishing his social security number to the bankruptcy court, but that he had serious reservations about the continuing use of that number on documents filed with the court and subsequently made a matter of public record.

The bankruptcy court denied his motion, citing the bankruptcy code, 11 U.S.C. §110 (c), which requires that:

> 1) A bankruptcy petition preparer who prepares a document for filing shall place on the document, after the preparer's signature, an identifying number that identifies individuals who prepared the document.
> 2) For purposes of this section, the identifying number of a bankruptcy petition preparer shall be the Social Security account number of each individual who prepared the document or assisted in its preparation.

The court agreed that Ferm's concern might be legitimate, and that the disclosure of one's social security number makes that person vulnerable to becoming a victim of certain crimes. But the court also pointed out that "the dire consequences of identity theft must be discounted by the probability of its occurrence." After weighing the interest of the government in ensuring that bankruptcy petition preparers are properly identifiable from the records filed with the court against the interests of any such bankruptcy petition preparer in protecting his or her identity, the court decided that the requirement of the inclusion of one's social security number was not an unreasonable requirement when balanced against speculative or potential harm faced by the bankruptcy petition preparer. The fines against Ferm were upheld by the court, and his petition for permission to use a substitute identifying number on the forms submitted by him in the bankruptcy proceedings that led to this appeal was denied.

In *Bennett v. Kohler*[307] a tenured professor at the Oregon Health Sciences University (OHSU) alleged that he was forced to retire because he refused to provide a copy of his federal income tax return, or at least a copy of Schedule C of his federal tax return, to his department as required by departmental policy. (This policy was adopted by a majority vote of the "partners," the members of the department faculty.) Bennett's argument was grounded in the protection of his right to informational privacy, as defined by the court in *In re Crawford.*

According to Bennett, the requirement that he provide these documents amounted to a violation of his right to privacy, of his right to free speech, and of his right to due process. He alleged that because he refused to accede to these violations of his rights he was constructively wrongfully discharged. Relying of the precedent from *Crawford,* the court applied a similar balancing test to the Bennett motion. While admitting that revealing the sources and amounts of one's outside income is not information that is normally shared or disclosed to others, this requirement was balanced by the fact that the majority of the members of the partnership had voted for the disclosure. Further strengthening the argument against Bennett's assertion, the partnership had taken steps to ensure that the information would not be shared with or disclosed to others, including having the information submitted directly to an accounting firm rather than to members of the partnership itself. Based on these factors, the court granted summary judgment against Bennett.

[307] 2002 U.S. Dist. LEXIS 10326 (Ore. 2002).

In *Kuhn v. Capital One Financial Corporation*[308] Deborah Kuhn filed suit against Capital One Financial, seeking damages due to having her identity stolen. Kuhn based her claim on the fact that a computer hacker broke into a website server. The website owner informed Capital One that a number of its credit cards, including the one issued to Kuhn, had been compromised as a result of the hacker's conduct. Capital One subsequently informed Kuhn and the other affected cardholders of the situation and closed the compromised accounts. When Kuhn was informed of the closing of the account and the fact that her card had been compromised, she was also told that she needed to take no additional action. She subsequently received a letter from Capital One telling her of the other steps that she could take in order to prevent any additional fraudulent charges on her account. Since a Capital One representative had told her that she needed to take no additional action to protect herself from losses, she took no additional actions, even after receiving the follow-up letter from Capital One.

Unfortunately for Kuhn, within a matter of days there were eighteen different accounts opened in her name, and some $25,000 had been charged to these fraudulent accounts. Kuhn then sued Capital One, alleging that the fraudulent charges accumulated on accounts opened by others in her name constituted a breach of the promises made to her and other account holders in the Capital One Privacy Notice and Consumer Agreement, and that Capital One should be liable for her losses due to this breach.

Capital One's Privacy Notice and Consumer Agreement states, in pertinent part, that "At Capital One we appreciate how important privacy is to our customers… Also, we can protect you from identity theft, fraud, and unauthorized access to personal information about you."[309] Kuhn argued that this constituted a guarantee that she would not be the victim of any identity theft or fraud while she had an account with Capital One. However, the court disagreed. According to the court, the representations made by Capital One in its Privacy Notice and Consumer Agreement only referred to losses on the customer's Capital One account. There was no reference to any outside accounts, nor any coverage extended to any outside accounts by the agreement. Capital One met its obligation to the customer and complied with the terms of the agreement when it promptly notified the customer of the fact that her card had been comprised and closed that account. Capital One honored the terms of its agreement and had no liability for the other charges made in the customer's name through fraudulent means by others. While Kuhn had the right to seek recourse from the party or parties who had fraudulently opened accounts in her name, she had no recourse against Capital One and little likelihood of successfully recovering from the parties committing the fraud.

Daly v. Metropolitan Life Insurance Company[310]also involved both an identity theft and a "Privacy Notice" that allegedly was breached. In 2001 Sarah Daly applied for a life insurance contract from Metropolitan Life. In order to complete the application for insurance, Ms. Daly was required to provide the company with her social security number, her driver's license number, her full name and her date of birth, among other things. After she had completed the application, but before a policy had been issued, Ms. Daly was provided with a copy of Met Life's "Privacy Notice" that explained the company's privacy policy and how confidential information was treated, including how it was stored and how and with whom it might be shared. The notice stated, in pertinent part:

> How We Protect What We Know About You: We treat what we know about you confidentially. Our employees are told to take care in handling your information. They may get information about you only when there is

[308] 2004 Mass. Super. LEXIS 564 (2004).
[309] *Id.*
[310] 782 N.Y.S.2d 530, 2004 N.Y. Misc. LEXIS 1142 (2004).

> a good reason to do so. We take steps to make our computer data bases secure and to safeguard the information we have about you.[311]

Despite the assurances contained in the privacy notice, however, Daly alleged that Met Life negligently allowed one or more non-employees access to her confidential information, and that those parties in turn opened a number of different accounts in her name. As a result of this misuse of her personal and confidential information to open various accounts, Ms. Daly sued Met Life, alleging that Met Life had been negligent in the handling of her confidential information and also seeking damages because her personal lines of credit had been compromised to her detriment.

Met Life denied any liability, arguing that the identity thieves were not employees of the insurance company, but rather were employees who worked as custodians for the owner of the building in which Met Life leased office space. Met Life asserted that it was not negligent in its handling of the information provided by Daly. Met Life further noted that, even if it was shown to be negligent, there was no evidence of any damages suffered by Daly, and even if any damages were shown, Met Life would be shielded from liability due to the intervening actions of the parties who misappropriated the information. Met Life also argued that it did not owe any fiduciary duty to Ms. Daly and thus could not be held liable for any alleged harm to her credit rating or line of credit due to the misuse of her information by the actual tortfeasors.

The court began its opinion by noting that "[w]ith the emergence of identity theft as one of this country's growing concerns, this court is required to address what promises to be a new area of law, namely the duties and responsibilities incidental to the safeguarding of confidential personal information, and more particularly, whether liability may attach to an entity that fails to safeguard personal and confidential information obtained in conjunction with the purchase of a life insurance policy."[312]

After reviewing the facts and noting that this was possibly a case of first impression in New York, the court denied Met Life's motion for summary judgment. The complaint filed by Ms. Daly was summarized by observing that, in order to obtain a life insurance policy from the defendant, Ms. Daly was required to provide sensitive and confidential information to Met Life, but Met Life represented that it would provide adequate protections to keep the information provided secure and confidential. The court found that these representations by Met Life were analogous to the expectation of confidentiality in a doctor-patient relationship, a relationship long recognized as fiduciary in nature. From this analogy the court decided that a "similar covenant of trust and confidence may be inferred in business dealings. Indeed… under New York law… 'a fiduciary duty arises, even in a commercial transaction, where one party reposed trust and confidence in another who exercises discretionary functions for the party's benefit or possesses superior expertise on which the party relied.'"[313]

The court concluded by stating that "while this concept has never before been applied to issues surrounding the protection of confidential personal information, perhaps in the absence of appropriate legislative action, it should."[314]

The fifth case, *Menton v. Experian Corporation,*[315] involved a claim for damages against Experian for refusing to provide a credit report in a timely manner because the person requesting the report did not include his social security number with his request. Menton requested a credit report from Experian on February 15, 2002. He enclosed a check for the appropriate fee, along with a copy of his driver's license, a copy of a bank statement that included his name and address, his phone number, and the name and address of his law firm's web site. Menton did not include his social security number because he alleged that Experian had provided no promise or assurance that

[311] *Id.*
[312] *Id.*
[313] *Id.*
[314] *Id.*
[315] 2003 U.S. Dist. LEXIS 3325 (S.D. N.Y. 2003).

the social security number would be treated in an appropriately confidential manner, nor would Experian provide a confidentiality agreement.

Experian replied to the application for the credit report with an unsigned form letter stating that it could not provide the report without submission by the applicant of his social security number. When Menton had not received his requested credit report by March 13, 2002, he once again submitted a request for his credit report. This second request contained all of the information previously submitted in February, together with a notarized copy of his signature and a check for the appropriate fee. Experian did not reply to this second application, nor did it provide a credit report to Menton.

Menton filed suit against Experian June 18, 2002, alleging that Experian had violated the Fair Credit Reporting Act and the New York Fair Credit Reporting Act and had breached its fiduciary duty to Menton. In his suit he sought a permanent injunction against Experian that would require Experian to provide credit reports upon the presentation of reasonable identification information that did not include a social security number, that would prohibit Experian from selling any identifying information of Menton without his prior written consent, and that would require Experian to delete Menton's social security number from its system. He also sought monetary damages under the FCRA.

Following the filing of this suit and a meeting between the parties, Experian provided Menton with a copy of his credit report and offered to comply with any future requests for credit reports in a timely manner without requiring the inclusion of the social security number on the request, and removed Menton from any marketing services provided by Experian. When Menton refused to drop his suit despite all of these accommodations, Experian filed a motion to dismiss.

One reason asserted by Experian in support of its motion to dismiss was that Menton never supplied "proper identification" with his request since he did not include his social security number. To support this assertion, Experian relied on a consent decree entered into twelve years earlier in which TRW, Experian's predecessor, modified its computer system in order to include social security numbers as identifiers.[316] However, the court was not persuaded that "proper identification" should be so narrowly construed as to require the inclusion of a social security number before a person is entitled to receive a credit report.

The court refused to grant the entire motion to dismiss, although it did dismiss most of the plaintiff's case. The court dismissed the claim of breach of fiduciary duty, pointing out that Menton had failed to present any facts supporting the existence of a fiduciary duty between the parties, and noting that "the mere communication of confidential information [is not] sufficient in and of itself to create a fiduciary relationship."[317] The court could "perceive no basis for a broad rule whereby all credit reporting agencies are held to be fiduciaries of consumers."[318]

The court also granted the motion to dismiss with regard to all of the injunctive relief sought by the plaintiff under the FRCA and the NYFRCA, and the monetary damages sought under the NYFCRA. However, the motion to dismiss the claim of monetary damages under the FCRA was denied since the FCRA provides for statutory damages even if no other damages are shown.

The Menton court did observe in a footnote that it "was not unsympathetic to Mr. Menton's concern regarding the large-scale problem of identity theft,"[319] referring to several recent articles from the New York Times and the Washington Post, among others, as indicative of the scope of the problem.

These court opinions seem to indicate that while the courts are aware of the problem of identity theft, and are also concerned about the potential harm that might befall a person whose personal information is misappropriated, there is little judicial protection afforded to individuals who do not wish to disclose such information. In only one of the five cases was the individual provided with

[316] *See FTC v. TRW, Inc.,* 784 F.Supp. 361, 363 (N.D. Tex. 1991).
[317] *Supra* note 46 (quoting *Wiener v. Lazard Freres & Co.,* 672 N.Y.S.2d 8, 14 (1st Dep't 1998)).
[318] *Id.*
[319] *Id.* at 9.

relief or remedies, and that person had been the victim of an identity theft. In the other four cases the court denied relief to plaintiffs who were concerned about the risk of making confidential information available, but none of the plaintiffs had been victimized through misuse of the information, and thus none of them were provided with protection *in advance* by the court. Thus, it appears that the courts are willing to provide remedies once an identity is stolen, but they are not willing to provide preventative protections prior to such a loss or theft.

VII. PREVENTION

What can an individual do to help prevent identity theft, or at least reduce his or her susceptibility to the crime? There are a series of steps that can and should be taken to minimize the risk of becoming a victim. For example, MSN Money lists ten simple steps, set out in Table 1, that anyone can take to reduce the risk of becoming another victim of identity thieves.[320]

In addition to these ten steps, a person should consider using a fake name when a credit provider or Internet site asks for his or her mother's maiden name or his or her place of birth as an identifier, and consider adding passwords to his or her accounts, both online and offline.

A major source of information that allows identity theft is the appropriation of discarded mail or receipts. This method, commonly referred to as *dumpster diving*, entails retrieving "pre-approved" credit card solicitations, bills, and receipts from the garbage. Individuals disposing of such materials should burn, shred, or otherwise obliterate the materials prior to disposal. As an additional safeguard, an individual who does not wish to receive "pre-approved" credit card solicitations, insurance solicitations, and the like can visit the Consumer Credit Opt-Out web site, fill out a form, and opt out of receiving such offers in the mail. This in turn prevents the possibility of someone stealing from another's mailbox or garbage and then using the information illegally.

Even if a person follows all of these steps, identities can be stolen. Victims of identity theft need to alert their banks and financial institutions immediately, and also need to contact the credit reporting agencies to place a fraud alert on their accounts. A report should be filed with the police, with a copy retained by the victim. Compromised accounts should be closed immediately, and passwords on all accounts should be changed.

VIII. THE EUROPEAN APPROACH

What else can be done? Europe, excluding the United Kingdom, does not seem to have much of a problem with identity theft, so perhaps the European Union can provide some useful guidelines for the U.S. to consider. Liz Pulliam Weston highlighted some of these guidelines, discussed below, in a recent MSN Money article.[321]

In Europe a Social Security number or its equivalent is used strictly for retirement benefits, not as an identifier. Since the Social Security number or its equivalent is not used for identification, the credit reporting agencies develop unique identifying numbers for the customers in their databases, and the agencies do not share information as readily as their American counterparts.

Most of the countries in Europe, at least on the continent, require their citizens to carry an identification card that must be produced for a number of ordinary activities such as opening or accessing bank accounts, renting cars, or checking in at hotels. Since these identification cards are difficult to counterfeit, and since the card must be physically presented in order to complete the

[320] J. Wuorio, *Ten Ways to Stop Identity Theft Cold*, MSN MONEY (2006), http://moneycentral.msn.com/content/Banking/FinancialPrivacy/P33715.asp (last visited March 2, 2006).

[321] L. P. Weston, *What Europe Can Teach Us About Identity Theft*, MSN MONEY (2006), http://moneycentral.msn.com/content/Banking/FinancialPrivacy/P116528.asp. (last visited March 2, 2006).

activity, identity fraud in much less likely to occur.[322] Of course, there is a fear among many Americans that a national identity card will allow the government to monitor all of a person's activities, infringing on the rights and freedoms of the individual, so the development and use of such a card is unlikely in the United States at this time.

The EU has laws that restrict businesses from selling or sharing private or financial information about customers. This means that information is not as readily available or as easily obtained within the EU as it is in the United States. In addition, credit bureaus in many European nations are maintained by banking groups and only share information with one another. They do not provide information to outsiders. Further, three European countries – France, Spain, and Denmark – only allow credit bureaus to report negative information about credit applicants. If there is nothing negative to report, an inquiry about a credit applicant will only report that there is no negative information about the applicant. Such restricted information is of little use to an identity thief.

Perhaps most important, credit is not as commonly used by consumers in Europe as it is used in the United States. Debit cards are more popular than credit cards. Also, in most European nations debit cards and credit cards are likely to have computer chips rather than magnetic strips, making the copying of the card much more difficult and expensive. Cardholders also personally enter a PIN rather than signing a slip or voucher. This "chip and PIN" technology was introduced in France in 1992, and it is believed to have reduced the fraudulent use of credit cards and debit cards in making payments by at least fifty percent.

IX. CONCLUSIONS AND RECOMMENDATIONS

The problem of identity theft is serious, and there is some evidence that is has become more serious of late. Even with a narrower definition of the term "identity theft" than is used by the government, more than three million consumers in the United States were victims of identity theft in 2004. These persons had accounts opened in their names, apartments rented in their names, medical treatment provided to persons using their names, or jobs acquired by persons using their names. Such conduct is, obviously, a matter for concern. However, it does not reach the epidemic stage that the media has portrayed, and steps have been taken to reduce the risk and to prevent some of the more obvious sources for such theft. The legislature, the banks, and the credit card industry have all been active in addressing the issue. What is left now is for the potential victim to take steps to protect his or her interests. Individuals need to exercise common sense; they need to treat confidential and personal information in a confidential manner; they need to check their monthly statements, review their credit reports, and properly dispose of papers containing personal information. Most important, they need to be proactive in safeguarding their information and their identities.

[322] *"Country Dependence"* a subsection of *"Identity Theft,"* WIKIPEDIA, THE FREE ENCYCLOPEDIA http://en.wikipedia.org/wiki/Identity_theft. (last visited March 2, 2006).

TABLE 1: TEN WAYS TO STOP IDENTITY THEFT COLD[323]

1. Destroy private records and statements. Tear up, shred, or burn these items before throwing them out.
2. Secure your mail. Get a locking mailbox or a post-office box for receiving mail, and then empty your mailbox promptly. Do not place bill payments or checks in your home mailbox, unless it is a locking mailbox.
3. Safeguard your Social Security number. Do not carry your Social Security card, and do not use your Social Security number for identification purposes.[324]
4. Don't leave a paper trail. Do not leave ATM receipts or credit card receipts behind after using your debit or credit card.
5. Never let your credit card out of your sight.
6. Know who you are dealing with. Do not respond to requests for personal information in telephone calls or emails that you receive. If you have any doubts about the legitimacy of the request, do not respond in any fashion. If you believe the request is legitimate, contact the company yourself, verify the legitimacy of the request and the need for the information, and then decide whether you are willing to provide it.
7. Remove your name from marketers' lists. Register with the "Do-Not-Call registry" to remove your name from telemarketing lists; opt out of credit card solicitations, and ask your credit card companies and your bank not to send you blank checks to use in accessing your credit accounts.
8. Be defensive with personal information. Ask salesclerks why they need any requested information, and also what will happen if you do not provide the information. If you are required to provide the information, ask about the privacy protection policies of the company and how your personal information will be handled and protected.
9. Monitor your credit report. Obtain and review your credit report at least once a year. If you are planning a major purchase, obtain a copy of your credit report a month ahead of the planned purchase to make sure there are no surprises awaiting you.
10. Review your credit card and bank statements carefully. If you have any doubts about any entries, follow up immediately

[323] *Supra* note 53.

[324] See Bankrate.com, *Safeguard Your Social Security Number* (2006), http://moneycentral.msn.com/content/Banking/FinancialPrivacy/P33718.asp, for additional information and suggestions.