The Recognition of a Negligence Cause of Action for Victims of Identity Theft: Someone Stole My Identity, Now Who Is Going to Pay for It?

Anthony E. White

Follow this and additional works at: http://scholarship.law.marquette.edu/mulr

Part of the Law Commons

Repository Citation

Available at: http://scholarship.law.marquette.edu/mulr/vol88/iss4/4

This Article is brought to you for free and open access by the Journals at Marquette Law Scholarly Commons. It has been accepted for inclusion in Marquette Law Review by an authorized administrator of Marquette Law Scholarly Commons. For more information, please contact megan.obriens@marquette.edu.
THE RECOGNITION OF A NEGLIGENCE CAUSE OF ACTION FOR VICTIMS OF IDENTITY THEFT: SOMEONE STOLE MY IDENTITY, NOW WHO IS GOING TO PAY FOR IT?

I. INTRODUCTION

Imagine a scenario in which a young husband and wife, the Smiths, are in the process of buying their first home. They have completed the necessary paperwork and have hired an attorney to assist them with the closing. The Smiths have also given their current landlord notice that they will not be renewing their lease. All that remains is for the real estate agent to run one more quick credit check before the papers are signed. But the sale hits a snag. The real estate agent notifies the Smiths that their credit report came back negative and, unfortunately, the sale will not go through.

The Smiths rush home in a panic and call their bank. After receiving a copy of their credit report, they learn that someone has been using Mr. Smith’s name to open credit accounts. It turns out that this unknown “identity thief” has charged thousands of dollars in Mr. Smith’s name. The Smiths contact their attorney. After many phone calls, countless weeks, and loads of paperwork, their credit is eventually restored. In addition, the police are fortunate enough to arrest the identity thief: an unemployed, adult computer hacker. The identity thief used his computer skills to exploit a security vulnerability at the Smiths’ bank to retrieve information about Mr. Smith. The thief then used this information to open credit accounts under Mr. Smith’s name.

Regrettably, despite clearing their name, it is too late for the Smiths. The house of their dreams has been sold to someone else. They must find a new place to live because the landlord rented their apartment to someone else after the Smiths gave notice of departure. They have spent thousands of dollars in attorney’s fees to correct their credit problems and have expended countless hours in an effort to remedy this credit fiasco. The Smiths’ attorney recommends suing the identity thief for the harm he caused, but he mentions that there is a problem: the identity thief has no apparent assets; therefore, they would not be able to collect a judgment against the identity thief. Mr. and Mrs. Smith
wonder if there is some way that they can be compensated.

Situations similar to the Smiths’ situation are far too common. Recent estimates indicate that one in four adults have been affected by identity theft. It is estimated that identity theft has cost Americans at least five billion dollars. In addition, the average victim of identity theft spends over 600 hours and $1400 fixing his credit. Unfortunately, the problem is only getting worse: Identity theft has increased in recent years. Even though most states have laws in place that criminalize identity theft, it has been difficult for identity theft victims to receive compensation for their injuries. Some victims have attempted to hold financial or credit institutions liable for the identity theft when the institution allowed the identity thief to use the stolen information to open bank or credit accounts. However, the financial institutions have usually been able to avoid liability through various laws and court holdings.

The rise in identity theft is even more troubling when one considers the ease with which information can be transferred via computers. Before the advent of mass computer use, personal information typically was stored on paper and easily could be secured in a file cabinet with a lock and key. Therefore, identity thieves had to use more devious and indirect methods to steal personal information, such as stealing mail or digging through someone’s trash. Today, an identity thief with the

---

5. It is estimated that in 2002, there were 7,000,000 cases of identity theft. This is an 87.7% increase in identity theft from 2001. See Identity Theft 911, Identity Fraud Analysis of Compelling Statistics (Aug. 2003), at http://www.identitytheft911.com/education/fundamentals/idtheftstatistics.htm.
7. Few states have statutes in place that require restitution by the identity thief or provide assistance to the victim in correcting the problems caused by the identity thief. Daniel J. Solove, Enforcing Privacy Rights Symposium: Remedy for Privacy Wrongs—New Models: Identity Theft, Privacy, and the Architecture of Vulnerability, 54 HASTINGS L.J. 1227, 1248 (2003).
8. See infra Part III.
9. See infra Parts II and III.
10. See Brandon McKelvey, Comment, Financial Institution’s Duty of Confidentiality to Keep Customer’s Personal Information Secure from the Threat of Identity Theft, 34 U.C.
right amount of computer knowledge can gather all of the information he needs about an individual from the comfort of his home computer. With the recent outbreaks of fast-spreading computer viruses that take advantage of computer vulnerabilities, one has to wonder whether the financial institutions that hold personal information sought by identity thieves have the requisite security measures to protect their files. Do they have the necessary digital lock and key?

This Comment proposes that courts should permit victims of identity theft to have a cause of action against financial institutions whose negligence in establishing sufficient computer security measures allows an identity thief to obtain the victim's personal information and use that information to the financial detriment of the victim. To fully explore this proposal, Part II of this Comment will provide some general background into the concept of identity theft and other proposed remedies to the problem. Part III of the Comment will explore the issues surrounding the recognition of the tort of negligent enablement of impostor fraud as a cause of action for identity theft victims, and in Part IV, this Comment will explore the potential use of negligence per se as a cause of action for identity theft victims. Finally, Part V of the Comment will conclude that recognition of new causes of action for identity theft victims may help to reduce the rate of identity theft by placing more responsibility on financial institutions.

II. IDENTITY THEFT: BACKGROUND

To demonstrate why courts should recognize a cause of action for

---

11. The collection of information about individuals has increased with the growth of the Internet. Such "databases" of personal information raise privacy issues and provide identity thieves with a potential resource. See generally James P. Nehf, Recognizing the Societal Value in Information Privacy, 78 WASH. L. REV. 1 (2003) (discussing the value of information privacy in today's society).

12. The SoBig.F and Blaster viruses that infected computers within weeks of each other in the summer of 2003 created mass havoc among computer users and spread to over 148 countries. Helen Cook, Email Virus Chaos; SoBig-F Grinding Internet to a Halt, THE MIRROR, Aug. 22, 2003, at News 1, 6. It is estimated that 500,000 computers were harmed by the Blaster virus and that the SoBig.F virus was attached to one in every seventeen emails. Id.


14. See infra Part II.
15. See infra Part III.
16. See infra Part IV.
17. See infra Part V.
victims of identity theft, this Comment first will examine the process of identity theft, the end result of an instance of identity theft, and why identity theft is a growing problem. Additionally, to demonstrate why a cause of action for identity theft victims is necessary, this Comment will examine past and present proposals to reduce identity theft that have been inadequate.

A. The Process of Identity Theft

An instance of identity theft "occurs when someone uses another individual's personal information for fraudulent purposes."18 Due to the nature of identity theft, it is often difficult for the victim to realize that he has been victimized.19 This is because the fruits of an identity thief's crime take weeks, months, or even years to ripen.20 Only in certain instances, such as when a wallet is stolen or a home is burglarized, are potential identity theft victims aware of the possibility that their personal information may be used for fraudulent purposes. Thus, victims in those situations can minimize potential financial losses by promptly canceling their credit cards and warning their banks.21

The rise in identity theft has occurred in a large part because of the increased sophistication and anonymity of identity thieves. Some techniques are fairly simple but still allow identity thieves to anonymously steal personal information.22 Such techniques include observing individuals when they enter their credit card number on a telephone or digging through someone's trash searching for credit card receipts. Thieves can also attempt to use a technique known as "pretexting."23 Pretexting can occur when a thief calls a financial institution pretending to be a customer or when a thief calls a customer pretending to be a financial institution.24 In either instance, the identity thief's goal is to solicit personal information from the caller. Another

18. McKelvey, supra note 10, at 1082.
20. Id. at 1425–26.
21. See Provenza, supra note 2, at 322 n.40. In addition, under most credit card policies, the victim of a fraudulently used credit card is responsible for only fifty dollars, regardless of how much the thief charges on the card. Hoar, supra note 19, at 1436–37.
22. See Hoar, supra note 19, at 1426. Identity thieves can also attempt to "dumpster dive" at places such as banks and hospitals in the hopes of discovering confidential information. Id.
23. Id. See also Barbara Anthony, Practicing Law Institute Corporate Law and Practice Course Handbook Series, 1172 PLI/Corp 387, 393 (2000).
24. McKelvey, supra note 10, at 1083.
growing technique for identity theft has been for identity thieves to become employed at financial institutions and then gain access to confidential customer information.\footnote{25}{See id. at 1083–84.}

The most recent and troubling technique used to obtain personal information has been the use of computers.\footnote{26}{See David Breitkopf, Visa, MC Get Tougher on Hackers, Data Collectors, THE AMERICAN BANKER, Apr. 11, 2003, at 9.} With the amount of information available on the Internet, identity thieves have a wide range of sources to utilize to accumulate personal information.\footnote{27}{See Solove, supra note 7, at 1255.} In addition, computer hackers can attempt to gain access to the computers of financial institutions in order to access confidential customer records.\footnote{28}{Id. at 1259.} At least one online security firm has found that "the average U.S. company's computer security is attacked by intruders thirty times per week."\footnote{29}{Timothy H. Skinner, California's Database Breach Notification Security Act: The First State Breach Notification Law Is Not Yet a Suitable Template for National Identity Theft Legislation, 10 RICH. J.L. & TECH. 1, ¶ 5 (2003), at http://law.richmond.edu/jolt/v10i1/article1.pdf.} Due to the increased vulnerabilities of computer systems to hackers, government legislation has attempted to regulate the implementation of computer network security.\footnote{30}{See infra Part II.E.}

B. The Results of Identity Theft

1. Account Takeovers

Instances in which identity thieves take over existing financial accounts are called "account takeovers."\footnote{31}{See Sovem, supra note 6, at 355.} Account takeovers are less of a threat to a victim’s finances because the harm usually is discovered within a short period of time, typically when the victim receives a statement from his bank or credit card company.\footnote{32}{See Provenza, supra note 2, at 321.} However, within that time, the identity thief can attempt to charge purchases to the victim’s credit card, cash checks in the victim’s name, or even attempt to withdraw funds from the account directly.\footnote{33}{Id.}
2. True Name Fraud

The more potentially damaging form of identity theft is known as “true name fraud.” The key difference between true name fraud and account takeover is that with true name fraud, the identity thief opens new bank and credit accounts in the victim’s name, while account takeover involves the use of existing bank and credit accounts only. Usually, in an instance of true name fraud, the identity thief will open new accounts in the victim’s name, but under a different address to avoid alerting the victim. Since the victim will not know his personal information has been stolen, it is unlikely he will discover the nature of the crime for an extended period of time. Frequently, victims of true name fraud do not learn of the crime until they attempt to finance the purchase of a home or vehicle. It is only after the victims review their credit reports that they learn of accounts that have been opened without their knowledge.

C. Why Identity Theft Occurs

The recent rise of identity theft probably can be attributed to weaknesses in the structure in which personal information flows in society. The main weakness that identity thieves have exploited have been the “digital dossiers” of individuals. These dossiers contain personal information, including an individual’s name, address, phone number, and social security number (“SSN”) and are collected by various private and governmental organizations, such as banks, video stores, and Department of Motor Vehicle centers. Frequently, an individual does not know how much information is stored in his digital dossier, or who has compiled it. This makes it difficult, if not impossible, for an individual to control access to his personal information and, thus, limit his vulnerability to instances of identity theft.

34. See Sovern, supra note 6, at 355.
35. Id.
36. See Provenza, supra note 2, at 320–21.
37. See Hoar, supra note 19, at 1425.
38. Id.
39. “According to the FBI, identity theft is the most rapidly growing type of white-collar criminal activity.” Solove, supra note 7, at 1244 n.71.
40. See generally Solove, supra note 7. Solove’s article provides detailed information about the architecture surrounding identity theft and potential reforms regarding how personal information is used to reduce the opportunity for identity theft.
41. Id. at 1251–52.
One of the chief pieces of information desired by identity thieves is the SSN. Even though SSNs "were not designed to be used as . . . general identifier[s]," the widespread use of SSNs has caused them to become just that. Today, an individual's SSN is his primary source for identification for financial institutions, schools, and government agencies. Thus, identity thieves can use an individual's SSN to access bank accounts or medical records in the hopes of finding additional personal information. Then, identity thieves can use this additional information, along with the SSN, to open new bank and credit accounts.

Given the identity thief's desire to obtain SSNs, it is important to discuss how those who possess SSNs handle that personal information and digital dossiers in general. For example, an individual probably will have to give his SSN and other personal information to a bank when he opens a new account. Unbeknownst to the individual, the bank may end up selling or trading its new customer's information to a third-party institution. Therefore, an individual's SSN may be possessed by more institutions than the individual would expect or know. When an individual chooses to give his information to one institution, he may do so because he trusts the institution or knows that it has security measures sufficient to protect his personal information. However, the security features of the institution that buys a digital dossier may be poor or insufficient, and thus an individual may be vulnerable to potential identity theft.

42. Id.
43. Id. at 1252.
44. Id.
45. Id.
46. See Flavio L. Komuves, We've Got Your Number: An Overview of Legislation and Decisions to Control the Use of Social Security Numbers as Personal Identifiers, 16 J. MARSHALL J. COMPUTER & INFO. L. 529, 536-49 (1998). The Privacy Act of 1974 passed amid privacy concerns over the growing use of SSNs as general identifiers; the Act prohibited the government from denying service to an individual for his refusal to divulge his SSN. See Solove, supra note 7, at 1253. The Privacy Act, however, did not prohibit the use of SSNs in the private sector. Id.
47. Komuves, supra note 46, at 536-40.
48. Solove, supra note 7, at 1253.
49. Komuves, supra note 46, at 536-37.
50. See Provenza, supra note 2, at 329. Because banks have become more aware of the need to protect customer information, many have added high-tech security features such as voice recognition software, fingerprinting, and other evolving measures where cost effective. Id.
Along with the increase of computer usage and the rise of the Internet has come a corresponding rise in instances of network computer hacking. This is of great concern because as more financial institutions store confidential customer information on computers that are accessible via the Internet, it becomes possible for a hacker to gain access to or control over customer information from the comfort of his own home. Without proper security systems in place, a financial institution whose computer network is constantly connected is at continuous risk of attack. If financial institutions are not responsive to the potential for computer hackers to attack their computer networks, they risk disseminating private information of their customers.

D. Past Proposals to Reduce Identity Theft

As instances of identity theft have increased, so have the measures taken to prevent theft or punish offenders. Generally, these measures can be classified into four groups. The first has been for individuals to take greater responsibility in protecting their personal information. The second measure is the creation of criminal statutes to punish identity thieves. The third is the Fair Credit Reporting Act ("FCRA"). And the fourth measure has been to allow civil remedies based on claims of invasion of privacy and breach of confidentiality.

1. Personal Responsibility

One way to reduce identity theft is to have individuals protect their


52. Breitkopf, supra note 26, at 9. Hacking has become so prevalent that there are over 400,000 hacking-tip web sites. Id. Some web sites even provide amateurs with step-by-step procedures on how to break into web sites. Id.

53. See Hoar, supra note 19, at 1440. Computer protections, such as firewalls, are critical to protect computers that are "always on" from network attacks. Id.

54. In one extreme example of hacking, a computer hacker gained access to roughly eight million customer credit card numbers by exploiting a security vulnerability that affected several major banks and credit card companies. David Boraks and W.A. Lee, Assessing Damage of Processor Data Hack; Record 8 Million Cards Said Affected; No Word Yet of Fraud, AMERICAN BANKER, Feb. 19, 2003, at 1.

55. See infra Part II.D.1.

56. See infra Part II.D.2.

57. See infra Part II.D.3.

58. See infra Part II.D.4.
personal information.\textsuperscript{59} Essentially, an individual would take steps to limit his potential vulnerability to identity thieves. For example, documents containing personal information could be stored or disposed of with special care.\textsuperscript{60} Small measures, such as keeping important documents in a safe place and shredding receipts instead of simply throwing them away, can greatly reduce the chance that identity thieves will find personal information.\textsuperscript{61}

Individuals could also take steps to protect bank and credit accounts. Individuals can be careful when providing account information. By confirming requests for account information, whether these requests are via phone, mail, or email, an individual can prevent identity thieves from gathering account information through pretexting methods.\textsuperscript{62} Additional precautions should be taken when providing sensitive account information over the Internet.\textsuperscript{63} The most important precaution is to be certain that a secure connection is provided when account information is requested online.\textsuperscript{64} A secure connection greatly reduces the possibility that identity thieves can hack into an individual's connection and steal his account information without his knowledge.\textsuperscript{65}

Individuals can also request annual credit reports.\textsuperscript{66} Given that a victim of identity theft frequently does not know he is a victim, an annual review of credit reports can alert an individual that he has been victimized. Even though reviewing credit reports cannot prevent identity theft from occurring, it can help to mitigate the harm and allow the victim to begin the long, arduous process of trying to reestablish his finances.


\textsuperscript{60} See Hoar, \textit{supra} note 19, at 1438–43, for suggestions on what steps to take to minimize the risks of identity theft.

\textsuperscript{61} \textit{Id.} at 1441.

\textsuperscript{62} For information on how to avoid pretexting and other identity theft situations, see generally Federal Trade Commission, \textit{About Identity Theft}, at http://www.consumer.gov/idtheft/consumertopics_bk.html (last visited Jan. 11, 2005).

\textsuperscript{63} For tips on how to avoid identity theft while shopping online, see MasterCard International, \textit{Preventing Payment Card Fraud}, at http://www.mastercardintl.com/docs/s_r_consumer_tips_final.pdf (last visited Jan. 11, 2005).

\textsuperscript{64} \textit{Id.}

\textsuperscript{65} \textit{Id.}

\textsuperscript{66} Solove, \textit{supra} note 7, at 1249. It costs a consumer $8.50, per report, to order a credit report from each of the three major credit reporting agencies.
2. Criminal Statutes

Legislatures have responded to the growing number of identity theft cases by enacting statutes to criminalize this type of theft. Until 1998, only three states had statutes that specifically dealt with identity theft. Since that time, additional states have enacted identity theft statutes, bringing the total number of states with identity theft statutes to forty-four. States differ in how they penalize identity theft and how they address victims' rights. Some states treat identity theft as a felony with a set penalty, while others vary the severity of the punishment based on the amount of money involved. Additionally, some states have incorporated victim restitution procedures into their statutes.

In 1998, Congress addressed concerns over identity theft by passing the Identity Theft and Deterrence Act ("ITADA"). The ITADA makes it a crime to "knowingly transfer[], possess[], or use[], without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet,... any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law." Under the ITADA, the Federal Trade Commission ("FTC") has taken a central role in identity theft prevention. The FTC's goal is to "assist victims and law enforcement by collecting and sharing information from public and private entities." One way that the FTC assists identity theft victims is by providing victims with "step-by-step instructions on contacting the various credit reporting agencies to remove any record of the crime." In essence, the FTC's role under the ITADA has been to educate consumers and

67. Id. at 1247.
68. Id.
69. For example, Florida, Pennsylvania, and New Jersey all vary their punishment of identity theft based upon the amount of money involved in the crime. Id. Wisconsin, under Wisconsin Statutes section 943.41(8) (2003), also varies the penalty imposed based upon the amount of money involved in the crime.
70. California, by statute, provides victims with assistance in repairing their finances after an instance of identity theft. Id. at 1247.
72. Id.
74. Id. at 371. The FTC has created the Identity Theft Hotline and the Identity Theft Clearinghouse, along with consumer education programs, as attempts to decrease incidents of identity theft. Id. at 372-75.
victims about identity theft prevention methods, as well as to provide consumers with assistance after an identity theft has occurred.\(^{76}\)

Unfortunately, there have been problems with criminal identity theft statutes and the ITADA. The biggest problem is that law enforcement agencies lack the resources to investigate and prosecute identity thieves.\(^{77}\) Given the lack of urgency and ability for the police to catch identity thieves, it is rare for identity thieves to be arrested.\(^{78}\) Because arrests are infrequent, it is difficult, if not impossible, for victims to receive restitution for their financial losses.\(^{79}\) Even if the identity thief is arrested, restitution is not always possible or required.\(^{80}\) Regrettably, the ITADA does not remedy this problem, as it "does not allow the courts to award restitution to the victim for costs related to the identity theft."\(^{81}\)

3. Fair Credit Reporting Act\(^{82}\)

Because identity thieves frequently "mislead" credit companies in order to apply for credit in the victim's name, identity theft victims can attempt to receive restitution from the credit companies that issued credit to the identity thief under the Fair Credit Reporting Act ("FCRA").\(^{83}\) However, there are several reasons why the FCRA is inadequate in dealing with occurrences of identity theft.\(^{84}\)

One of the biggest obstacles in applying the FCRA to instances of identity theft is the FCRA’s short statute of limitations.\(^{85}\) The statute of limitations is of concern because identity theft victims frequently

---

\(^{76}\) Id.

\(^{77}\) Solove, supra note 7, at 1248. Identity theft investigation requires a high degree of specialized training and frequently ends without an arrest. In addition, police departments have a hard time justifying the use of additional resources for an identity theft investigation due to its white-collar criminal status. Most departments spend most of their resources investigating violent crimes and drug offenses and have little money left to direct toward identity theft investigations. Id.

\(^{78}\) Identity Theft Resource Center, Facts and Statistics, at http://www.idtheftcenter.org/facts.shtml (last modified Feb. 15, 2004). "The average arrest rate (according to law enforcement) is under 5% of all reported cases by victims." Id.

\(^{79}\) Solove, supra note 7, at 1248.

\(^{80}\) Id. at 1247–48.

\(^{81}\) Alwin, supra note 75, at 363–64.


\(^{83}\) Sovern, supra note 6, at 388.

\(^{84}\) See id. at 388–401 for an in-depth examination of how the FCRA applies to instances of identity theft. This Comment will only briefly examine the relationship between the FCRA and identity theft.

\(^{85}\) Id. at 389. The FCRA has a two-year statute of limitations. Id.
discover that they have been victimized only after the claim has expired.\textsuperscript{86} Therefore, few victims of identity theft have an opportunity to utilize the FCRA.\textsuperscript{87} Another problem with the FCRA is its scope. The FCRA allows claims only against credit reporting agencies and cannot be used against financial institutions, which are frequently involved in instances of identity theft.\textsuperscript{88}

Even if an identity theft victim is able to bring a claim under the FCRA, the remedies offered by the FCRA are limited and usually do not provide adequate relief. The main reason for this is that the FCRA is applicable in only certain situations.\textsuperscript{89} Unfortunately, these situations do not cover most instances of identity theft. For the situations in which the FCRA can be applied, the protection offered by the FCRA to creditors makes the chances of success of a private claim slim.\textsuperscript{90} Therefore, credit agencies have little incentive to increase security measures that could insure the legitimacy of credit applicants and thus reduce instances of identity theft.\textsuperscript{91}

4. Civil Remedies

The majority of identity theft victims have attempted to bring claims against financial institutions under theories of invasion of privacy and breach of confidentiality.

\textit{i. Privacy Claims}

Some identity theft victims have attempted to sue financial institutions under an invasion of privacy theory.\textsuperscript{92} It is generally accepted that an individual should be able to expect that a financial institution will keep customer information secure and use it only for business purposes.\textsuperscript{93} Even though an invasion of privacy claim appears applicable in identity theft situations, courts have been unwilling to make extensive use of it.\textsuperscript{94} Usually, invasion of privacy claims fail

\begin{itemize}
  \item \textsuperscript{86} \textit{Id.}
  \item \textsuperscript{87} \textit{See TRW Inc. v. Andrews, 534 U.S. 19, 28 (2001)} (holding that the statute of limitations began to run when the FCRA was violated even though the victim did not know that the fraud had occurred).
  \item \textsuperscript{88} McKelvey, \textit{supra} note 10, at 1091.
  \item \textsuperscript{89} Sovern, \textit{supra} note 6, at 406.
  \item \textsuperscript{90} \textit{Id.}
  \item \textsuperscript{91} \textit{Id.}
  \item \textsuperscript{92} McKelvey, \textit{supra} note 10, at 1113.
  \item \textsuperscript{93} \textit{Id.} at 1113 n.248.
  \item \textsuperscript{94} \textit{Id.} at 1113–14.
\end{itemize}
because "most financial institution customers cannot satisfy the requirement of public dissemination." In addition, various judicial limitations have eroded the effectiveness of invasion of privacy claims in identity theft cases. For example, where a victim's information is disclosed to only one financial institution, courts have held that an identity thief does not invade a victim's privacy because he does not disclose the victim's private information to the public. Thus, even though the theory of invasion of privacy could be applied, the theory is inadequate to deal with the typical identity theft situation where one identity thief uses the information of one victim exclusively.

ii. Confidentiality

Another possible remedy for identity theft victim lies in tort, where victims can sue financial institutions for breaching their duty of confidentiality. This remedy is based on the premise that financial institutions are required to keep customer information confidential, unless authorization to disclose is given by the customer. Courts have even been willing to require financial institutions to keep customer information confidential in situations where there is no explicit contractual duty due to the customer's vulnerability and reliance on the financial institution. Even though the damages available to a victim of identity theft through a breach of confidentiality claim may seem adequate, courts have yet to conclude that a breach of confidentiality claim should be applied to an identity theft claim. The main reason for this has been that past cases in which breach of confidentiality has been applied have involved instances where employees of the financial institution "intentionally communicated customer information to third parties." Therefore, in situations similar to the example mentioned earlier in this Comment, in which there is no intentional involvement

95. Id. at 1113.
96. Id. at 1098-99, 1114.
97. Id.
98. Id. at 1114.
99. Id. at 1115.
100. Id. at 1102-04.
101. Id. at 1103 n.163.
102. Id. at 1104-07 (citing Peterson v. Idaho First Nat'l Bank, 367 P.2d 284 (Idaho 1961); Djowharzadeh v. City Nat'l Bank & Trust Co., 646 P.2d 616 (Okla. Ct. App. 1982)).
103. Id. at 1111-12.
104. Id. at 1107 n.196.
105. Id. at 1107.
106. See supra Part I.
by a financial institution employee in the identity theft, a breach of confidentiality claim could not be used to assist the victim in receiving restitution.

E. Current Government Responses to Identity Theft

1. Gramm-Leach-Bliley Act

The Gramm-Leach-Bliley Act of 1999\(^\text{107}\) ("GLB Act") was passed "to address the need for increased competition in the financial services industry."\(^\text{108}\) The GLB Act also addresses the need for privacy in handling consumer financial information.\(^\text{109}\) The GLB Act's privacy provisions\(^\text{110}\) prohibit the gathering of consumer information by pretexting\(^\text{111}\) and require that financial institutions have "policies, procedures, and controls in place to prevent the unauthorized disclosure of customer financial information and to deter and detect fraudulent access to such information."\(^\text{112}\)

The privacy provision of the GLB Act states "that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information."\(^\text{113}\) This provision of the GLB Act has been given effect in three ways.\(^\text{114}\) First, and most important, the GLB Act requires that various governmental agencies, including the Federal Trade Commission, the Securities and Exchange Commission, and the Secretary of the Treasury, "must establish standards relating to administrative, technical and physical safeguards"
with regard to private customer financial information. Second, the GLB Act requires customer notification before private information can be disclosed to nonaffiliated third parties. Last, privacy policies must be disclosed to customers of the financial institutions.

In addition to requiring certain governmental agencies to establish standards regarding the protection of customer financial information, the GLB Act also requires these governmental agencies to enforce these provisions.

However, the mechanisms in place for the enforcement of the GLB Act are not effective in protecting customers from identity theft. In particular, the GLB Act requires financial institutions to implement security measures to protect consumer information, but it does not specify what measures are to be taken or what the penalty would be for failure to comply with the statute. Additionally, "[t]he GLB Act . . . does not provide for a private right of action for consumers to sue the financial institution[s] directly for violation of the statute." Since consumers have no explicit private cause of action under the GLB Act, unless the Federal Trade Commission strictly enforces its "Safeguards Rule," it is unlikely financial institutions will be motivated to implement greater security measures due to the high costs involved with doing so.

115. Id.

116. Id.


119. Id. § 6801(b).

120. Even though there are no specific guidelines for compliance in the GLB Act, "the bank and thrift regulatory agencies have issued . . . joint guidelines for safeguarding confidential consumer information." Schiller, supra note 114, at 363. However, financial institutions need only implement methods suggested by the guidelines if they choose to do so. Id.

121. Id. at 359.

122. The Federal Trade Commission released its Safeguards Rule in May 2002. "The Safeguards Rule sets forth standards for developing, implementing, and maintaining reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information handled by all financial institutions over which the FTC has jurisdiction." Benoit & Lovoy, supra note 110, at 1164. For a detailed description of the Safeguards Rule's provisions, see id. at 1164–71.

123. Id. at 1170.
2. Database Breach Notification Security Act (SB 1386)

California has taken a unique approach in hopes of curbing instances of identity theft. Effective July 1, 2003, the Database Breach Notification Security Act ("SB 1386") requires that any government agencies, organizations, or businesses "that do business in California . . . promptly notify California ‘residents’ when they have a reasonable belief that a system breach [has] occurred which possibly exposed data subjects’ personal information to third parties."124 SB 1386 protects a wide range of consumer information, including SSNs, driver’s license numbers, and bank account numbers and requires notification after various forms of security breaches, including attacks on computer networks and the theft of computer hard drives.125 If a security breach does occur, SB 1386 requires that notice be given to customers "in the most expedient time possible” and "without reasonable delay."126 If prompt notice is not given and a customer suffers harm, SB 1386 permits the harmed customer to have a private cause of action against the financial institution, and it is predicted that SB 1386 will result in the creation of class action lawsuits in response to security breaches.127

While SB 1386 is a desirable piece of legislation in response to the rise of identity theft, it has its shortcomings and only begins to deal with the problem of identity theft.128 One problem with SB 1386 is that its language is too vague in describing what constitutes a security breach and when such a breach requires customer notification.129 This is a problem because as technology changes and advances, the language of SB 1386 may not be sufficient to cover most instances of security breaches.130 Perhaps the most daunting problem with SB 1386, in regard to victim recovery, is that if a business promptly notifies its customers of

126. Id.
128. For a detailed discussion of the problems with SB 1386, see Skinner, supra note 29. This Comment will discuss only problems that deal most directly with the issue of giving victims of identity theft a means of recovery.
129. Id. at 32–33.
130. Id.
a security breach, SB 1386 seems to relieve the business of any liability for the security breach.\textsuperscript{131} Because SB 1386 limits damages to instances where the business fails to give notice to the customer for a security breach, identity theft victims must search for other causes of action to recover from the business where that business has complied with SB 1386.\textsuperscript{132}

III. RECOGNITION OF NEGLIGENT ENABLEMENT OF IMPOSTOR FRAUD

Because identity theft continues to be a problem\textsuperscript{133} and past and current proposals have been inadequate,\textsuperscript{134} new responses are required if the identity theft problem is to be solved. These proposed responses\textsuperscript{135} are designed to combat identity theft by allowing victims of identity theft to sue financial institutions in instances where the financial institutions' negligence in maintaining adequate computer security allowed the identity theft to occur. By allowing identity theft victims to sue for damages, it is theorized that financial institutions will increase computer security to prevent claims by identity theft victims from arising. Hopefully, if financial institutions follow this logic and increase computer security, instances of identity theft will decrease as a result.

Some victims of identity theft have attempted to sue financial institutions and credit companies under the claim of negligent enablement of impostor fraud.\textsuperscript{136} Recently, the Supreme Court of South Carolina decided not to recognize the claim of negligent enablement of impostor fraud in \textit{Huggins v. Citibank}.\textsuperscript{137} The plaintiff in \textit{Huggins} was the victim of an unknown identity thief who applied for, and was granted, credit cards in the plaintiff's name by the defendant bank.\textsuperscript{138} Huggins claimed that Citibank was negligent in issuing the credit card to the identity thief because the bank did not corroborate the thief's identity and because the bank did not have policies in place to check the identities of applicants.\textsuperscript{139} In deciding not to recognize the claim of negligent enablement of impostor fraud, the court followed the

\begin{flushleft}
\textsuperscript{132} Skinner, \textit{supra} note 29, at 57.
\textsuperscript{133} See \textit{supra} Parts II.A–C.
\textsuperscript{134} See \textit{supra} Parts II.D–E.
\textsuperscript{135} See \textit{infra} Parts III and IV.
\textsuperscript{136} Sovern, \textit{supra} note 6, at 401.
\textsuperscript{137} 585 S.E.2d 275 (S.C. 2003).
\textsuperscript{138} \textit{Id.} at 276.
\textsuperscript{139} \textit{Id.}
\end{flushleft}
reasoning in *Polzer v. TRW, Inc.*\(^{140}\). In *Polzer*, the court held that there was not enough of a relationship between the bank issuing the credit card and the identity thief or plaintiff to impose a duty of care.\(^{141}\) Therefore, applying the reasoning of *Polzer*, the court in *Huggins* held that there was not enough of a relationship between Huggins and Citibank to allow a cause of negligent enablement of impostor fraud to proceed.\(^{142}\)

Because past proposals to reduce identity theft have failed,\(^{143}\) courts should begin to recognize the cause of negligent enablement of impostor fraud in certain instances. Doing so likely will lead to a reduction of identity theft. However, in response to the worries stated in *Huggins*,\(^{144}\) courts should limit the application of this cause of action to instances where a financial institution is negligent in protecting the financial information of one of its customers, and this negligence allows an identity thief to exploit the customer’s information to the customer’s detriment.\(^{145}\) By requiring an existing customer relationship, the duty requirement of negligence would be fulfilled,\(^{146}\) yet it would not be overly broad, thus reducing the concerns of the court in *Huggins*.\(^{147}\) Therefore, to have an actionable negligent enablement of impostor fraud claim, one would have to show that an identity thief stole customer information from a financial institution, that the identity theft could have been prevented with reasonable security measures,\(^{148}\) and that one of the financial institution’s customers was harmed as a result.\(^{149}\)

141. *Id.*
143. *See supra* Part II.
144. *See supra* Part II.
145. For an example of such a situation, see *supra* Part I.
147. *Huggins*, 585 S.E.2d at 334.
148. It is beyond the scope of this Comment to propose “reasonable” security measures necessary to protect customer financial information. The legislative body enacting the statute should perform a cost-benefit analysis to determine what is reasonable.
149. The four basic elements of a negligence claim are duty, breach, cause, and harm. *Restatement (Second) of Torts* § 281 (2004). Normally, the causal link for negligence is broken by intervening criminal acts. *See id.* §§ 448–449 (2004). However, since customers must provide their personal information to financial institutions to do business and are not in the position to safeguard this information, it should be the responsibility of the financial institutions to protect customer information. Because identity theft is a well-documented problem and is on the rise, *see supra* notes 1–5 and accompanying text, financial institutions should expect identity thieves to attempt to gain access to customer information. Therefore, the intervening criminal acts of an identity thief should not relieve a negligent financial institution from liability.
IV. NEGLIGENCE PER SE UNDER THE GLB ACT

Yet another possible way for identity theft victims to seek relief for damages would be under the GLB Act. Since the GLB Act requires that financial institutions implement certain security measures, harm resulting from the violation of the GLB Act could be seen as negligence per se. By allowing claims under a negligence per se theory, victims would have an easier time proving negligence because violation of the security provisions under the GLB Act would be conclusive as to the financial institution’s negligence in implementing a security system. In addition, a negligence per se cause of action would be beneficial to financial institutions because they would know how to avoid liability for instances of identity theft. If financial institutions simply comply with the standards of the GLB Act, they would not be responsible for instances of identity theft that occur from a security breach under a negligence per se claim. Therefore, a negligence per se cause of action not only provides victims with a potential way to receive restitution for their harm, but it motivates financial institutions to either comply with the GLB Act or to face potential liability if an actual security breach occurs.

A negligence per se cause of action would also be beneficial to victims of identity theft because of the burden such an action would place on the financial institution. Unlike a cause of action under a negligent enablement of impostor fraud theory, it would not be the victim’s responsibility to prove that the financial institution lacked the requisite security measures. Once the government successfully proves that a financial institution has violated the GLB Act, the violation can serve as proof of negligence for an identity theft victim’s claim against a financial institution. Therefore, since identity theft victims would not have to bear the cost and responsibility of proving that the financial institutions were negligent with their security measures, claims would be

150. Skinner, supra note 29, at 57 n.196.
151. See supra notes 107–109 and accompanying text.
153. Id.
154. Because a negligence per se claim requires the violation of a statute or other legislative enactment, a claim would fail without such a violation. Id.
155. Id.
156. See supra Part II.E.1 for a description of security methods required by the GLB Act.
easier to bring for instances of identity theft. Hopefully the ease with which identity theft victims could bring suit against financial institutions that violate the GLB Act would encourage better compliance with the security measures of the GLB Act and lead to fewer occurrences of identity theft as a result of weak computer security measures.

V. CONCLUSION

Identity theft is a problem that is growing larger on a yearly basis. While there have been many attempts by legislatures and other governmental agencies in the past to reduce instances of identity theft, these attempts have not been very successful. In addition, current government responses to identity theft do not provide the victim with adequate restitution for the costs that he must incur to correct his credit. SB 1386 is a good start in placing responsibility on financial institutions for information security, but it is not enough. Therefore, courts should begin to recognize causes of action against financial institutions for their negligence in the protection of customer personal information. By allowing identity theft victims to sue financial institutions under a negligent enablement of impostor fraud theory or a negligence per se cause of action when a violation under the GLB Act occurs, financial institutions will attempt to increase security to avoid potential liability. Hopefully, this increase in security will lower instances of identity theft and provide customers with an added feeling of confidence knowing that their personal information is being guarded carefully.

ANTHONY E. WHITE

158. The cost of proving negligence would be shifted to the government when a violation of the GLB Act by a financial institution is alleged. Since the government has more resources and clout than an individual victim of identity theft, one could assume that the government is in a better position than an identity theft victim to prove a financial institution's negligence.

159. See supra notes 1-5 and accompanying text. Instances of identity theft continue to be a major problem as evidenced by the recent ChoicePoint security breach where nineteen billion public records were put at risk and tens of thousands of individuals were affected. See Senate Committee to hold hearings on identity theft, at http://www.cnn.com/2005/ALL POLITICS/02/24/congress.identitytheft.ap/index.html. This Comment went to press as this story first arose; however, the ChoicePoint situation only reaffirms the author's beliefs as stated in this Comment.

160. See supra Part II.

161. See supra Part II.E.

162. See supra Part II.E.2.

163. See supra Parts III and IV.