NORTH CAROLINA BANKING INSTITUTE

Volume 3 | Issue 1 Article 15

1999

Identity Theft: Prevention and Liability

Kristen S. Provenza

Identity Theft: Prevention and Liability

I. INTRODUCTION

Scott Clinton Gilbert incurred debts of more than $110,000.[1] He purchased three pickup trucks, two motorcycles, and a double-wide mobile home.[2] He was issued a driver's license, received a speeding ticket, was involved in an automobile accident, obtained employment, failed to pay taxes, opened bank accounts, and even obtained an FAA security pass at the Phoenix International Airport.[3] He also filed a bankruptcy petition for $44,756.97, obtained four life insurance policies, and claimed the status of a Vietnam veteran.[4] The problem with Gilbert's actions is that he did all of this using the identity of Robert Hartle.[5] Hartle knew nothing of Gilbert's actions until he received a phone call from a collection agency regarding an unpaid bill in the amount of $185.30 from a Las Vegas printing shop.[6] Hartle spent time, energy, and approximately $15,000 of his own money to clear his name and attempt to restore his good credit.[7]

One survey indicates that one in four adults have been the victim of some sort of identity theft.[8] In 1997, the United States Secret Service alone made nearly 9,500 arrests for crimes involving identity theft.[9] Those arrests involved crimes totaling $745 million in losses that were incurred by financial institutions and individual victims.[10] Furthermore, losses from identity theft are increasing,

---

1. *See* Michael Higgins, *Identity Thieves*, A.B.A. J., October 1998, at 42.
2. *See id.*
3. *See The Identity Theft and Assumption Deterrence Act: Hearings on S. 512 Before the Subcomm. on Technology, Terrorism and Government Information of the Senate Comm. on the Judiciary*, 105th Cong. 3 (1998) [hereinafter *Identity Theft Hearings*] (statement of Robert Hartle).
4. *See id.*
5. *See id.*
6. *See* Higgins, *supra* note 1 at 42.
7. *See Identity Theft Hearings*, *supra* note 3, at 3 (statement of Robert Hartle).
8. *See id.* at 24 (statement of Mari J. Frank).
9. *See id.* at 1 (opening statement of Chairman Jon Kyl).
10. *See id.*

nearly doubling in the last two years.[11] The U.S. Public Interest Research Group estimates that each year nearly 40,000 people are victims of identity theft.[12]

This Comment will first address the nature of identity theft and explain how the identity thief acquires the necessary personal information.[13] Next, the Comment will examine recent federal legislation that makes identity theft a crime.[14] Lastly, the Comment will discuss what efforts must be made to resolve the problems posed by identity theft.[15] The Comment will address the role that financial institutions can play in combating the problem[16] and the repercussions that they may face if the problem persists.[17] State law may provide causes of action for bank customers whose personal information is disclosed.[18] Also, if the financial industry is unsuccessful in self-regulating its confidentiality policies, federal regulations may be imposed.[19] However, if financial institutions stop depending upon common, easily obtainable personal information as their password protections and if they employ stricter privacy policies, government regulatory intervention may not be necessary to protect consumers.[20]

II. IDENTITY THEFT

A. Methods of Economic Identity Theft

Banks and other financial institutions are directly involved in the problem of identity theft. The theft can occur in a variety of ways. Identity theft can occur by the fraudulent use of existing deposit or credit accounts.[21] This "account takeover fraud" is perpetrated by

11. *See id.*
12. *See* Patrick Leahy, *Congress Clears Kyl-Leahy 'Identity Theft' Bill for President's Signature, Press Release*, Oct. 14, 1998, *available in* 1998 WL 19793204.
13. *See infra* notes 21-53 and accompanying text.
14. *See infra* notes 54-73 and accompanying text.
15. *See infra* notes 74-135 and accompanying text.
16. *See infra* notes 84-91 and accompanying text.
17. *See infra* notes 84-88 and accompanying text.
18. *See infra* notes 94-135 and accompanying text.
19. *See infra* notes 84-88 and accompanying text.
20. *See infra* notes 87, 139-41 and accompanying text.
21. *See H.R. 4321 - Financial Information Privacy Act: Hearing Before House*

changing the address of an existing credit account.[22] The individual is unlikely to know of the change until the following billing cycle, if the account is active, or until the account becomes past due.[23] The perpetrator can also fraudulently obtain funds by depositing an uncollectable check and requesting that part of the funds be paid in cash.[24] The identity thief can directly steal funds from an individual's account by impersonating the individual and effecting a wire transfer, or by making credit card purchases over the internet or by telephone.[25] The theft can even occur by cashing in an individual's investment holdings or insurance policies.[26]

In addition to using existing accounts, identity thieves can fraudulently open new accounts using an individual victim's personal information.[27] Identity thieves impersonate individual victims and obtain credit cards and/or finance property, including homes and automobiles.[28] Usually, the perpetrator can utilize one person's identity repeatedly, often without the victim's immediate knowledge.[29]

Identity thieves are further aided by the fact that current law does not provide victims of fraud with ready aid from law enforcement agencies.[30] Current federal laws utilized in criminal prosecutions for fraud include: the fraudulent use and production of identification documents,[31] access device fraud,[32] computer fraud,[33] wire fraud,[34]

Comm. on Banking and Financial Services, 105th Cong. 148-49 (1998) [hereinafter *Privacy Act Hearings*] (statement of Boris Melnikoff, Senior Vice President, Wachovia Corporation).

22. *See id.* at 148.

23. *See id.*

24. *See id.* at 150.

25. *See Privacy Act Hearings*, *supra* note 21, at 82 (statement of Robert Douglas).

26. *See id.* at 86.

27. *See Identity Theft Hearings*, *supra* note 3, at 5 (statement of James Bauer, Deputy Assistant Director, United States Secret Service, Office of Investigations).

28. *See id.* at 6.

29. *See id.*

30. *See id.* at 5.

31. *See* 18 U.S.C. § 1028 (1994), *amended by* 18 U.S.C.A. § 1028 (West Supp. 1998) (pertaining to fraud and related activity in connection with identification documents).

32. *See* 18 U.S.C. § 1029 (1994), *amended by* 18 U.S.C.A. § 1029 (West Supp. 1998) (pertaining to fraud and related activity in connection with access devices).

33. *See* 18 U.S.C. § 1030 (1994), *amended by* 18 U.S.C.A. § 1030 (West Supp. 1998) (pertaining to fraud and related activity in connection with computers).

34. *See* 18 U.S.C. § 1343 (1994) (pertaining to fraud by wire, radio, or television).

economic espionage,[35] and money laundering.[36] These statutes require an overtly fraudulent act or the creation of a fraudulent document before law enforcement can get involved.[37] The act of stealing a person's identity in order to commit any of the aforementioned crimes is not legally sufficient for individual victims to receive assistance and cooperation from law enforcement.[38] It is the fraudulent use of another person's identity that constitutes the crime.[39] Furthermore, because the individual whose identity has been misappropriated is not liable for the thief's debts,[40] the current law does not even view the individual as the victim of the crime.[41] Victims of identity theft often spend thousands of dollars and devote extensive time to restore their good credit ratings and convince creditors that they themselves incurred the perpetrator's debts.[42] It is also a priority of victims to have fraud warnings placed on their credit reports so that the perpetrator is not able to continue using the victim's identity to obtain further credit.[43] However, since the individual is not considered the actual victim of the crime, victims are left to their own devices to alert financial institutions, credit reporting agencies and creditors regarding fraudulent use of their personal information.[44]

B. Methods of Gaining the Necessary Personal Information

Identity thieves are able to commit their crimes through the use of an individual's personal, and sometimes confidential, information. This information includes data that banks and other financial institutions have access to and utilize in the course of their business.

---

35. *See* 18 U.S.C.A. § 1831 (West Supp. 1998) (pertaining to economic espionage).

36. *See* 18 U.S.C. § 1956 (1994), *as amended by* 18 U.S.C.A. § 1956 (West Supp. 1998) (pertaining to the laundering of monetary instruments).

37. *See Identity Theft Hearings*, supra note 3, at 13 (statement of James Bauer, Deputy Assistant Director, United States Secret Service, Office of Investigations).

38. *See id.*

39. *See id.*

40. *See, e.g.*, 15 U.S.C.A. § 1643 (1998) (pertaining to the liability of credit card holders).

41. *See* Higgins, *supra* note 1, at 43-44.

42. *See id.* at 46-47.

43. *See id.*

44. *See, e.g.*, Maria Ramirez-Palafox, *Identity Theft on the Rise: Will the Real John Doe Please Step Forward?*, 29 MCGEORGE. L. REV. 483, 483-88 (1998) (discussing the difficulties faced by individual identity theft victims).

Crucial information for identity thieves includes social security numbers, maiden names (both of the victim and the victim's mother), dates of birth, past addresses, and driver's license numbers.[45] The documents on which this information can be found include social security cards, state driver's licenses, birth certificates, passports, and voter registration cards and records.[46] Methods by which the information can be obtained include sorting through trash, looking through a co-worker's desk drawers, stealing mail, soliciting information through bogus job application or refund distribution schemes, and investigation on the Internet.[47]

Another common method of obtaining personal information, as well as confidential information such as account numbers, is so-called "pretext calling." This method involves the identity thief, or an information broker hired by the identity thief, misrepresenting his own identity in order to obtain personal and/or confidential information about the victim.[48] This may be done in one of two ways. First, the caller may identify himself as the individual victim and request information about that person's financial accounts from banks or other financial institutions.[49] Armed with personal information such as someone's name, address, social security number and/or mother's maiden name, the pretext caller is able to breach most confidentiality systems employed by a financial institution. A pretext caller may obtain information such as account balances, account numbers, payments made or due, and the dates and amounts of recent transactions.[50] Second, the caller may identify himself as an employee

45. *See* Higgins, *supra* note 1, at 46.

46. *See Identity Theft Hearings*, *supra* note 3, at 10 (statement of James Bauer).

47. *See id.* The Internet includes a wealth of personal information. Perpetrators may intercept information, such as credit card account numbers. Easily available information also includes names, phone numbers, and addresses. *See, e.g.*, *Switchboard: The Internet Directory* (visited Jan. 19, 1999) <http://www.switchboard.com> (providing names, addresses and phone numbers of individuals); *Welcome to WhoWhere?!* (visited Jan. 19, 1999) <http://www.whowhere.lycos.com> (providing names, addresses and phone numbers of individuals); *Yahoo! People Search* (visited Jan. 19, 1999) <http://www.people.yahoo.com> (providing names, addresses and phone numbers of individuals). The danger of having personal information available online must be balanced with benefits such as locating out-of-touch friends and loved ones.

48. *See, e.g.*, *Privacy Act Hearings*, *supra* note 21, at 83 (statement of Robert Douglas) (discussing methods in which identity thieves obtain an individual's personal information).

49. *See id.* at 82.

50. *See id.* at 85-86.

of the financial institution when calling the victim.[51] In so doing, the caller may elicit personal or confidential information, including account numbers and passwords.[52] This gathering of personal information with the intent of using the information for fraudulent purposes was not considered a crime; however, newly passed federal legislation has changed that.[53]

III. HOUSE BILL 4151 - THE IDENTITY THEFT AND ASSUMPTION DETERRENCE ACT OF 1998

A. Purpose of the Act

On October 30, 1998, President Clinton signed into law House Bill 4151, entitled the Identity Theft and Assumption Deterrence Act.[54] This Act is intended to close a gap in federal law that enables identity thieves to steal funds from financial institutions and to steal the identities of individuals without pursuit from law enforcement officials during the early stages of their actions.[55] The Identity Theft and Assumption Deterrence Act (the Act) enables federal law enforcement officials to initiate an investigation earlier than they otherwise could since the new law criminalizes the gathering of an individual's personal identifying information with the intent to perpetrate a fraud.[56] Additionally, the Act is needed to provide individual victims with some legal path to take.[57] While some states are taking the initiative in addressing the problems of identity theft, the problem is nationwide

51. *See id.* at 82.

52. *See id.* at 83.

53. *See infra* notes 54-73 and accompanying text.

54. *See* Pub. L. No. 105-318, 112 Stat. 3007 (codified as amended at 18 U.S.C.A. § 1028 (1998)). H.R. 4151 was introduced by Representative John B. Shadegg (R-AZ) on June 25, 1998. *See* 144 CONG. REC. H5402 (daily ed. Jun. 25, 1998). The bill was considered and passed by the House of Representatives on October 7, 1998. *See* 144 CONG. REC. H9993 (daily ed. Oct. 7, 1998). Senate Bill 512, 105th Cong. (1998), is a companion piece to House Bill 4151. Senate Bill 512 was introduced by Senator Jon L. Kyl (R-AZ) on March 21, 1997. *See* 144 CONG. REC. S2741 (daily ed. Mar. 21, 1997). Sentate Bill 512 was passed, as amended, by the Senate on July 30, 1998. *See* 144 CONG. REC. S9332 (daily ed. Jul. 30, 1998). The Senate considered and passed House Bill 4151 on October 14, 1998. *See* 144 CONG. REC. S12604 (daily ed. Oct. 14, 1998).

55. *See Hearings*, *supra* note 3, at 4-7 (statement of James Bauer).

56. *See id.*

57. *See id.*

and frequently crosses state lines.[58] Victims may live in one state while the perpetrator acts in another state also defrauding creditors who may be located in a third state.[59] The Act addresses this aspect by making the offense a federal crime, subject to federal enforcement and federal penalties, thus removing state law jurisdiction restrictions.[60]

B. Contents of the Act

Section 3 of the Act establishes the offense of identity theft.[61] The Act imposes criminal liability for identity theft on one who "knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a felony under any applicable state or local law."[62] "Means of identification" is defined to include an individual's name, social security number, date of birth, driver's license or government-issued identification number, taxpayer identification number, passport number, biometric data, electronic identification number, address or routing code, or telecommunication identifying information.[63]

The Act provides for criminal penalties of imprisonment of not more than twenty years and/or a fine.[64] The Act also amends the federal sentencing guidelines to allow the United States Sentencing Commission to consider such factors as the number of victims and the extent of their injuries, including harm to reputation and inconvenience;[65] the number of means of identification, identification documents or false identification documents utilized by the perpetrator;[66] and the value of the loss caused by the crime.[67]

---

58. *See id.* at 1-2 (opening statement of Chairman Jon Kyl).

59. *See id.*

60. *See id.*

61. *See* The Identity Theft and Assumption Deterrence Act, Pub. L. No. 105-318, § 3, 112 Stat. 3007 (codified as amended at 18 U.S.C.A. § 1028 (1998)).

62. *Id.* at § 3(a)(7).

63. *See id.* at § 3(d)(3).

64. *See id.* at § 3(b)(3). This maximum penalty is for violations that were committed "(A) to facilitate a drug trafficking crime . . . (B) in connection with a crime of violence . . . or (C) after a prior conviction under this section becomes final." *Id.*

65. *See id.* at § 4(b)(1).

66. *See id.* at § 4(b)(2).

Section 5 provides for the enactment of a centralized complaint and consumer education service for identity theft victims by the Federal Trade Commission (FTC).[68] No later than one year after the date of enactment of the Act, the FTC will establish procedures to log complaints by individuals who reasonably believe themselves to be the victims of identity theft as defined by the Act.[69] Additionally, the FTC will provide informational materials to those individuals,[70] and will refer the complaints to the appropriate entities, including, but not limited to consumer credit reporting agencies and law enforcement agencies.[71]

This Act will enable individual victims to contact and receive help from law enforcement agencies.[72] Such help may include searches for the perpetrator and may also include the act of filing a criminal report that will help inform and convince creditors and credit reporting agencies that a fraud has in fact occurred. The Act will also make identity theft a crime before the point at which other federal crimes, such as wire fraud or the fraudulent use and production of identification documents are committed.[73] Although the act of gathering the information with the requisite criminal intent is now a crime, one weakness of the new law is that it does not focus on the procedures used by perpetrators to gather confidential information. While the actual crime is technically being committed earlier under the new law, the methods of gathering confidential information should be targeted by lawmakers.

IV. ANALYSIS

A Other Legislative and Regulatory Measures Currently Under Consideration

One important piece of legislation addressing the issue of

67. *See id.* at § 4(b)(3).
68. *See id.* at § 5.
69. *See id.* at § 5(a)(1).
70. *See id.* at § 5(a)(2).
71. *See id.* at § 5 (a)(3)(A)-(B).
72. *See supra* notes 55-57 and accompanying text.
73. *See supra* notes 61-62 and accompanying text.

identity theft is the Financial Information Privacy Act of 1999 (Privacy Act). This proposed legislation directly affects the role of banks and other financial institutions in the gathering of confidential information by identity thieves. The Privacy Act was originally introduced during the 105th Congress[74] and has been reintroduced by House Banking Committee Chairman James Leach as House Bill 30.[75] The Privacy Act specifically targets identity thieves who obtain or attempt to obtain customer information from financial institutions by false pretenses.[76] The proposed legislation targets pretext callers who contact customers of financial institutions and make false or fraudulent statements with the intent to induce the customer into releasing customer information.[77] Provisions of the bill specify that law enforcement agencies are exempt from the act.[78] Additionally, the bill does not prevent any person from obtaining customer information otherwise available as a public record filed pursuant to section 3(a)(47) of the Securities Exchange Act of 1934.[79] Certain activities by financial institutions themselves are also exempt. This legislation does not prevent financial institutions from obtaining customer information in the course of testing security systems in place for maintaining confidential customer information, investigating alleged misconduct or negligence by officers, employees or agents of the financial institution, or recovering information obtained or received by another person.[80] Criminal penalties are provided and those penalties are expressly increased for aggravated cases.[81] Civil liability is also imposed upon any person who violates

74. H.R. 4321, 105th Cong. 1998.

75. *See* H.R. 30, 106th Cong. 1999; R. Christian Bruce, *Financial Services Reform: Leach Introduces New Version of H.R. 10, Hopes to Regain Momentum from Last Year*, 72 Banking Rep. (BNA) 47 (Jan. 11, 1999). A bill that addresses the protection of consumers' confidential financial information has also been introduced in the Senate. *See* Senate Bill 187, 106th Cong. 1999; Paul Sarbanes, *Senators Seek to Protect Consumers Confidential Financial Information, Press Release*, Jan. 21, 1999, *available in* 1999 WL 2221911.

76. *See* R. Christian Bruce, *Privacy Bill Clears House Banking Panel With Amendments Allowing Court Action*, 71 Banking Rep. (BNA) 256 (Aug. 10, 1998).

77. *See* H.R. 30, 106th Cong. § 1003(a)(2) (1999).

78. *See id.* at § 1003(c).

79. *See id.* at § 1003(e).

80. *See id.* at § 1003(d).

81. *See id.* at § 1006. The circumstances in which the increased penalties apply are based upon violations of this act in accordance with violations of other law involving more than $100,000 in a twelve-month period. *See id.*

the Privacy Act; however, financial institutions are expressly excluded from liability and are entitled to recover damages and attorney's fees from those who violate the Privacy Act.[82]

The Privacy Act does not address all methods in which pretext callers and identity thieves obtain confidential consumer information, but makes some of the more common methods illegal. The bill strikes some balance between the privacy interests of consumers and the legitimate uses of pretext calling because the legislation does not prohibit the use of pretext calling by law enforcement agencies. Chairman Leach described the bill as "both pro-consumer and pro-privacy . . . [and as] respond[ing] to an urgent threat to the integrity of financial institutions themselves."[83] The American Bankers Association has announced that it supports the legislation but opposes any efforts to codify industry guidelines on privacy, choosing instead to continue with self-regulation in the privacy area.[84]

The Office of the Comptroller of the Currency (OCC), the regulator of national banks, has issued statements in regard to the problem of privacy and pretext calling. Amidst self-regulatory efforts to protect the privacy of confidential consumer information, Acting Comptroller Julie L. Williams has called upon the banking industry to demonstrate leadership in the protection of customer privacy.[85] The OCC has warned the banking industry of the dangers of information brokers and the method of pretext calling as a means of obtaining information from financial institutions.[86] The OCC suggests that the use of two common personal identifiers, social security numbers and mothers'maiden names, should be avoided in favor of more sophisticated passwords less easily obtained.[87] The OCC also suggests

82. *See id* at § 1005. Actual damages would equal the greater of the actual damages incurred by the customer or by the financial institution as a result of the violation or any amount received by the perpetrator. *See id.* at § 1005(1).

83. James A. Leach, *House Banking Committee Approves Privacy Bill, Press Release*, Aug. 5, 1998, *available in* 1998 WL 7326130 (referring to H.R. 4321).

84. *See* R. Christian Bruce, *Privacy Bill Clears House Banking Panel With Amendments Allowing Court Action*, 71 Banking Rep. (BNA) 257 (Aug. 10, 1998).

85. *See* OCC News Release 98-50, *Acting Comptroller Julie L. Williams Urges Industry Leadership on Consumer Privacy* (May 8, 1998) (remarks of Julie L. Williams before the Banking Roundtable Lawyers Counsel).

86. *See* OCC News Release 98-86, *OCC Warns Banks About Pretext Calling by Information Brokers* (Aug. 20, 1998).

87. *See* Robert O'Harrow, Jr., *Banks Told to Boost Data Safeguards; Regulators Call Procedures on Customer Information Inadequate to Curb Internet Abuses*, WASH. POST,

that banks routinely check their security systems, possibly even by hiring their own pretext callers as a test.[88]

B. *Protective Measures Available to Financial Institutions*

The standard of what constitutes reasonable protection by financial institutions is evolving. This evolution is due in part to technological advances. New fraud prevention methods feature biometrics, including fingerprinting, iris scanning, and voice or face recognition.[89] While many of these methods are still too cost-prohibitive to be effective on a large scale, fingerprinting is currently being utilized by some financial institutions with some success. Individuals who wish to cash a check at a bank with which they do not have an account may be required to provide a thumbprint. The benefit of fingerprinting in combating check fraud is two-fold. First, it serves as a deterrent for those who would otherwise have committed fraud but are hesitant to provide incriminating evidence. Second, for those who do provide a fingerprint, law enforcement has useful physical evidence from the start of an investigation.[90] One 1996 study showed a 47% year-to-date reduction in check fraud losses.[91]

In addition to the economic losses that can be prevented by utilizing stronger privacy protections, financial institutions will also benefit from less government regulation and greater freedom for industry self-regulation.[92] Without adequate privacy protections,

---

Aug. 21, 1998, at G1.

88. *See id.*

89. *See, e.g., Privacy Act Hearings, supra* note 21, at 151(statement of Boris Melnikoff) (discussing new technologies and techniques that may aid in fraud prevention). For a discussion of biometrics, see generally John D. Woodward, *Biometric Scanning, Law & Policy: Identifying the Concerns—Drafting the Biometric Blueprint*, 59 U. PITT. L. REV. 97 (1997) (exploring biometrics and biometric applications as well as the associated legal and policy issues); David A. Petti, *An Argument for the Implementation of a Biometric Authentication System ("BAS")*, 80 J. PAT. & TRADEMARK OFF. SOC'Y 703 (1998).

90. *See Privacy Act Hearings, supra* note 21, at 151 (statement of Boris Melnikoff).

91. *See id.* (citing a 1996 study by the Clearing House Association of the Southwest of the effect on check fraud losses following implementation of practices fingerprinting non-customers cashing checks at financial institutions).

92. *See* Julie L. Williams, *Remarks by Julie L. Williams Acting Comptroller of the Currency before the Consumer Bankers Association, Aventura, Florida* (October 26, 1998) (visited Jan. 26, 1999) <http://www.occ.treas.gov/ftp/release/98-109a.txt>. Ms. Williams refers to "the ability [fof financial institutions] to shape their own policies and

government regulations will likely be imposed, thus minimizing the industry's ability to impose and enforce its own policies.[93] Another benefit of stronger privacy protections is that they may reduce the bank's potential liability to customers under state law causes of action relating to disclosures of personal and/or confidential information.

C. *Causes of Action Available to Individual Victims*

Existing state law may provide causes of action for customers against financial institutions for releasing confidential information to third parties. These causes of action may be grounded in tort, such as negligence or an invasion of privacy, or they may be grounded in contract, such as breach of an implied contract. Plaintiffs may also utilize specific state statutes.

The factual contexts of the following cases typically do not involve identity theft. However, the following cases address available legal recourses for customers of financial institutions whose employees have disclosed personal and/or confidential information in other contexts. Often, the disclosure was made to law enforcement officials; however, the holdings may be extended to apply to the situation of identity theft since courts have addressed that issue in terms of permissible disclosures to third parties and in terms of duties owed by banks to their customers. The following cases provide some examples of how state courts have treated customers' causes of actions and give an indication of how courts may react to cases pertaining to identity theft.[94]

---

avoid being subject to the one-size-fits-all approach that might be mandated under the law" as a benefit of self-regulation. *Id.*

93. *See id.*

94. *See* Thomas C. Russler and Steven H. Epstein, *Disclosure of Customer Information to Third Parties: When is the Bank Liable?*, 111 BANKING L.J. 258 (1994) (examining the case law interpreting the legal duties of banks); Roy Elbert Huhs, Jr., *To Disclose or not to Disclose Customer Records*, 108 BANKING L.J. 30 (1991) (discussing banks' conflicting duties of maintaining the confidentiality of customer records and the duty to disclose those records under special circumstances); THOMAS P. VARTANIAN ET AL., 21ST CENTURY MONEY, BANKING & COMMERCE § 12.03, at 297-99 (1998) (addressing a bank's duty of confidentiality in light of the problem of identity theft). *See generally* Cheryl B. Preston, *Honor Among Bankers: Ethics in the Exchange of Commercial Credit Information and the Protection of Customer Interests*, 40 KAN. L. REV. 943 (1992) (addressing the exchange of commercial credit information, the effect on the interests of customers in accuracy, privacy, and fairness, and the insufficiencies of self-regulation).

In *Suburban Trust Company v. Waller*,[95] the plaintiff sought to cash an income tax refund check approximately one month after opening an account.[96] When the bank refused to cash the check because the plaintiff did not have enough money in his account to cover the check, the plaintiff instead went to the United States Treasury Department in Washington, D.C. and cashed the check there.[97] Plaintiff returned to his bank and deposited $800 in fifty and one hundred dollar bills, numbered sequentially.[98] The teller found this suspicious, and bank personnel proceeded to inform the Federal Bureau of Investigation and the Montgomery County Police Department.[99] An assistant security officer for the bank provided the police with plaintiff's name, address, physical description, employment, and deposit information, as well as bank surveillance photographs.[100] This disclosure led to the identification of plaintiff by the victim of a local residential robbery, and the plaintiff was arrested.[101] After the victim retracted the identification, the charges against the plaintiff were dropped.[102]

Plaintiff filed suit against the bank alleging an invasion of privacy and a breach of implied contract.[103] The court of appeals affirmed the lower court's ruling as to the bank's liability for wrongful disclosure.[104] The Court of Special Appeals of Maryland stated that:

> We think that a bank depositor in this State has a right to expect that the bank will, to the extent permitted by law, treat as confidential, all information regarding his account and any transaction relating thereto. Accordingly, we hold that, absent compulsion by law, a bank may not make any disclosures concerning a depositor's account without the express or implied

95. 408 A.2d 758 (Md. Ct. Spec. App. 1979).
96. *See id.* at 760.
97. *See id.*
98. *See id.*
99. *See id.* at 761.
100. *See id.*
101. *See id.*
102. *See id.*
103. *See id.*
104. *See id.* at 765-66. The trial judge directed a verdict for the plaintiff. *See id.*

consent of the depositor. [105]

This standard arguably enables customers to bring an action against their financial institution for unauthorized disclosure of personal information. The issue of consent may hinge on the institution's policies regarding the confidentiality of customer information.

In *Indiana National Bank v. Chapman*,[106] a bank loan officer disclosed information to a state police officer regarding the plaintiff's automobile loan payments.[107] Plaintiff's car had been reported stolen and was later found in a burned-out condition.[108] Based in part on information provided by the loan officer that the plaintiff had missed a monthly payment, plaintiff was charged with fourth degree arson.[109] During trial, the prosecution moved for dismissal of the charge following testimony that it believed indicated a different account of plaintiff's payment history.[110]

Plaintiff filed suit against the bank alleging invasion of privacy, slander, breach of implied contract, and negligence.[111] The Court of Appeals of Indiana held that a legitimate inquiry by law enforcement could not give rise to a private cause of action for invasion of privacy.[112] In support of this ruling, the court cited *United States v. Miller*[113] in which the United States Supreme Court reversed a lower court ruling finding that bank records, such as checks and deposit slips, were "the business records of the bank and not the private papers of the respondent"[114] and therefore not within a "zone of privacy."[115] The court of appeals then ruled in favor of the bank as to the slander allegation because the bank had a qualified privilege

105. *Id.* at 764.
106. 482 N.E.2d 474 (Ind. 1985).
107. *See id.* at 475-76.
108. *See id.* at 476.
109. *See id.*
110. *See id.* at 477.
111. *See id.* at 476.
112. *See id.*, at 478.
113. 425 U.S. 435 (1976).
114. *Indiana Nat'l Bank*, 482 N.E.2d at 478.
115. *See id.* The Court in *Miller* held that such information is voluntarily conveyed to the bank by the customer so that the customer could have no legitimate expectation of privacy. *See United States v. Miller*, 425 U.S. 435, 442 (1976).

regarding communications made in good faith pursuant to a legitimate law enforcement investigation.[116] Additionally, the court found no evidence of malice on the part of the bank.[117]

In addressing plaintiff's claim that the bank breached an implied contract, the court held that a bank has an implied contract with customers not to disclose certain financial information.[118] The court acknowledged exceptions to this general principle, but limited those exceptions to situations in which a public duty has arisen.[119] This public duty test is satisfied if disclosures are made in conjunction with a legitimate law enforcement investigation.[120] In ruling on plaintiff's negligence action, the court found that there was no evidence supporting a breach of the bank's duty not to disclose customer information to someone who does not have a compelling public interest.[121] Again, the court acknowledged that duties are owed by financial institutions to their customers regarding account information, and again the court limited the exceptions to those duties. Therefore, in cases of identity theft and pretext calling, financial institutions may be exposed to liabilities for disclosures to someone who does not have a public interest in the information.

In *Milohnich v. First National Bank of Miami Springs*,[122] the plaintiff brought suit against the defendant for the disclosure of confidential information to third parties that resulted in legal actions against the plaintiff by the third parties. The District Court of Appeal of Florida addressed whether or not the bank breached an implied contractual duty to the plaintiff to keep the plaintiff's personal information confidential.[123] The court relied on two earlier cases to arrive at a decision that acknowledged that banks have a duty to depositors to keep account information confidential and not to divulge such information to third parties.[124] The Florida Supreme Court

116. *See Indiana Nat'l Bank*, 482 N.E.2d at 479-80 (citing *Conn v. Paul Harris Stores*, 439 N.E.2d 195, 200 (Ind. 1982); *Zakas v. Mills*, 251 S.E.2d 135 (Ga. Ct. App. 1978)).

117. *See id.* at 480.

118. *See id.*

119. *See id.* at 480-82.

120. *See id.* at 482.

121. *See id.* at 482-84.

122. 224 So. 2d 759 (Fla. Dist. Ct. App. 1969).

123. *See id.* at 760.

124. *See id.* at 760-62. The court made note of *Tournier v. National Provincial & Union Bank*, 1 K.B. 461 (1924), a leading English case which held that terms that were

modified the *Milohnich* ruling in *Barnett Bank of West Florida v. Hooper.*[125] The *Hooper* court limited the *Milohnich* holding to depositors (thus excluding loan holders) and provided for four circumstances in which disclosure was permissible.[126] The court added that other circumstances may allow for disclosure.[127]

One case that directly involves identity theft is *Andrews v. Trans Union Corporation.*[128] In this case, the plaintiff was suing two credit reporting agencies in connection with their release of credit reports in response to an identity thief's credit application, and also in connection with the inclusion in the plaintiff's credit report of information regarding an imposter's credit activities.[129] The action was brought under the Fair Credit Reporting Act,[130] and it focused in part on issues of the accuracy of the credit reports and the permissibility of providing the plaintiff's credit reports.[131] While the district court granted summary judgment for the defendants on the permissibility claim, the court denied summary judgment as to issues of accuracy and the failure to correct inaccurate information.[132]

State law actions may be brought by the states themselves. Connecticut Attorney General Richard Blumenthal has announced that his office is investigating information brokers in connection with

---

necessarily in the contemplation of the parties making a contract will be implied by the court, and that it is implied that a bank will not disclose account information except in certain circumstances. *See Milohnich*, 224 So. 2d at 760-61. The court noted that *Peterson v. Idaho First National Bank*, 83 Idaho 578, 367 P.2d 284 (1961) comported with the *Tournier* court's holding that a bank has an implied duty not to disclose a depositor's account information unless authorized by law or by the depositor. *See Milohnich*, 224 So. 2d at 760.

125. 498 So. 2d 923, 924-25 (Fla. 1986).

126. *See id.* at 925. The four circumstances are: (1) under compulsion of law; (2) pursuant to a public interest; (3) pursuant to the bank's interests; or (4) when made with the expressed or implied consent of the customer. *See id.*

127. *See id.* In this particular case, the additional "special circumstance" under which a bank may disclose the account information of a depositor was when the bank had actual knowledge of a fraud that was being perpetrated on a customer by another bank customer. *See id.* In *Hooper*, the customer brought action because the bank failed to disclose the fraud. *See id.* at 924.

128. 7 F. Supp. 2d 1056 (C.D. Cal. 1998).

129. *See id.* at 1063-65.

130. 15 U.S.C.A. § 1681 (West Supp. 1998). *See, e.g.*, Albert S. Jacquez & Amy S. Friend, *The Fair Credit Reporting Act: Is it Fair for Consumers?*, 5 LOY. CONSUMER L. REP. 81 (1993) (summarizing the FCRA and the legislative purpose for its enactment).

131. *See Andrews*, 7 F. Supp. 2d at 1060.

132. *See id.* at 1084.

possible privacy violations.[133] He also said that there are plans to subpoena as many as six banks operating in Connecticut.[134] Those banks may face some responsibility for privacy violations.[135]

As these cases illustrate, customers of financial institutions face obstacles in bringing actions for the improper release of confidential information. However, courts have allowed these suits in many cases and plaintiffs have found success. While banks that divulge customer information enjoy some liability protection, the implied contractual right of nondisclosure suggests that stricter security measures be implemented by financial institutions for the protection of their customers. In light of available technology and the relative ease with which identity thieves can obtain personal information, customers will expect financial institutions to execute more rigid security schemes.

V. CONCLUSION

Identity theft is a widespread, national problem.[136] The Identity Theft and Assumption Deterrence Act of 1998 is an important first step in addressing the problem and trying to aid all victims of identity theft.[137] However, the act does not address any of the specific means by which information is being misappropriated.[138] Legislation may help solve that aspect of identity theft, but financial institutions themselves can also do much to prevent unwarranted disclosures of customer information.[139] Possible strategies that financial institutions may utilize include no longer using traditional passwords such as social security numbers or mothers' maiden names and/or employing biometric techniques to prevent impersonation by identity thieves or pretext callers.[140] The benefits of employing these techniques include lower economic losses due to fraud, the avoidance of additional layers

133. *See* Jon G. Auerbach et al., *Prying Eyes: With These Operators, Your Bank Account Is Now an Open Book*, WALL ST. J., Nov. 5, 1998, at A1.

134. *See id.*

135. *See id.*

136. *See supra* notes 1-12, 21-53 and accompanying text.

137. *See supra* notes 53-73 and accompanying text.

138. *See supra* notes 74-83 and accompanying text.

139. *See supra* notes 84-91 and accompanying text.

140. *See supra* notes 87-90 and accompanying text.

of federal regulation, and a minimization of state law actions by customers.[141] One additional potential benefit is a happier customer base. One customer whose account information had been disclosed to a pretext caller said that he is considering changing banks because of a lack of security in the bank that divulged his account balances to an information broker.[142] That may provide the greatest motivation for financial institutions to prevent unauthorized disclosures and to tighten existing security practices.

KRISTEN S. PROVENZA

141. *See supra* notes 90-135 and accompanying text.
142. *See* Auerbach et al., *supra* note 133, at A13.