DATA SECURITY BREACH AND THIRD PARTY IDENTITY THEFT: BUSINESSES FACE A NEW ERA OF LEGAL LIABILITY IN AFTERMATH OF EVOLVING CONSUMER FRAUD

Jennifer Barger Johnson and Aubree Helvey

According to the Federal Trade Commission's 2005 annual report on consumer fraud, identity theft is the fastest growing form of consumer fraud in the United States.[1] It also tops the list as the most commonly reported type of consumer fraud.[2] Identity theft occurs when one steals the name, address, social security number, or other personal identification and uses the information to obtain credit or to purchase goods or services.[3] Common examples of identity theft include using another's identity to open a credit card account or bank account, rent an apartment, obtain a loan, gain employment, or access a current bank or credit card account.[4] Perhaps the most damaging form of identity theft occurs when the victim is arrested for crimes committed when the thief has wrongly used the victim's identity.[5] The number of reported identity theft cases continues to increase each year, with over

* Assistant Professor of Legal Studies and Assistant Chairperson, Department of General Business, University of Central Oklahoma, College of Business Administration, Edmond, OK. Member, Oklahoma Bar, 1998, Arkansas Bar, 1998, and Texas Bar, 2002; J.D., 1998, University of Arkansas, School of Law, Robert A. Leflar Law Center; B.B.A., Management, 1993, Cameron University; A.A., Business Management, 1992, Carl Albert State College, Poteau, OK.

**Assistant Professor of Business Law and Assistant Dean, School of Business, Cameron University, Lawton, OK. Member, Oklahoma Bar, 2002; J.D., 2002, University of Oklahoma College of Law; Bachelor of Accounting, 1999, Cameron University; Certified Public Accountant, 2002.

[1] *See* Federal Trade Commission, Consumer Fraud and Identity Theft Complaint Data, January-December 2005, January 2006, 4. Retrieved Sept. 28, 2006, from http://www.consumer.gov/sentinel/pubs/ Topl0Fraud2005.pdf. [hereinafter *FTC Identity Theft Report], See also* R. Bradley McMahon, *After Billions Spent to Comply With HIPAA and GLBA Privacy Provisions, Why is Identity Theft the Most Prevalent Crime in America?* 49 VILL. L. REV. 625, 660 n. 2 (2004) (summarizing statistics on prevalence of identity theft in America).

[2] *See FTC Identity Theft Report, supra* note 1 (noting identity theft complaints totaled 37% of all consumer fraud claims for 2005).

[3] *See* 18 U.S.C. § 1028 (2000); *see also* S. Rep. No. 150-274, at 6 (1998), and Jeff Sovem, *The Jewel of Their Souls: Preventing Identity Theft Through Loss Allocation Rules,* 64 U. PlTT. L. Rev. 343, 406 n. 4 (2003) (noting that many people use the terms identity theft and identity fraud interchangeably and providing an explanation of the difference).

[4] *See* Sean B. Hoar, *Identity Theft: The Crime of the New Millennium,* 80 OR. L. REV. 1423, 1426-1427 (2001); *see also FTC Identity Theft Report,* at 3. ("Credit card fraud (26%) was the most common form of reported identity theft followed by phone or utilities fraud (18%), bank fraud (17%), and employment fraud (12%). Other significant categories of identity theft reported by victims were government documents/benefits fraud (9%) and loan fraud (5%).").

[5] *See* Patrick v. Union State Bank, 681 So.2d 1365 (Ala. 1996) (Bridgette Patrick was arrested on a check fraud warrant related to actions of an identity thief and detained in eleven jurisdictions before being released).

255,500 complaints reported in 2005 alone.[6] Consumers can be grateful that recent trends show that the rate of increase is slowing.[7]

The idea of identity theft often conjures images of a thief who steals credit cards, checkbooks, and driver's licenses by riffling through personal trash cans, mail boxes, or by stealing purses and wallets.[8] While these traditional methods are still used by identity thieves, recent news accounts reveal a different reality: many identity thieves are now stealing identifications directly from commercial institutions that have been entrusted with consumer information.

In carrying out normal business practices, many companies are charged with care, custody, and control of both customer and employee data. For example, to complete a credit card sale, either online or in a traditional purchase, a merchandiser will acquire the customer's name, address, and credit card account number. A copy of the information will be transmitted to the credit card company for reimbursement. Personnel files often contain an employee's name, address, social security number, and sometimes bank account number for automatic payroll deposits. Although sometimes maintained in paper form, customer and employee data are more often collected in an electronic format. Private records are at risk for theft and unauthorized exposure when a company fails to implement and maintain adequate security measures to protect consumer data. One might debate whether security breaches are a new occurrence or, alternatively, are an organizational weakness that has existed for some time and is just beginning to receive public attention. Either way, recent news accounts reveal the true vulnerability of data. According to the Privacy Rights Clearinghouse,[9] from February 2005 until September 2006, over 200 companies experienced data breaches,[10] with at least 93,804,336 different records compromised during this time period.[11] Obviously, the volume of compromised records is staggering and clearly indicates an existing weakness in data security. Releasing private records to unauthorized individuals greatly enhances the risk that the customer or employee will fall victim to identity theft.

One of the largest known breaches of consumer data was reported in 2005, when ChoicePoint revealed the company had unintentionally and erroneously sold private information on over 163,000 individuals to a group of criminals[12] posing as

[6] *See FTC Identity Theft Report, supra* note 1, at 4.

[7] Christopher Conkey, *ID Theft Complaints Still Rising, but Rate of Increase Slows*, Post Gazette, Jan 26, 2006. Retrieved Sept. 29,2006, from http://www.post-gazette.com/pg/06026/644909.stm.

[8] *See* Holly K. Towle, *Identity Theft: Myths, Methods, and New Law*, 30 RUTGERS COMPUTER & TECH. L.J. 237,239 (2004).

[9] The Privacy Rights Clearinghouse is a nonprofit organization formed to inform consumers and engage in consumer advocacy. Privacy Rights Clearinghouse, A Chronology of Data Breaches, posted April 20, 2006, updated Sept. 27, 2006 Retrieved Sept. 28, 2006 from http://www.privacyrights.org/ar/ ChronDataBreaches.htm [hereinafter *Privacy Rights Clearinghouse Report],*

[10] *See Privacy Rights Clearinghouse Report, supra* note 9.

[11] *See id.*

[12] *See* Complaint United States of America v. ChoicePoint, Inc., Civ. Action No. 06-CV-0198, at 1J12 (N.D. Ga, Atlanta Div., Jan. 30, 2006). Retrieved Sept. 28, 2006 from http://www.ftc.gov/os/caselist/ choicepoint/0523069complaint.pdf.

real estate agents.[13] Approximately 800 cases of identity theft resulted from this data breach.[14] ChoicePoint, a data broker that maintains 10 billion records on private consumers, is in the business of providing background checks for private businesses and other governmental agencies.[15] These data include consumer credit histories, Social Security numbers, and employment information.[16] Some victims in this case face substantial monetary effects if the thief s activities negatively affect the victim's credit rating. For example, a bank might refuse to lend money to the victim or might require the victim to pay a higher interest rate. Victims also spend countless hours proving to businesses and the credit agency that these resulting charges are fraudulent. In extreme cases, negative credit reports have prevented victims from obtaining employment. Identity theft victims have the legal right to seek reimbursement of their losses from a convicted identity thief. In reality, victims often remain uncompensated, because the perpetrator either cannot be located or is judgment-proof. Both regulatory agencies and individual victims have started pointing fingers at, and requesting financial reimbursement from, the entities that suffered the security breach.

The purpose of this article is to examine several of the emerging legal issues facing all entities that suffer a breach of data security. The legal vulnerability of all entities, regardless of the size or industry, is discussed and the methods used by identity thieves to steal business records are examined. An emerging method of retribution brought by the Federal Trade Commission's unfair and deceptive trade practice charges against entities failing to provide adequate data security is also discussed. Some of the Federal Trade Commission settlements in these cases have included substantial monetary fines, a portion of which has been segregated for reimbursement of harmed consumers. Not all Federal Trade Commission settlements include a reimbursement fund and individuals do not have a private cause of action under federal law for unfair and deceptive trade practices. However, states also have deceptive trade practices acts, many of which permit private lawsuits and treble damages. An overview of potential liability under state law deceptive trade practices acts is also provided.

Negligence actions filed against business entities generally involve two types of plaintiffs suffering from the data breach. The first plaintiff group consists of a customer or employee who had an ongoing relationship with the entity when the records were stolen. The second type of plaintiff lacks an existing relationship with the defendant business, but the business somehow compromised security of the plaintiffs private data. For example, one bank opened a checking account for an imposter, even though the imposter could not present photo identification and would

[13] *See* Federal Trade Commission, Press Release, ChoicePoint Settles Data Security Breach Charges; to Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress, Jan. 26, 2006. Retrieved Sept. 28, 2006 from http;// www.ftc.gov/opa/2006/01/choicepoint.htm.

[14] *See id.*

[15] *See* Bob Sullivan, *Database giant gives access to fake firms: ChoicePoint warns more than 30,000 they may be at risk*, MSNBC.com, Feb. 14, 2005. Retrieved Sept. 28, 2006 from http://www.msnbc.msn. com/id/ 6969799/.

[16] *See id.*

not give a physical address.[17] The imposter proceeded to write numerous bad checks and the true individual was arrested. This article examines how rulings have been different depending upon the type of plaintiff.

I. How Thieves Breach Data Security

As a result of the portable nature of electronic data, many individuals are finding personal information at risk of theft by identity thieves. The federal government has addressed customer privacy by drafting legislation aimed at protecting private customer information. The most notable of these federal laws are the Gramm-Leach-Bliley Act (GLBA)[18] and the Health Insurance Portability and Accountability Act (HIPAA).[19] Although they are illustrative of Congress's proactive approach to preventing identity theft, it is important to note that these Acts do not necessarily apply to all commercial entities, but instead each Act is generally tailored to a defined niche of consumers and entities. For instance, the GLBA's "safeguards rule" only applies to financial institutions that provide financial products or services to consumers. Similarly, HIPAA's scope is limited to the health care industry. This article focuses on legal theories that affect all businesses, regardless of the industry.

In order to avoid theft of data, a company must first acknowledge the various organizational weaknesses that lead to security breaches. A 2002 study by TransUnion revealed that theft of business records, which can include both employee and customer records, causes more identity theft than lost wallets, stolen mail, or stolen purses. Thieves can acquire business records by a variety of methods and these are presented herein in three categories: (1) thieves acquire electronic records by hacking into insecure databases; (2) employees steal business records; and (3) data are lost or stolen as a result of weak logistics or weak business procedures.

A. *Insecure Electronic Databases: Hacking*

In 2005 alone, approximately 44 different company databases were hacked into by unauthorized individuals."[1] The security breaches compromised over 42 million records." CardSystems was one of the companies that fell victim to a hacker,

[1/] *See Patrick, supra* note 5.

18 Gramm-Leach-Bliley Act of 1999, Pub. L. No. 106-102, 111 Stat. 1338 (1999)(codified in various sections of 12 U.S.C. and 15 U.S.C.)..

[19] Health Insurance Portability and Accountability Act of 1996, Pub L No 104-191 110 Stat 1936

(1996)(codified at 42 U.S.C. § 1301 *etseq.).*

20 See Stephanie Armour, *Employment records prove ripe source for identity theft,* USA TODAY, Jan. 23, 2003. Retrieved Sept. 28, 2006 from http://www.usatoday.com/money/workplace/2003-01-23-idtheft- cover_x.htm.

[21] *See Privacy Rights Clearinghouse Report, supra* note 10

[22] *See id.*

exposing over 40 million customer records to potential theft.[23] CardSystems provided verification services and software for several credit card companies.[4] Customer account numbers and other personal information were stored on CardSystems' database.[25] The Federal Trade Commission has begun to look more closely at companies experiencing security breaches. The FTC acknowledges companies cannot provide complete defenses against hackers.[26] The regulatory agency will instead examine whether the current security measures are "reasonable" measures for protecting "sensitive consumer information."[27] The same analysis applies to negligence cases. If a court determines that a defendant company owes the plaintiff a duty of care, the trier of fact will then decide whether the defendant company's security measures were reasonable.

Although data security is one of the prime concerns for many businesses, numerous cases of leaked data occur outside the online forum. A study by the Council of Better Business Bureaus and Javelin Strategy & Research reveals that the Internet is not the main source of identity theft.[28] Rather "offline" channels contribute to approximately 90% of all reported cases.[29] No matter how secure a computer network may be, insiders can always collude to obtain information that an outsider might be unable to access.

B. *Employee Theft of Data*

Employee theft can result from a scheme developed internally by employees or externally wherein a third party contacts an employee and offers to pay for access to customer and employee personal information. In May 2005, four large U.S. banks, including Bank of America Corporation and Wachovia Corporation, disclosed that account information was stolen for more than 670,000 customers, in one of the biggest security breaches in the banking history.[30] Upper level bank

[23] Federal Trade Commission, Press Release, CardSystems Solutions Settles FTC Charges: Tens of Millions of Consumer Credit Card Numbers Compromised, Feb. 23, 2006. Retrieved Sept. 28, 2006 from http://www.ftc.gov/opa/2006/02/cardsystems_r.htm..

[24] *See id.*

[25] *See id.*

[26] *See* Federal Trade Commission, Prepared Statement of the Federal Trade Commission Before the House Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census Committee on Government Reform, Apr. 21, 2004, at 4 [hereinafter *FTC Statement].* Retrieved Sept. 28, 2006 from http://www.ftc.gov/os/2004/04/042104cybersecuritytestimony.pdf.

[27] *See id.* (noting that "a company's security procedures must be appropriate for the kind of information it collects and maintains. Different levels of sensitivity may dictate different types of security measures ").

[28] *See New Research Shows Identity Fraud Growth Is Contained and Consumers Have More Control Than They Think,_Javelin Strategy and Research,* Jan. 31, 2006. Retrieved March 1, 2006 from http://www.javelinstrategy.com/products/AD35BA/delivery.pdf.

[29] *See id.*

[30] *See* CNN Money, *Data breach may be biggest yet: Account info at Bank of America, Wachovia sold by employees: more arrests expected, N.J. police say,* CNN.com, May 23, 2005. Retrieved Sept. 28, 2006 from http://money.cnn.com/2005/05/23/news/fortune500/bank_info/. The four banks involved in this case were identified in the article as Bank of America Corp., Wachovia Corp., Commerce Bancorp, and PNC Financial Services Group, Inc.

employees sold customer account information, typically for as little as $10 a name, to Orazio Lembo.[31] Lembo allegedly sold the illegally acquired data to various clients, including more than 40 law firms and collection agencies.[32] Authorities estimate that Lembo earned millions over the past four years, while his coconspirators likely netted tens of thousands of dollars.[33]

Bank of America employees stole customer data. However, many instances of employee theft involve employee records.[34] An estimated 90% of stolen business records consist of employee records, rather than customer lists or customer identification.[35] The human resource files of many companies often contain employees' Social Security numbers, addresses, employment histories, and wage information, including direct deposit authorizations with checking account numbers. Seeing the marked increase in employee theft, the major U.S. financial institutions have begun working toward a cooperative database, which would assist in identifying potential employees that might pose a risk.[36] The database will identify employees who were fired from financial institutions for compromising customer data.[37]

Employee theft is perhaps one of the most threatening outlets for data theft, because organizations cannot realistically design a foolproof method of prevention. However, the third category of data loss concerns inadequate business procedures that could be prevented.

C. *Weak Logistics and Weak Business Procedures*

Inadequate business practices have contributed to a many cases of data theft. In 2005, approximately 8 million records were lost when laptops or backup tapes were stolen.[38] CitiFinancial lost records on 3.9 million customers when backup tapes were lost during transit to credit bureaus.[39] Although the third-party courier was in possession of the tapes at the time of loss, CitiFinancial had not encrypted the data. CitiFinancial subsequently announced plans to encrypt the data and adopt electronic transmission procedures.[41]

[31] *See* CNN Money, *supra* note 32.

[32] *See id.*

[33] *See id.*

[34] *See* Stephanie Armour, *supra* note 22.

[35] *See id.*

[36] *See* Joris Evers, *Banks to blacklist rogue workers in fraud fight*, CNETNews.com, Oct. 26, 2005. Retrieved on Sept. 28, 2006 from http://news.com.com/Banks+to+blacklist+rogue+workers+in+fraud+ fight/2100-1029 3-5915678.html. The effort includes a consortium of 100 of the largest U.S. financial institutions.

[37] *See id.*

[38] *See Privacy Rights Clearinghouse Report, supra* note 10.

39 See Paul Shread, *CitiFinancial Drops Backup Tapes After Data Loss*, Internet News.com, June 6, 2005. Retrieved on Sept. 28,2006 from http://www.intemetnews.com/storage/article.php/3510481.

40 See id.

[41] *See id.*

Employees and executives often have custody of company laptops, either to complete work at home or on business trips. Thieves can easily gain access to customer or employee data just by walking off with one of the portable computers. Companies should evaluate the necessity of allowing employees to travel with sensitive data and, at a minimum, install encryption software and other security measures to protect the data.

Some inadequate business procedures are completely unrelated to electronic storage. In one case, a computer glitch resulted in 1099s being sent to the wrong addressee.[42] The recipients opened the mail only to find the name, address, and social security number of another individual.[43] In 2005, a university accidentally distributed e-mails containing names, social security numbers, and other personal information for students other than the e-mail recipient.[44] In January 2006, the Boston Globe used old, discarded scrap paper to pack newspapers in mailing boxes.[45] The scrap paper happened to contain credit card numbers, checking account routing numbers, and debit card numbers for various customers.[46]

The FTC filed a complaint against Eli Lilly, a pharmaceutical company, for failing to properly train employees about maintaining the privacy of sensitive customer information.[47] An Eli Lilly employee sent an e-mail to a group of customers that used the drug Prozac.[48] The e-mail address line did not conceal the identities of individual customers.[49] Each recipient could discern the identities of all other Eli Lilly customers who were using Prozac.[50] Eli Lilly was the first case in which the FTC attacked a security breach as an unfair and deceptive practice.[51] The following section closely examines the provisions of FTC settlement agreements with companies that failed to implement adequate security measures.

II. UNFAIR AND DECEPTIVE TRADE PRACTICES

Section 5 of the Federal Trade Commission Act (FTC Act) prohibits unfair or deceptive acts against consumers.[52] The FTC Act, as originally passed in 1914,

[42] *See Privacy Rights Clearinghouse Report*, *supra* note 10 (California State Employment Development Division erroneously sends tax forms to wrong addressee).

[43] *See id.*

[44] *See id.* (Colorado Tech. University sent emails to wrong students).

[45] *See id.*

[46] *See id.*

[47] *See* Decision and Order, *In the matter* of Eli Lilly and Company, Docket No. C-4047, (Federal Trade Commission, May 8, 2002). Retrieved Sept. 28, 2006 from http://www.ftc.gov/os/2002/05/elililly do.htm. *Also see* Complaint, *In the matter* of Eli Lilly and Company, Docket No. C-4047 (Federal Trade Commission, May 8, 2002). Retrieved Sept. 28, 2006 from http://www.ftc.gov/os/2002/05/ elililly cmp.htm.

[48] *See* Eli Lilly Complaint, *supra* note 49 at 1]6.

[49] *See id.*

[50] *See* Eli Lilly Complaint, *supra* note 49 at *Jl.*

[51] *See FTC Statement*, *supra* note 28, at 4.

[52] *See* 15 U.S.C. § 45(a)(1). This statute defines unfair acts as those that "cause[] or [are] likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition." *See* 15 U.S.C. § 45(n). The

prohibited only unfair trade practices. In 1938, the Act was amended to include both unfair and deceptive trade practices.[53] The Federal Trade Commission is given the sole authority to litigate unfair and deceptive acts at the federal level and, because the FTC Act does not define "unfair" and "deceptive," the FTC has the ability to exercise judgment on this issue, subject only to judicial review.[54]

Since 1999, the FTC has settled at least nine cases pursuant to section 5, alleging that the companies' lack of, or inadequacy of, data-security measures compromised the privacy of customer data and constituted a deceptive trade practice.[55] The settlements generally require companies to adopt new security measures, hire licensed individuals to evaluate the effectiveness of the security measures, and submit to annual FTC audits regarding the effectiveness and appropriateness of the implemented security.[56] In a few cases, hefty penalties were also assessed.[57] Aside from the cost of regulatory sanctions, companies may lose customers and experience decreases in profits.[58] The following discussion highlights three of the companies that reached settlement with the FTC and briefly explains what conduct led to the data breach.

A. *Background: Facts of Settled Cases*

1. CardSystems Solutions

CardSystems Solutions acts as an intermediary between merchants and creditors, such as credit card companies, banks, or other financial institutions.[59] At the time of a credit sale, merchants swipe the credit card and the information stored on the magnetic stripe is sent via CardSystems to the credit card company or

Commission defines deception as "a material representation or omission that is likely to mislead consumers acting reasonably under the circumstances." *See FTC Statement, supra* note 28, at 3 (citing Letter from FTC to Hon. John D. Dingell, Chairman, Subcommittee on Oversight and Investigations (Oct. 14,1983), *reprinted in* appendix to *Cliffdale Associates, Inc.*, 103 F.T.C. 110,174 (1984)).

53*See* Sovem, *supra* note 3, at 440.

54 See id.

55 The Federal Trade Commission has defined security breaches primarily as acts of deception, rather than as unfair practices. *See FTC Statement, supra* note 28, at 3.

[56] *See generally* Eli Lilly Decision and Order, *supra* note 49.

57. For example, ChoicePoint was required to pay a total of $15 million pursuant to the settlement agreement with the FTC. *See* Federal Trade Commission, Press Release, ChoicePoint Settles Data Security Breach Charges; to Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress, Jan. 26,

2006. Retrieved on Sept 28,2006 from http://www.ftc.gov/opa/2006/01/ choicepoint.htm.

58. After CardSystems data breach, the company lost American Express as a customer. *See CardSystems Solutions Losing Big Customers*, July 20, 2005. Retrieved Sept. 29, 2006 from http://www. consumeraifairs.com/news04/2005/ cardsystems_customers.html; *see also CardSystems Sells Out After Massive Data Breach*, Oct. 19, 2005. Retrieved Sept. 29, 2006 from http://www.consumeraffairs.com/ news04/2005/cardsystems_sold.html (noting that CardSystems eventually sold out to Pay By Touch).

59. See Complaint, *In the matter* o/CardSystems Solutions, Inc., Docket No. C-4168, at K3. Retrieved Sept. 28, 2006 from http:// www.ftc.gov/os/caselist/0523148/0523148CardSystemscomplaint.pdf. *See also*

CardSystems Solutions, Inc., Final Decision and Order, as issued on Sept 5, 2006. Retrieved Sept. 28, 2006 from http://www.ftc.gov/os/caselist/0523148/ 0523148CardSystemsdo.pdf.

financial institution.[60] CardSystems then sends the financial institutions approval or disapproval of the transaction back to the merchant.[61] CardSystems retained the customer information, such as account number, expiration date, and customer name in its database, but failed to implement sufficient measures to prevent outsiders from accessing the information.[62] Hackers obtained the private information and subsequently used the credit accounts to enter into fraudulent transactions.[63] Over 40 *million* customer records were compromised as a result of this data breach.[64]

2. BJ's Wholesale Club, Inc.

BJ's Wholesale, a membership store, serves approximately 8 million customers in 17 states.[65] BJ's accepts credit cards and, as a result of swiping a customer's card, would store the information from the magnetic stripe on the company database.[66] BJ's did not encrypt the data, retained customer data longer than necessary, and failed to use available technology to secure the electronic database.[67] Thieves used the accessed data to make fraudulent purchases.[68] Credit card companies and banks subsequently had to issue new cards and filed lawsuits against BJ's, seeking approximately $13 million in damages.[69]

3. ChoicePoint, Inc.

As previously described in the introduction to this article, ChoicePoint is a data broker that erroneously sold consumer information, such as social security numbers, account numbers, and addresses, to criminals posing as a legitimate business.[70] In the complaint filed against ChoicePoint, the FTC made two charges of unfair and deceptive trade practices. The first claim was based on ChoicePoint's failure to establish reasonable measures for verifying the authenticity of subscribers and whether the subscriber had a right to the requested consumer information.[71]

60 *See* CardSystems Solutions, Inc. Complaint, *supra* note 61, at 14.

61 *See id.*

62 *See id.* at 16.

63 *See id.* at 18.

64 *See Privacy Rights Clearinghouse Report*, *supra* note 10.

65 *See* BJ's Wholesale Club, Inc. Complaint, 1)3. Retrieved Sept. 28, 2006 from http:// www.ftc.gov/os/caselist/0423160/092305comp0423160.pdf. *See also* BJ's Wholesale Club, Inc. Decision and Order, as issued on Sept. 20, 2005. Retrieved Sept. 28, 2006 from http://www.ftc.gov/os/caselist/ 0423160/ 092305do0423160.pdf.

66 *See* BJ's Wholesale Club, Inc. Complaint, *supra* note 67 at 15.

67 *See* BJ's Wholesale Club, Inc. Complaint, *supra* note 67 at f7.

68 *See id.* at 18.

69 *See* Analysis of Proposed Consent Order to Aid Public Comment, In the Matter of BJ's Wholesale Club, Inc., FTC File No. 042 310. Retrieved Sept. 28, 2006 from http://www.ftc.gov/os/caselist/0523148/ 0523148analysis.pdf.

70 *See* ChoicePoint Complaint, *supra* note 11 at 19 and 12.

71 *See id.* at Count III:

> As described in Paragraphs 12 through 14, ChoicePoint has not employed reasonable and appropriate measures to secure the personal information it collects

ChoicePoint did require subscribers to verify their identity by providing documentation of the business address, tax identification number, subscriber's full name, and phone number.[72] Subscribers could verify this information by providing business documents with the company name and address.[73] The FTC complaint alleged the verification measures used by ChoicePoint's were inadequate, because subscribers were approved based on unreliable and inconsistent proof.[74] Some of the fraudulent subscribers submitted documents with residential, instead of business, addresses; tax forms indicating that the certificate of incorporation was no longer active; multiple documents with contradictory addresses and federal tax identification numbers; and some even responded by faxing the information from an unrelated, commercial fax number.[75] Any of these facts, individually, should have created suspicion about the authenticity of the subscribers, but ultimately the information was sold to these fraudulent subscribers anyway.

The second charge of unfair and deceptive trade practices focused on ChoicePoint's failure to uphold various data security promises. The representations concerning privacy of information were published on the company website, in contracts entered into with subscribers, and in the company's Annual Reports.[76] Specifically, ChoicePoint's Agreement For Service contained the following language:

> ChoicePoint uses administrative, technical, personnel, and physical safeguards to protect the confidentiality and security of personally identifiable consumer information in our possession. These safeguards are designed to ensure a level of security appropriate to the nature of the data being processed and the risks of confidentiality violations involved.[77]

> for sale to its subscribers, including reasonable policies and procedures to (1) verify or authenticate the identities and qualifications of prospective subscribers; or (2) monitor or otherwise identify unauthorized subscriber activity.

[72] *See* BJ's Wholesale Club, Inc. Complaint, *supra* note 67 at 111

[73] *See id.* at 1(13.

[74] *See id.*

[75] *See id.*

[76] *See generally id.*

77 See ChoicePoint Complaint, *supra* note 11, at **p.** 10 and Exhibit A, 18. (The information comes from ChoicePoint s Agreement For Service - Agents/Others.) The FTC complaint also claims that ChoicePoint made additional promises concerning privacy of information in the following statements from ChoicePoint's website:

> Because ChoicePoint's ChoiceTrust understands its responsibility to treat consumers fairly and to protect their privacy, we have developed Fair Information Practices. These practices are derived from the Federal Fair Credit Reporting Act, but go beyond the requirements of that law. . . . ChoicePoint operated under its own Fair Information Practices even before passage of this Act, and continues to offer greater protection to the consumer than is required by the FCRA.

Upon request, ChoicePoint distributed fact sheets to consumers. The following statement, contained in the fact sheet, explained to whom ChoicePoint would sell information and described ChoicePoint's authenticity verification process:

> Every ChoicePoint customer must successfully complete a rigorous credentialing process. ChoicePoint does not distribute information to the general public and monitors the use of its public record information to ensure appropriate use.[78]

A majority of the complaints filed by the FTC focused on companies that failed to uphold privacy representations. However, a published privacy statement is not necessarily a prerequisite to legal liability. ChoicePoint provides an example of a case in which one of the charges for unfair and deceptive trade practice dealt solely with the company's failure to implement adequate measures for reviewing the credibility of subscribers. In the alternative, an actual security breach is also not a prerequisite for FTC action.[79] The FTC filed a complaint against Microsoft, even though the company had not yet experienced a data breach. "Because appropriate information security practices are necessary to protect consumers' privacy, companies cannot simply wait for a breach to occur before they take action."[80] Compiling an all-encompassing and complete list of "best practices" for data security is a daunting task. However, examination of the FTC complaints provides some rudimentary examples of the actions, or inactions, contributing to electronic data breaches.

B. *Data Security: Information Security Flaws That Resulted in Charges of Unfair and Deceptive Trade Practices*

The following list provides guidance to businesses in their search for potential security weaknesses. It should be recognized as a starting point for businesses and not an exhaustive or exclusive list of practices.

/, *Encryption of all data.* The FTC investigates whether data are encrypted at the business location and whether they are encrypted while being transmitted to another site or business.[81]

2. *Use of secure passwords.* A company should avoid using default passwords or log-ins.[82] Default security codes provide anonymity to the user, whereas individually assigned passwords and log-ins allow for identification of the user. Individual passwords also provide more protection against a hacker.

3. *Prevention or limitation of "wireless access point" access to system networks*,[83] In several cases, such as *BJ's Wholesale* and *CardSystems*, the FTC pointed out that

[78] *See* ChoicePoint Complaint, *supra* note 11, at 10 and Exhibit C.

[79] *See FTC Statement*, *supra* note 28, at 6.

[80] *See id.* at 6.

[81] *See id.* at 2.

[82] *See* BJ's Wholesale Club, Inc. Complaint, *supra* note 67, at 2.

[83] *See id.*

technology exists to prevent or limit access via a "wireless access point on the network."[84] Failure to implement such technology can be deemed an unfair or deceptive trade practice.

4. *Implementation of all "readily-available measures " to detect and prevent security breach.* If technology exists to prevent or detect security breaches, and the entity can easily access or purchase the technology, failure to implement the measures might constitute an unfair or deceptive trade practice.[85]

5. *Implementation of periodic security reviews.**[6] Adequate review procedures include auditing the effectiveness of the implemented procedures, the ability to detect security breaches, and periodic consideration of weaknesses that require new security measures.[87]

6. *Establishment of an information retention policy.* An entity should retain private customer information only if there is a business need. Subsequent storage in an electronic format, coupled with ineffective security measures, increases the likelihood of a data breach.[88]

7. *Retaining sensitive data when the information is no longer needed.* A company should not retain data longer than is necessary to complete the transaction. The FTC examines whether the data are retained in an insecure format for an unreasonable or unnecessary length of time.[89]

C. *Enforcement Provisions of FTC Settlements: Guidance on Best Practice to Avoid Charge of Unfair or Deceptive Trade Practice*

In each settlement agreement, the FTC generally required that the defendant company implement an information security program and detailed what actions or weaknesses must be addressed by the security program. Virtually the same language is used in all settlements, detailing two phases to the information security programs. The first phase concerns the design/development and implementation of an effective security program. The second phase is an assessment period, wherein an independent third party is retained to review the adequacy of the program.

1. Design/Development and Implementation

Generally, the FTC requires the company to design and implement appropriate safeguards for administrative, technical, and physical characteristics in a manner appropriate for the size and complexity of the business.[90] The design should address the nature and scope of all business activities and the sensitivity of the

[84] *See id.*

[85] *See id.*

[86] *See* BJ's Wholesale Club, Inc. Complaint, *supra* note 67, at 2.

[87] *See* CardSystems Solutions, Inc. Complaint, *supra* note 60, at f6. (The FTC complaint specifically mentions the vulnerability to attack by "Structured Query Language" injection attacks.)

[88] *See* CardSystems Solutions, Inc. Complaint, *supra* note 60, at %

[89] *See id.*, 1(6.

90 See generally BJ s Wholesale Club, Inc. Agreement Containing Consent Order, *supra* note 71.

personal information collected and should establish accountability, by designating an employee responsible for coordination.[91] Further, the FTC generally requires that the company identify both internal and external risks material to the security, confidentiality, and integrity of personal information that could potentially result in unauthorized use or misuse of the information.[92] The overall risk assessment should, at a minimum, include consideration of risks in each area of relevant operations, including:

(1) employee training and management;
(2) information systems, including network and software design, information processing, storage, transmission, and disposal; and
(3) prevention, detection, and response to attacks, intrusions, or other system failures.[93]

Finally, the system must be regularly tested and monitored, and as a result of such testing and monitoring, implement any necessary adjustment of system safeguards.[94]

2. Assessment

On a biennial basis, the entities are required to hire an independent individual to assess the extent to which the program complies with the details of the design and implementation phase.[95] The FTC will accept a report from a Certified Information System Security Professional, a Certified Information Systems Auditor, or an individual certified by the SysAdmin, Audit, Network, Security Institute with the Global Information Assurance Certification.[96] An entity can certainly protect itself upfront by hiring a certified professional to assist in the design, implementation, and eventual audit of a data security program. A proactive approach certainly aids in future litigation with the FTC and provides evidence of "reasonable" practices if the company is defending a negligence suit.

[91] BJ's Wholesale Club, Inc. Agreement Containing Consent Order, *supra* note 71.

[92] *See generally id.*

[93] *See id.* at 3-4.

[94] "Hackers and thieves will adapt to whatever measures are in place, and new technologies likely will have new vulnerabilities waiting to be discovered. As a result, companies need to assess the risks they face on an ongoing basis and make adjustment to reduce these risks." *FTC Statement*, *supra* note 28, at 7.

[95] *See* BJ's Wholesale Club, Inc., Agreement Containing consent Order, *supra* note 71, at 3-4. The assessment report compiled by the certified profession must contain information that:

> A. sets forth the specific administrative, technical, and physical safeguards that respondent has implemented and maintained during the reporting period;
> B. explains how such safeguards are appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the personal information collected from or about consumers;
> C. explains how the safeguards that have been implemented meet or exceed the protections required by [the design and implementation phase] of the order; and
> D. certifies that respondent's security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of personal information is protected and, for biennial reports, has so operated throughout the reporting period.

[96] *See id.*

D. *State Law Unfair, Deceptive, or False Advertising Claims*

The FTC has brought claims only against the high profile cases that resulted in exposure of numerous private records. Most states, however, also have laws prohibiting unfair, deceptive, and false advertising acts. States may be more willing to pursue smaller instances of data breach. For example, in 2002, Ziff Davis, a multimedia company, entered into a settlement with New York, California, and Vermont for a security breach that exposed credit card account numbers on only 50 customers.[97] The settlement read much like the FTC settlements, requiring implementation and periodic audit of security measures.[98] In addition, Ziff Davis was required to pay $500 to each of the 50 affected customers, plus $100,000 to the three states.[99]

Unlike the federal law for unfair and deceptive practices, individuals can bring a private cause of action under most state laws that prohibit unfair, deceptive, or false advertising claims.[100] Many times the state law allows for treble damages. In fact, the Ziff Davis settlement specifically stated that private actions were not precluded by the settlement.[101]

III. STATE LAW NEGLIGENCE CLAIMS: WHEN DOES A BUSINESS OWE A DUTY OF CARE TO IDENTITY THEFT VICTIMS?

Prior to 1998, the law awarded "victim" status only to the business entities, because often the private person was not required to pay the debt created by the identity thief.[10"] Historically, the law viewed the business as the victim of identity theft, because, depending on the type of theft, the institution suffered the economic loss.[103] For example, federal law limits consumer liability for lost and stolen ATM or debit cards, as long as the consumer reports the theft within 60 days.[104] In most cases, the thief cannot be located, so the financial institution suffers the loss.

In reality, the aftermath of identity theft is often financially and emotionally overwhelming, if not devastating, to the innocent individual. By the time the identity theft is discovered, the victim can be faced with a ruined credit history, bankruptcies that were filed by the thief, and even a criminal record or arrests. The average victim of identity theft will spend approximately 600 hours and $740 attempting to repair

97. See In re Ziff Davis Media Inc. Retrieved Sept. 2, 2006 from http://www.oag.state.ny.us/press/2002/ aug/ aug28a_02_attach.pdf.
98. See id. at UH 24 and 25.

[99] *See id.* at TJ28.

[100] *See* KIMBERLY KIEFER *et al.*, Information Security: A Legal, Business, and Technical Handbook 41 (2004).

[101] *See In re* Ziff Davis Media Inc, *supra* note 99, at ^[29.

102. See Stephen L. Wood & Bradley I. Schector, *Identity Theft: Developments in Third Party Liability*, 8 Am. B. Assoc., Sec LrriG. Consumer & Pers. Rts. Newsl., No. 3, at 3-4 (Summer 2002).
[103] *See id.*

[104] Electronic Fund Transfer Act, 15 U.S.C. § 1693 *et seq.*

his or her reputation.[105] Aside from the financial loss, studies reveal that the emotional trauma is comparable to that experienced by victims of violent crime.[106]

The Identity Theft and Assumption Deterrence Act (ITADA)[107] was passed in 1998 to impose stricter penalties on those committing identity theft. The ITADA properly addresses the "victim" issue, by providing true identity theft victims with the ability to seek restitution from a convicted identity thief, but fails to accurately identity all responsible parties in its definition. In situations where they are entrusted with valuable data, and they are in the best position to detect and prevent misappropriation of private information, an entity like ChoicePoint should bear as much responsibility for a victim's loss as the true identity thief. The courts have long held that "where one of two innocent persons must suffer by reason of the fraud of a third person, the party whose act, omission, or negligence enables the third person to consummate the fraud should bear the loss."[108] At least one court, however, has affirmatively ruled that the ITADA does not establish a cause of action against a third party like ChoicePoint.[109]

The unfortunate reality is that the ITADA has done little to decrease the occurrence of identity theft or to combat the devastating economic and emotional losses suffered by victims. Even if a thief is located, he or she is likely to be judgment-proof and incapable of compensating the victim.[110] So, although consumers are now treated as victims in relation to the true identity thief, they are still left without recourse under federal law, because they have no cause of action against the entity that failed to adequately secure their personal information. Consumers have sought recourse by filing state law negligence claims against the business.

There are essentially two groups of plaintiffs that might seek recovery of damages from the business. The first group comprises customers and employees, each of which has a current relationship with the defendant business at the moment the identifying information is stolen. The second category of plaintiffs consists of individuals who were neither customers nor employees when the business misused or in someway contributed to the misuse of identity. These types of cases are still quite new, but the emerging case law seems to indicate that only the customer and employee plaintiffs will be able win negligence suits. The courts seem very reluctant to hold the same businesses liable for damages suffered by non-customers.

The distinguishing factor between these two categories of plaintiffs is whether or not there was a duty of care. It is much easier for customer or employee plaintiffs to prove a duty of care existed, because there was a legal relationship at the time the identifying information was stolen from the business. The trend in non

[105] *See FTC Identity Theft Report*, *supra* note 1, at 3. ("While 62% of victims did not incur any out-of- pocket expenses, 38% did, representing 13-14 million Americans. Since January 2001, these 38% have paid approximately $3.8 billion, or an average of $1.5 billion per year.")

[106] *See id.*

[107] 18U.S.C. §1028.

[108] *See* Brownlow v. Aman, 740 F.2d 1476,1489 (10th Cir. 1984).

[109] *See* Ganay v. US Bancorp, 303 F. Supp. 2d 299 (E.D.N.Y. 2004).

[110] *See* McMahon, *supra* note 1, at 632.

customer cases is for the court to hold that the business owes no duty of care to a non-customer and, thus, the plaintiff cannot prove all essential elements of the negligence action. The following cases illustrate the legal analysis courts have used in cases involving the two types of plaintiffs.

A. *Customer and Employee Plaintiffs*

On March 1, 2005, Michigan became the first state with direct regulation requiring every employer to maintain a policy for safeguarding employee social security numbers.[111] Since this legislation passed in Michigan, another half dozen states have followed suit, including Arizona, California, Colorado, Illinois, and Texas. In addition, in 2005, a Michigan Appellate Court became the first to hold an organization liable for failing to adequately safeguard personal information that was ultimately used for identity theft.[112]

In the *Bell* case, employees sued their local union for negligently handling personal information that ultimately resulted in identity theft. The trial jury found that the union had been negligent and awarded the plaintiffs $275,000. On appeal, the appellate court considered whether or not the union actually owed a duty of care to the employee plaintiffs. At trial, it was determined that the identity theft occurred as a result of the union's allowing its treasurer, Yvonne Berry, to take personnel files home with her. While the files were in her home, Ms. Berry's daughter ultimately acquired the personnel information, with which she later committed identity theft. In its decision, the appellate court stated the general rule that "[t]here is no duty to protect against the acts of a third person absent a special relationship between the defendant and the plaintiff or the defendant and the third person."

The court also indicated that to determine whether a "duty-imposing special relationship exists" would involve determining whether the plaintiff entrusted the defendant with the control and protection of the information. The court stated that the following factors must be examined when determining whether a special relationship creating a duty of care exists between plaintiff and defendant:

1) the societal interests involved,
2) the severity of the risk
3) the burden on the defendant,
4) the likelihood of the occurrence of the risk,
5) the relationship between the parties,
6) the foreseeability of harm,
7) defendant's ability to comply with the duty,
8) the victim's inability to protect himself,
9) the cost of providing protection, and
10) whether the victim bestowed any economic benefit on the defendant.[113]

[111] *See* Michigan's Social Security Number Privacy Act, Mich. Comp. Laws Ann. §445.84 (West 2005).

[112] *See* Bell v. Michigan Council 25 AFSCME, 2005 WL 356306 (Mich. Ct. App., February 15,, 2005) (unpublished).

[113] *See* Bell, *supra* note 113.

Examining this list, the court ultimately upheld the jury's determination, holding that a duty of care did exist between the union and the employees.

The court held that a fiduciary relationship existed between a union and its members, as unions are specifically established to protect the individual interests of its members. The court found that you must analyze the foreseeability of the ultimate harm, not the foreseeability of the third party's criminal conduct.[114] Based on the facts of this case, including that management had discussed the risk of identity theft, it was foreseeable that the current practices could lead to identity theft. Finally, the court reiterated that a business is not expected to implement 100% safeguards against theft.[115] However, the defendant in this case was unable to show any established procedures designed to safeguard the personal information. The court limited this holding to the specific facts of this case and this case was unpublished. The latter is a clear indication of the wariness in the legal community to hold a business liable for identity theft committed by a third party, but illustrates a customer or employee plaintiff can prove the defendant business owed a duty of care.

In *Kuhn* v. *Capital One*,[116] the plaintiff, Deborah Kuhn, was a customer who maintained a VISA credit card account with Capital One. A computer hacker infiltrated a merchant's server and compromised the privacy of Ms. Kuhn's personal identifying information. Capital One contacted Ms. Kuhn the same day, closed her account, and sent her information explaining how to avoid fraudulent charges to her account. Even so, Ms. Kuhn's personal information was subsequently used to open 18 fraudulent accounts and accumulate a fraudulent charge balance of $25,000.

Ms. Kuhn brought suit against Capital One in a Massachusetts state court, alleging, in part, negligence.[117] In that case, the plaintiff lost at summary judgment for failing to prove causation of damages. The court never discussed the issue of duty of care and it does not appear that Capital One denied it owed her one. Capital One presented evidence that associated retailers and company websites were not provided with customers' "social security numbers, dates of birth, mother's maiden name or PIN numbers."[118] The court held that causation was lacking, because identity theft cannot be committed with a credit card number only.[119]

The distinctions in these cases have nothing to do with the status of Bell as an employee and Kuhn as a customer. In fact, when comparing *Kuhn* with *Bell*, there are obvious material differences between the two factual scenarios. In *Kuhn*, Capital One had established procedures to protect and warn its customers and was actually diligent in implementing those procedures. In *Bell*, in contrast, the union had no such procedures, and, in fact, declined to implement any, even after admitting that identity theft could result. Unfortunately, not all cases will be as clearly

[114] *See id.*

[115] *See* Bell, *supra*, note 113.

[116] *See* Kuhn v. Capital One, 18 Mass. L. Rep. 524, 2004 Mass. Super. LEXIS 514 (2004).

[117] *See id.* Kuhn also claimed breach of contract, breach of implied covenant of good faith and fair dealing, misrepresentation, invasion of privacy, breach of fiduciary duty, and unfair/deceptive acts. The court also granted summary judgment on these causes of action in favor of Capital One.

[118] *See* Bell, *supra* note 113.

119 See id.

distinguishable. The difficult cases are those that fall in between. Recognizing that the judicial system is often slow to enter a finding of negligence, the authors believe that businesses can protect themselves by following the Federal Trade Commission guidelines discussed earlier in the article, by performing background checks on employees, and by implementing an internal auditing system to detect irregular conduct by employees.

B. *Non-customer cases*

Non-customer cases in this area have been dubbed "negligent enablement of imposter fraud." To date, there is no state that has passed a statute creating this tort and, therefore, most courts are refusing to recognize its existence. Victims want a new tort to provide relief for innocent consumers who do not contribute to their losses. Businesses often solicit new credit accounts or are eager to open a new account without verifying the identity of the individual applicant. The business is in a much better position to detect fraud and prevent it. Therefore, it is possible that these cases could be a new form of liability in the near future.

Those courts refusing to recognize the tort do so by claiming there is no duty of care owed by a business to an individual who is not currently a customer.[120] If there is no duty, there can be no negligence. Many courts hold true and fast to this reasoning, even when the business takes absolutely no steps to verify the validity of its applicant's identity.[121] In fact, negligence claims have been rejected consistently when brought by non-customers, because without a pre-existing relationship, no duty of care is owed by the business toward the non-customer.

The prevailing view is that legislators, not judges should address consumer protection matters.[122] In Huggins v. Citibank, N.A.,[12J] the South Carolina Supreme Court reiterated this prevailing view, asserting "the legislative arena is better equipped to access and address the impact of . . . fraud on victims and financial institutions alike."[124]

There is, however, at least one case in which the non-customer won by proving the business was negligent when handling the victim's identity. In 1996, the Alabama Supreme Court allowed an identity theft victim to recover from the bank that negligently enabled an imposter to use the victim's identity, resulting in criminal liability for the victim.[123] In this case, Union State Bank's employee allowed the imposter to open a checking account by presenting a $100 deposit. The bank relied on a temporary, photo-less driver's license, which had actually been stolen from Bridgette Patrick. Despite the facts that the imposter's signature did not match that on the license and no permanent address or Social Security number was provided, the bank still opened the account using Ms. Patrick's information. The imposter then

[120] Huggins v. Citibank, N.A., 585 S.E.2d 275,281 (S.C. 2003).
[121] Polzer v. TRW, Inc., 256 A.D.2d 248,252 (N.Y. App. Div. 1998)
[122] *Huggins*, 585 S.E.2d at 334.
[123] *Id.*
[124] *Id.*
[125] *See Patrick, supra* note 5.

proceeded to write numerous bad checks on the account, resulting in warrants being issued for Ms. Patrick's arrest. Ms. Patrick was indeed arrested in eleven different jurisdictions and subjected to the humiliating process of arrest, booking photos, fingerprinting, and jail detainment for a total of 10 days.[126]

Ms. Patrick filed suit alleging that Union State Bank had negligently allowed the imposter to open the account without proper identification or verification. Union State Bank was granted its motion for summary judgment at the trial court level indicating that Ms. Patrick had failed to establish the requisite element of a duty owed by the bank to Ms. Patrick, or that there was sufficient proximate cause linking the alleged negligence to injuries sustained by Ms. Patrick. The Alabama Supreme Court reversed the lower court finding that the defendant bank did owe a duty of care to Ms. Patrick, because the bank owed a fiduciary relationship to customers and the public at large.[127] In its ruling, the Court recognized that liability is not generally imposed upon one party based on the criminal actions of another, but that this principle was not applicable, because it was derived in cases related to physical assaults, not negligence. The Court further distinguished that in the present case, Union State Bank became involved with Ms. Patrick by opening an account in her name. The actual opening of the account created Ms. Patrick's problem, not any unrelated criminal activity. Additionally, the bank should have foreseen that failure to follow proper bank procedures could place citizens at risk of being victimized by fraudulent individuals and that the bank was in the best position to prevent the fraud.[128] Other jurisdictions have not been nearly as willing to find that institutions owe a non-customer any duty of care.

CONCLUSION

In the wake of the increasing data breach cases and possibility for identity theft, this article seeks clarity. Most business entities collect some form of sensitive information on either customers or employees. Failure to adequately protect the privacy of such information exposes entities to legal liability. The Federal Trade Commission settlements provide some guidance on properly securing private records. Whether the business faces civil sanctions from a regulatory agency or liability from a negligence lawsuit, "reasonable" business practices can provide immunity from liability. The Federal Trade Commission does not require perfect security measures and state law negligence claims require only "reasonable" behavior. While it is true that individuals may still find it difficult to bring a successful negligence suit against a company that suffered a data breach, a customer or employee plaintiff is much more likely to be successful.

[126] *Patrick*, *supra* note 5, at 1365-1367.

[127] *See id.* at 1368-1369.

[128] *See id.* at 1369.