Seventh Circuit Review

Volume 3 | Issue 2 Article 8

5-1-2008

Lost in Cyberspace: A Call for New Legislation to Fill the Black Hole in Information Privacy Law Following *Pisciotta v. Old National Bancorp*

Elena N. Vranas-Liveris
IIT Chicago-Kent College of Law

SEVENTH CIRCUIT REVIEW Volume 3, Issue 2 Spring 2008

LOST IN CYBERSPACE: A CALL FOR NEW LEGISLATION TO FILL THE BLACK HOLE IN INFORMATION PRIVACY LAW FOLLOWING *PISCIOTTA V. OLD NATIONAL BANCORP*

ELENA N. VRANAS-LIVERIS*

Cite as: Elena N. Vranas-Liveris, *Lost in Cyberspace: A Call for New Legislation to Fill the Black Hole in Information Privacy Law Following* Pisciotta v. Old National Bancorp, 3 SEVENTH CIRCUIT REV. 658 (2008), *at* http://www.kentlaw.edu/7cr/v3-2/vranas-liveris.pdf.

INTRODUCTION

We live in the Information Age,[1] an age in which we rely on computers and the Internet every day and in almost every aspect of our lives, from personal communications to business transactions to entertainment. Along with this constant use of computers and the Internet, however, comes a risk. In order to take advantage of the convenience which computers provide through online shopping and banking, for example, we must often provide our most personal information. Unfortunately, this personal information is not always

* J.D. candidate, May 2008, Chicago-Kent College of Law, Illinois Institute of Technology; B.A., Political Science, 2004, Northwestern University. I would like to thank my family for their continuous love and support. Thank you also to my peers in the SEVENTH CIRCUIT REVIEW Honors Seminar for their invaluable help in writing this note.

[1] Glossary, Readiness for the Networked World, *available at* http://cyber.law.harvard.edu/readinessguide/glossary.html (defining Information Age as "the current stage in societal development which began to emerge at the end of the twentieth century" and is "marked by the increased production, transmission, consumption of and reliance on information.").

completely secured by the database owners who store it. In exchange for the convenience of online dealings, therefore, we put ourselves at risk that our personal information will be wrongfully accessed. Since 2005, there have been hundreds of publicized database security breaches, which have affected the personal data of more than two hundred million people.[2]

With little legal precedent regarding liability surrounding database security breaches, there is great uncertainty as to who should bear the costs—consumers or database owners—associated with providing personal information for online transactions. Should consumers bear the costs in return for the conveniences of online transactions, or should database owners bear the costs in return for the opportunity to develop their business over the Internet?

Consumers throughout the country who have been affected by database security breaches have begun to bring civil lawsuits against database owners to place liability on them for these breaches. The Seventh Circuit first dealt with such a situation in *Pisciotta v. Old National Bancorp*.[3] The consumers in this case brought their action against the database owner under claims of negligence and breach of contract.[4] The issue that the Seventh Circuit dealt with in examining these claims was whether the plaintiffs had suffered the requisite harm, considering their personal information was wrongfully accessed but no identity theft or other fraud resulted from the security breach.[5] The Seventh Circuit was rather definitive in its ruling that the plaintiffs had not suffered the requisite harm to place liability on the database owner. *Pisciotta*, therefore, raises significant concerns for consumers. It also suggests important implications for the future of database security breach cases, which embody a new intersection of privacy law and tort law.

[2] *See* Privacy Rights Clearinghouse, *A Chronology of Data Breaches*, *available at* http://www.privacyrights.org/ar/ChronDataBreaches.htm.

[3] Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629 (7th Cir. 2007).

[4] *Id*. at 632.

[5] *Id*. at 635.

This Note examines *Pisciotta* and its effect on the state of the law regarding liability resulting from database security breaches. Part I of this Note reviews the background necessary to discuss *Pisciotta*, which includes a basic understanding of the Internet, privacy law, and current regulations addressing database security breaches. Part II then examines *Pisciotta*, detailing the facts of the case and analyzing the Seventh Circuit's holding. Part III explores whether *Pisciotta* could have come out differently, particularly had the court analogized the exposure of the plaintiffs' personal information to toxic exposure in toxic tort cases. Part III also discusses the role of the economic loss doctrine in database security breach cases and whether it should have played a part in *Pisciotta*. Lastly, Part IV assesses what should be done to protect consumers' privacy interests in light of the difficulties consumers face under current common law, as illustrated in *Pisciotta*. Specifically, this Note proposes that legislation be enacted to provide for the recovery of credit monitoring costs by affected consumers of a database security breach.

I. BACKGROUND

Pisciotta is particularly interesting because it illustrates a new intersection between privacy law and tort law in the context of technology. Considering this unique intersection of the law, one must have an understanding of certain technology, such as the Internet, as well as knowledge of privacy law and tort law, which are implicated because of this technology. This section provides this necessary background and also sheds light on federal and state regulations which address database security breaches. Through this background, one recognizes the lack of redress for victims of database security breaches whose personal information has been wrongfully accessed, but who have not yet suffered identity theft or other fraud.

A. What is the Internet?

As described by some of its developers, "[t]he Internet has revolutionized the computer and communications world like nothing

before. . . The Internet is at once a world-wide broadcasting capability, a mechanism for information dissemination, and a medium for collaboration and interaction between individuals and their computers without regard for geographic location."[6]

The Internet was created in 1969 following years of research by the Advanced Research Projects Agency of the Department of Defense.[7] It essentially is a worldwide series of networks which can transmit data between each other using a special language called the Internet Protocol.[8] One of the Internet's most distinctive characteristics is that it is a "packet switching" network.[9] This means that the Internet can break down information into packets, or formatted pieces of data, so that it can transmit the information as quickly and efficiently as capacity allows.[10] Packets are labeled with the address of their final destination and may then travel through different routes until they reach their destination computer where they are reassembled.[11] This differs from more traditional communication media, where information travels as a whole and may tie up an entire channel while it is transmitted.[12] The Internet is also controlled through "smart communications" such that there is no centralized control of the Internet.[13] Rather, all of the computers in the worldwide network assess the traffic of packets and control the flow of the information.[14] There is thus no central authority which governs who may use the Internet and for what purposes; it is an autonomous network.[15] Lastly,

[6] Barry M. Leiner, et. al., *A Brief History of the Internet*, Internet Society (2003), *available at* http://www.isoc.org/internet/history/brief.shtml.

[7] *Id*.

[8] Dan L. Burk, *Federalism in Cyberspace*, 28 CONN. L. REV. 1095, 1097-1100 (1996).

[9] *Id*. at 1097.

[10] *Id*.

[11] *Id*.

[12] *Id*.

[13] *Id*. at 1098.

[14] *Id*.

[15] *Id*.

the Internet provides for "telepresence," meaning that the Internet is unconstrained by geography.[16] A user may "access computers, retrieve information, or control various types of apparatus from around the world," while his or her physical location is unidentifiable.[17] This universe of international information that Internet users have access to is referred to as "cyberspace."[18]

The Internet was originally intended for use only by academics and government officials; however, the Internet became much more accessible with the development of personal home computers and "browser" software.[19] Today the Internet is widely used by businesses and consumers and its use continues to grow exponentially. Electronic commerce or "e-commerce," which includes the sale and purchase of products and services,[20] has become a multi-billion dollar industry, with approximately 259 billion dollars of online sales having been expected in 2007.[21]

Although the Internet provides consumers with many benefits, it also creates great concern for consumers who are required to provide personal information over the Internet for e-commerce transactions. These consumers face potential misuse of their information in several ways. For instance, consumers are susceptible to: the reuse of their information for purposes other than those for which they provided it; the replication of their information to third parties; the use of their information to commit fraud; the intrusive use of their information such as through telemarketing; and the interception or misappropriation of their information by third-party hacking, which

[16] *Id*.

[17] *Id*.

[18] *Id*. at 1099.

[19] Christopher F. Carlton, *The Right to Privacy in Internet Commerce: A Call for New Federal Guidelines and the Creation of an Independent Privacy Commission*, 16 ST. JOHN'S J.L. COMM. 393, 401 (2002).

[20] DANIEL J. SOLOVE, MARC ROTENBERG, & PAUL M. SCHWARTZ, PRIVACY, INFORMATION, AND TECHNOLOGY 112 (2006).

[21] *Online Sales Spike 19 Percent*, CNNMoney.com (May 14, 2007), http://money.cnn.com/2007/05/14/news/economy/online_retailing/.

was at issue in *Pisciotta*.[22] These examples of misuse of personal information which is provided over the Internet directly implicate the consumers' right to privacy, which leads us to the next section regarding privacy law.

B. Privacy Law

The concept of a right to privacy was first introduced in American jurisprudence by Samuel D. Warren and Louis D. Brandeis in their seminal article written in 1890, *The Right to Privacy*.[23] They wrote, "[p]olitical, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the demands of society."[24] Particularly, the new right they espoused in this era of change, marked by the Industrial Revolution, was the "right to be let alone."[25] The article was embraced by jurists throughout the country, and courts began deciding cases by looking at different principles of privacy.[26] This led to the creation of common law causes of action to protect an individual's right to privacy through property, tort, and contract law.[27]

The right of privacy came to the forefront of American jurisprudence again in the mid-twentieth century when the United States Supreme Court, through a series of decisions,[28] established a constitutional right of privacy. Although the right of privacy is not

[22] FRED H. CATE, PRIVACY IN PERSPECTIVE 6-7 (2001).

[23] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

[24] *Id*. at 193.

[25] *Id*. Justice Louis Brandeis later wrote of "the right to be let alone" that it is "the most comprehensive of rights and the right most valued by civilized men." Olmstead v. U.S., 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

[26] Carlton, *supra* note 19, at 399.

[27] *Id*.

[28] *See, e.g.*, Roe v. Wade, 410 U.S. 113 (1973); Stanley v. Georgia, 394 U.S. 557 (1969); Terry v. Ohio, 392 U.S. 1 (1968); Katz v. U.S., 389 U.S. 347 (1967); Loving v. Virginia, 388 U.S. 1 (1967); Griswold v. Connecticut, 381 U.S. 479 (1965); Mapp v. Ohio, 367 U.S. 643 (1961).

explicitly provided for in the Constitution, the Supreme Court found that the "roots of this right" were implied in the "'penumbras' and 'emanations' of the protections guaranteed in the Bill of Rights,"[29] and particularly in the First, Fourth, Fifth, Ninth, and Fourteenth Amendments.[30]

With the acceptance of the right of privacy in modern law, many scholars have devoted their research to exploring exactly which privacy interests are protected and to what extent. Professor Jerry Kang has described privacy in terms of being "clustered into three groupings": privacy regarding 1) physical space, 2) decisions, and 3) information.[31] This last grouping, information privacy, is most relevant in our discussion of the legal ramifications surrounding a database security breach. Information privacy "concerns an individual's control over . . . the acquisition, disclosure, and use [] of personal information."[32] Personal information is "information identifiable to the individual," meaning that it entails a connection between the information and the person, not necessarily that it is sensitive or private.[33] Information may be identifiable to an individual when the information 1) is authored by the individual—i.e., phone conversation or e-mail, 2) describes the individual—i.e., birth date or mother's maiden name, or 3) is "instrumentally mapped to the individual for institutional identification"—i.e., Social Security number or credit card number.[34]

[29] MARTIN KUHN, FEDERAL DATAVEILLANCE: IMPLICATIONS FOR CONSTITUTIONAL PRIVACY PROTECTIONS 8 (2007) (quoting *Griswold*, 381 U.S. 479).

[30] *Roe*, 410 U.S. at 152.

[31] Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1202 (1998).

[32] *Id*. at 1203 (adopting this definition from a report by the Information Infrastructure Task Force which was created under the Clinton administration).

[33] *Id*. at 1206-1207.

[34] *Id*. at 1207.

1. Privacy Torts

Following Warren and Brandeis's 1890 article, courts and legislatures recognized the "right to be let alone" through case law and statutory law.[35] In 1960, Dean William Prosser cataloged the more than three hundred privacy tort cases that were decided since the Warren and Brandeis article, and concluded that there were four distinct privacy torts.[36] These "invasion of privacy" torts have since been codified in the Restatement (Second) of Torts[37] as the following: 1) intrusion upon seclusion—when one intrudes "upon the solitude or seclusion of another or his private affairs or concerns" and where this "intrusion would be highly offensive to a reasonable person;"[38] 2) appropriation—when "one appropriates to his own use or benefit the name or likeness of another;"[39] 3) public disclosure of private facts—when one publicly discloses a private matter that is "highly offensive to a reasonable person" and "is not of legitimate concern to the public;"[40] and 4) false light—when one publicly discloses a matter that places a person "in a false light" that is "highly offensive to a reasonable person."[41]

These torts, however, provide little protection of personal information in the private sector.[42] Particularly, they are not useful against database owners who merely store information which is then misappropriated, as was the case in *Pisciotta*. First, intrusion upon seclusion does not provide a remedy in this scenario. In the context of

[35] DANIEL J. SOLOVE & MARC ROTENBERG, INFORMATION PRIVACY LAW 18 (2003).

[36] William Prosser, *Privacy*, 48 CAL. L. REV. 383 (1960).

[37] Restatement (Second) of Torts § 652A (1977).

[38] *Id*. at § 652B.

[39] *Id*. at § 652C.

[40] *Id*. at § 652D.

[41] *Id*. at § 652E.

[42] Jerry Kang, *supra* note 31, at 1231 n.159. See Matthew C. Keck, *Cookies, The Constitution, and the Common Law: A Framework for the Right of Privacy on the Internet*, 13 ALB. L.J. SCI. & TECH. 83 (2002) for an interesting proposal of a new tort to protect information privacy.

personal information, intrusion upon seclusion looks to whether the particular means used to collect the information is highly offensive.[43] This is not helpful in e-commerce situations, where consumers voluntarily provide information to receive goods or services; [44] there is no problem with the means the database owner uses to obtain that information. If any party has intruded upon seclusion in these situations, it is the third-party hacker; however, this is immaterial when a plaintiff seeks redress from the (wealthier) database owner.

Second, a plaintiff can only sue a database owner under appropriation when the database owner itself uses or benefits from the name or likeness of the consumer. This practically would only occur when a database owner disseminates "personal information for commercial purposes without consent."[45] That is not the situation in a database security breach where a third party hacker has misappropriated the information without the knowledge of the database owner. Privacy concerns with the collection or storage of data are therefore largely outside the scope of appropriation.[46]

Third, an action for public disclosure of private facts is unhelpful for a plaintiff under this scenario, because the tort entails that the information is distributed to the general public, not to an individual or small group of people,[47] as is often the case in a database security breach. Furthermore, like intrusion upon seclusion, public disclosure of private facts is not applicable when the plaintiff voluntarily provides information.[48] Again, such an action may work against the third-party hacker if he or she distributes the information publicly, but will not work against the database owner.

---

[43] Joel R. Reidenberg, *Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?* 44 FED. COMM. L.J. 195, 222-23 (1992).

[44] *Id*.

[45] *Id*. at 225.

[46] *Id*.

[47] *Id*. at 224.

[48] *Id*. at 223-24.

Lastly, the false light tort is inapplicable in this context because it pertains only to the dissemination of inaccurate information;[49] a database owner provides accurate information in a database security breach. As with public disclosure of private facts, the false light tort also requires that the information be disclosed to the public,[50] not to a small group of people as occurs in most data breaches. A plaintiff could use this tort against the third-party hacker, for example, if the hacker publicly and fraudulently uses the plaintiff's identity.

Parties who seek to hold database owners liable for wrongful access to their personal information following a database breach thus have limited means to do so under common law. Without an applicable invasion of privacy tort, they must rely on claims of negligence and/or breach of contract, as in *Pisciotta*. Although the requisite duty for a negligence claim may be found through a contractual privacy policy or fiduciary relationship, claims under negligence and/or breach of contract remain very difficult to recover under because of the plaintiffs' burden to prove a compensable injury, as we will see in *Pisciotta*. Recognizing the hurdles that consumers confront under common law to protect their information privacy, we now turn to what protection consumers have under federal and state regulation.

2. Federal Regulation

The United States currently has no comprehensive legislation dealing with the collection of personal information. Consequently, information privacy has been protected through a "patchwork of Constitutional, statutory, common law and private sector guidelines," which has often proven ineffective.[51] Congress has passed some industry-specific statutes to control the use of personal information in reaction to particular industry and consumer interests; however, these

[49] *Id*. at 224-25.

[50] *Id*.

[51] Seth Safier, *Between Big Brother and the Bottom Line: Privacy in Cyberspace*, 5 VA. J.L. & TECH. 6, ¶ 75 (2000).

statutes have not always been able to keep pace with advancing technology to protect consumers' privacy rights.[52]

Of some relevance in *Pisciotta*, which dealt with personal information provided to a bank, is the Gramm-Leach-Bliley Act ("GLBA").[53] The GLBA states that "[i]t is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information."[54] The GLBA accordingly requires certain agencies, including the Federal Trade Commission and the Securities Exchange Commission, to "establish appropriate standards for the financial institutions subject to their jurisdiction" in order to 1) "insure the security and confidentiality of customer records and information;" 2) "protect against any anticipated threats or hazards to the security or integrity of such records;" and 3) "protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer."[55] The GLBA further requires that financial institutions develop and give notice of their privacy policies to their customers at least annually.[56] Before a financial institution may share personal information with certain nonaffiliated companies, it must also provide its customers with the ability to opt out of this disclosure.[57] Although the GLBA is a move in the right direction for federal information privacy regulation, it does not create a private cause of action.[58] Therefore, a customer cannot sue

[52] *Id.* at ¶ 76.

[53] Financial Services Modernization (Gramm-Leach-Bliley) Act, 15 U.S.C. §§ 6801-6809 (2000).

[54] 15 U.S.C. § 6801(a).

[55] 15 U.S.C. § 6801(b).

[56] 15 U.S.C. § 6803(a).

[57] 15 U.S.C. § 6802(b).

[58] Vincent R. Johnson, *Cybersecurity, Identity Theft, and the Limits of Tort Liability*, 57 S.C. L. REV. 255, 267 (2005).

a financial institution for breaching its duty to protect the customer's personal information.[59]

Although there is not much federal guidance on information privacy, particularly within the context of personal information stored on databases, there is evidence that Congress realizes the growing necessity to regulate this area. Specifically, there are a number of Bills which are currently working their way through the political process.[60] These include S. 239: Notification of Risk to Personal Data Act,[61] H.R. 958: Data Accountability and Trust Act,[62] H.R. 836: Cyber-Security Enhancement & Consumer Data Protection Act,[63] and S. 495: Personal Data Privacy and Security Act of 2007.[64] These Bills contain provisions which would establish requirements for data security[65] and breach notification,[66] criminalize concealment of data breaches,[67] pre-empt state laws,[68] and delegate regulatory responsibility to the FTC.[69] Notably, however, none of these Bills provide for a private cause of action.

3. State Regulation

Considering the lack of regulation at the federal level, many states have attempted to provide some guidance in regulating database

[59] *Id.*

[60] *See* Scott Berinato, *Data Breach Notification Laws, State by State*, CSO, *available at* http://www.csoonline.com/read/020108/ammap/ammap.html.

[61] S. 239, 110th Cong. (2007).

[62] H.R. 958, 110th Cong. (2007).

[63] H.R. 836, 110th Cong. (2007).

[64] S. 495, 110th Cong. (2007).

[65] S. 495, 110th Cong. (2007); H.R. 958, 110th Cong. (2007).

[66] S. 495, 110th Cong. (2007); H.R. 958, 110th Cong. (2007); S. 239, 110th Cong. (2007); H.R. 836, 110th Cong. (2007).

[67] H.R. 836, 110th Cong. (2007).

[68] S. 495, 110th Cong. (2007); H.R. 958, 110th Cong. (2007); S. 239, 110th Cong. (2007); H.R. 836, 110th Cong. (2007).

[69] S. 239, 110th Cong. (2007); H.R. 958, 110th Cong. (2007); S. 495, 110th Cong. (2007).

security. Most of these states have followed the lead of California, which has the strongest privacy law in the country.[70] For example, as of January 2008, thirty-nine states and the District of Columbia have passed security breach notification laws,[71] with California the first to enact such a law in 2003.[72] Most security breach notification laws, as the one discussed in *Pisciotta*, require that companies which store personal information notify individuals in the event of a security breach where personal information is improperly accessed.[73]

Security breach notification laws became common following the security breach of ChoicePoint, a data aggregation company, in 2004.[74] At that time, California was the only state to have a notification law, and ChoicePoint sent more than 30,000 letters to California residents informing them that their personal information had been improperly accessed.[75] More than 145,000 consumers nationwide were affected by the breach though, many of whom were not notified of the breach due to lack of notification laws in their states of residence.[76] This incident caused many states to question their privacy standards and to enact notification laws of their own.[77]

Despite the states' efforts to create some protection for consumers' personal information through security breach notification statutes, consumers still have little means to ensure that their personal information is protected. Most of the notification statutes are extremely narrow in that they only create a duty to notify consumers of a security breach and do not expressly create a duty generally to protect data.[78] Additionally, most of these statutes do not provide for

[70] SOLOVE, *supra* note 20, at 227.

[71] *See* State Security Notification Laws, National Conference of State Legislatures, *available at* http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm.

[72] Security Breach Information Act, CAL. CIV. CODE § 1798.82(a) (2003).

[73] SOLOVE, *supra* note 20, at 228.

[74] *Id*. at 255.

[75] *Id*.

[76] *Id*.

[77] *Id*.

[78] *Id*.

civil action by an affected consumer in the event that a database owner breaches its duties under the statute.[79] The California notification statute is one of the few that both creates a data protection obligation and authorizes civil action for damages in this situation.[80]

It is with this understanding of the limited protection of information privacy in the context of database security breaches, and the limited avenues for redress by affected consumers in these situations, that we examine *Pisciotta v. Old National Bancorp.*

II. *PISCIOTTA V. OLD NATIONAL BANCORP*

Luciano Pisciotta and Daniel Mills brought a class action on behalf of customers and potential customers of Old National Bancorp ("ONB").[81] They alleged that ONB failed to secure personal information which had been solicited through ONB's website from applicants for banking services.[82] Depending on the service requested, customers or potential customers would provide their name, address, Social Security number, driver's license number, date of birth, mother's maiden name, and credit card or other financial account numbers over the website.[83] In 2005, as a result of ONB's failed security, a third-party computer hacker gained access to this private information of tens of thousands of people who used ONB's website.[84] The security breach was found to be "sophisticated, intentional and malicious."[85] ONB sent written notice to its customers of the intrusion, once it was notified by the hosting facility, NCR.[86]

---

[79] *See, e.g.*, LA. REV. STAT. ANN. § 51:3075 (2006); TENN. CODE ANN. § 47-1-101 (2005); WASH. REV. CODE ANN. § 19.255.010(10) (2005); N.C. GEN. STAT. ANN. § 75-65(d) (2005).

[80] CAL. CIV. CODE §§ 1798.81.5, 1798.84(b).

[81] Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 631 (7th Cir. 2007).

[82] *Id.*

[83] *Id.*

[84] *Id.*

[85] *Id.* at 632.

[86] *Id.*

A. Procedural History

The plaintiffs brought an action in the United States District Court for the Southern District of Indiana, having jurisdiction under the Class Action Fairness Act of 2005.[87] They alleged negligence claims against ONB and NCR, as well as breach of implied contract against ONB and breach of contract against NCR.[88] They alleged that they suffered "substantial potential economic damages and emotional distress and worry that third parties [would] use [the plaintiffs'] confidential personal information to cause them economic harm, or sell their confidential information to others who [would] in turn cause them economic harm."[89] The plaintiffs did not, however, claim any "*completed direct* financial loss" nor that any member of the class "*already had been* the victim of identity theft" because of the security breach.[90] The plaintiffs sought damages in the form of compensation for past and future credit monitoring costs.[91]

The district court granted NCR's motion to dismiss for failure to state a claim, leaving ONB as the sole defendant.[92] ONB moved for judgment on the pleadings and opposed the plaintiffs' motion for class certification.[93] The district court ruled in favor of ONB on both motions, concluding that "the plaintiffs' claims failed as a matter of law because 'they have not alleged that ONB's conduct caused them cognizable injury,'" where "under Indiana law, damages must be more

[87] *Id*. at 633. Under the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d), the district court had jurisdiction over the case because at least one member of the proposed class was a citizen of a state different from ONB (the class members included residents of Indiana, Illinois, Kentucky, Missouri, Ohio, and Tennessee) and the matter in controversy exceeded five million dollars, exclusive of interest and costs.

[88] *Pisciotta*, 499 F.3d 629, at 632.

[89] *Id*. (citing R.37 at 2).

[90] *Id*.

[91] *Id*. at 631.

[92] *Id*. at 632.

[93] *Id*.

than speculative."[94] Furthermore, the district court concluded that compensation for the cost of credit monitoring could not be an "'alternative award for what would otherwise be speculative and unrecoverable damages,'" as the cost to monitors one's credit is, "'not the result of any present injury, but rather the anticipation of the future injury that has not yet materialized.'"[95]

The plaintiffs appealed the judgment for ONB on the negligence and breach of implied contract claims to the Seventh Circuit, and also requested that the Seventh Circuit vacate the order denying class certification.[96]

B. Seventh Circuit Opinion

In an opinion written by Judge Ripple, the Seventh Circuit affirmed the judgment of the district court, concluding that the damages of past and future credit monitoring costs sought by the plaintiffs were not compensable under Indiana law.[97] Therefore, claims for negligence and breach of implied contract failed as a matter of law.[98] The Seventh Circuit reviewed the district court's decision *de novo* because it was based on a 12(c) motion for judgment on the pleadings.[99]

1. A Quick Look at Jurisdiction

Having found jurisdiction under the Class Action Fairness Act of 2005, the court went on to review its subject matter jurisdiction over the case.[100] In an interesting precursor to its discussion on the merits, the court noted that many federal courts (including those that the

[94] *Id*. (citing R.78 at 3).
[95] *Id*. (citing R.78 at 3-4).
[96] *Id*. at 633.
[97] *Id*. at 640.
[98] *Id*.
[99] *Id*. at 633.
[100] *Id*. at 633-34.

district court relied on in its reasoning) concluded that they did not have jurisdiction in similar cases where the plaintiffs' data had been compromised but not yet misused, because these plaintiffs had not met the injury-in-fact requirement for standing under Article III.[101] The court went on to say, however, that the injury-in-fact requirement of Article III could be "satisfied by a threat of future harm or by an act which harms the plaintiff only by increasing the risk of future harm that the plaintiff would have otherwise faced, absent the defendant's actions." Therefore, the court reasoned, it had jurisdiction over the matter.[102] In its following discussion, however, the court concluded that this potential harm, which was enough to confer standing, was not enough to bring a successful claim for negligence or breach of implied contract.[103]

2. Was There Requisite Harm?

The main issue in *Pisciotta* was whether "the harm caused by identity information exposure, coupled with the attendant costs to guard against identity theft, constitutes an existing *compensable injury and consequent damages* required to state a claim for negligence or for breach of contract."[104] Stemming from this issue was the more general question of whether Indiana would recognize a cause of action for a data exposure injury,[105] a question with substantial ramifications under Indiana law, considering it had never been addressed.

Because the case was brought under diversity jurisdiction and alleged causes of action under Indiana law, the court was required to apply the substantive law of Indiana.[106] As stated above, however, there was no Indiana precedent addressing the issue at hand.[107]

---

[101] *Id.* at 634.
[102] *Id*.
[103] *Id*. at 640.
[104] *Id*. at 635.
[105] *Id*. at 636.
[106] *Id*. at 634.
[107] *Id*. at 635.

Therefore, the court was required to examine the case based on its prediction of how the Supreme Court of Indiana would decide it.[108] To do this, the court considered 1) Indiana legislation on the issue,[109] 2) Indiana case law regarding analogous areas of the law,[110] and 3) the reasoning of other courts applying the law of other jurisdictions, but on the same legal issue.[111] Although the Seventh Circuit would look at this range of sources for guidance, it emphasized that it would take a restrictive approach to this "novel theory of liability."[112] The court asserted, "Without state authority to guide us, '[w]hen given a choice between an interpretation of [state] law which reasonably restricts liability, and one which greatly expands liability, we should choose the narrower and more reasonable path.'"[113]

a. Indiana Legislation

In deciding whether the plaintiffs had suffered the requisite harm for a successful negligence or breach of contract claim, the court first looked at Indiana legislation on the matter.[114] Specifically, it examined a statute which was enacted on March 21, 2006 and imposes certain duties on private entities (as well as state agencies) if their databases which contain personal information are accessed by unauthorized third parties.[115] The statute, in effect, is one of notification, requiring a database owner who knows or should know of a security breach to notify all potentially affected consumers of that breach.[116] It further requires the database owner to provide information to each consumer

[108] *Id*.
[109] *Id*. at 636-37.
[110] *Id*. at 637-39.
[111] *Id*. at 639-40.
[112] *Id*. at 636.
[113] *Id*. at 635-36 (quoting Todd v. Societe Vic, S.A., 21 F.3d 1402, 1412 (7th Cir 1994)).
[114] *Id*. at 636-37.
[115] *Id*. at 636 (citing I.C. § 24-4.9 *et seq*.).
[116] *Id*. at 637 n.6.

reporting agency, where the breach potentially affects more than one thousand consumers.[117] It is interesting to note that the court recognized that the statute took effect on July 1, 2006, after the incident involved in *Pisciotta*, and thus was not directly relevant to the case.[118] Nonetheless, the court looked at the statute for guidance on how the Indiana Supreme Court would rule on the matter.[119]

The Seventh Circuit noted that the Indiana statute requires no affirmative act other than notification, and that if the database owner fails to notify, enforcement actions may only be taken by the Attorney General of Indiana.[120] The court concluded, therefore, that the legislation creates no private right of action by a consumer against the database owner, and likewise creates "no duty to compensate affected individuals for inconvenience or potential harm to credit."[121] Significantly, the court rejected the plaintiffs' argument that the statute is evidence of the Indiana legislature's belief that an individual has suffered a compensable injury when his or her personal information is wrongfully acquired by a third party in a security breach.[122] Rather, the court concluded that the Indiana legislature would have made a definite statement of its intent to create a cause of action in such a situation.[123]

Having found no support for the plaintiffs' allegations in light of Indiana legislation, the court then turned to Indiana case law dealing with analogous legal issues.[124]

[117] *Id*.
[118] *Id*. at 636-37.
[119] *Id*.
[120] *Id*. at 637.
[121] *Id*.
[122] *Id*.
[123] *Id*.
[124] *Id*. at 637-39.

b. Indiana Case Law

The plaintiffs argued that there was Indiana case law in analogous settings acknowledging that banks have a special duty to prevent disclosure of their customers' private information.[125] They further argued that Indiana courts recognized that failure to perform this duty could result in harm to customers.[126] The court quickly dismissed these arguments, stating that the cases presented by the plaintiffs were of "marginal assistance" because the facts of the cases were not similar enough to the facts of the instant case.[127] Specifically, the court distinguished the cases cited by the plaintiffs by noting that the plaintiffs in those cases were compensated for harm from injuries to their reputation that were "direct and immediate," whereas the plaintiffs in *Pisciotta* sought compensation for "guarding against some future, anticipated harm."[128]

After dismissing the plaintiffs' arguments regarding analogous case law, the court, on its own, examined the possibly analogous case law of toxic tort liability.[129] In this setting, the court was able to find precedent from the Supreme Court of Indiana implying that "compensable damage requires more than an exposure to a future potential harm."[130] It explained further that even courts allowing medical monitoring damages, those being damages to monitor harm after toxic exposure, showed doubt that there should be an allowance for credit monitoring damages.[131] Moreover, no Indiana courts were

[125] *Id*. at 637-38.

[126] *Id*. The plaintiffs cited Ind. Nat'l Bank v. Chapman, 482 N.E.2d 474 (Ind. Ct. App. 1985) and Am. Fletcher Nat'l Bank & Trust Co. v. Flick, 252 N.E.2d 839 (Ind. Ct. App. 1969).

[127] *Pisciotta*, 499 F.3d at 638.

[128] *Id*.

[129] The court, however, was careful to qualify this argument, stating that it did not have to "endorse this analogy for present purposes." *Id*. at 639.

[130] *Id*. at 638-639 (citing Allied Signal, Inc. v. Ott, 785 N.E.2d 1068 (Ind. 2003)).

[131] *Id*. at 639 (citing the Southern District of Ohio in Kahle v. Litton Loan Servicing, LP, 486 F. Supp. 2d 705, 712 (S.D. Ohio 2007)).

among those allowing medical monitoring damages.[132] In fact, the court contended that by looking at the Supreme Court of Indiana's treatment of toxic tort liability, it seemed that the Supreme Court of Indiana actually "supports the view that no cause of action for credit monitoring is available."[133]

Again, having found no support for the plaintiffs' cause of action, and with no other authority from Indiana law, the Seventh Circuit proceeded to examine the reasoning of other courts applying the law of other jurisdictions, but to the same legal issue presented in *Pisciotta*.

c. Case Law From Other Jurisdictions

The court listed a number of district court cases, including from districts in Ohio, Minnesota, Arizona, and Michigan, where plaintiffs with similar allegations to those in *Pisciotta* were denied damages because they had not suffered the requisite harm.[134] The court concluded by stating that it would not "adopt a 'substantive innovation' in state law or '[] invent what would be a truly novel tort claim' on behalf of the state absent some authority to suggest that the approval of the Supreme Court of Indiana is forthcoming." [135] This was particularly in light of the fact that the plaintiffs had not brought forth any case or statute authorizing the cause of action they sought recovery under.[136]

---

[132] *Id*.

[133] *Id*. (citing *Allied Signal*, 785 N.E.2d 1068).

[134] *Id*. (citing *Kahle*, 486 F. Supp. 2d at 712-13; Hendricks v. DSW Shoe Warehouse, 444 F. Supp. 2d 775, 783 (W.D. Mich. 2006); Guin v. Brazos Higher Educ. Serv. Corp., Inc., No. 05-668, 2006 U.S. Dist. LEXIS 4846 (D. Minn. Feb. 7, 2006); Stollenwerk v. Tri-West Healthcare Alliance, No. 03-0185, 2005 U.S. Dist. LEXIS 41054 (D. Ariz. Sept. 8, 2005)).

[135] *Id*. at 640 (quoting Combs v. Int'l Ins. Co., 354 F.3d 568, 578 (6th Cir. 2004) and Insolia v. Philip Morris, Inc., 216 F.3d 596, 607 (7th Cir. 2000); and citing Birchler v. Gehl Co., 88 F.3d 518, 521 (7th Cir. 1996) and Ry Express Agency, Inc. v. Super Scale Models, Ltd., 934 F.2d 135, 138 (7th Cir. 1991)).

[136] *Id*. at 639-40.

III. COULD *PISCIOTTA* HAVE COME OUT DIFFERENTLY?

The Seventh Circuit made clear in *Pisciotta* that it would not recognize a claim to recover past and future credit monitoring damages from a database owner following a database security breach, where the only harm suffered was the wrongful access of the plaintiffs' personal information, and where no identity theft or other fraud resulted. Despite the Seventh Circuit's definite language in reaching this conclusion, it is valuable to explore whether *Pisciotta* could have come out differently for the plaintiff consumers (and consequently for similarly situated consumers in future cases). In particular, we look at whether the plaintiffs could have recovered by analogizing their injury to that suffered in a toxic tort claim. We also look at whether the court could have disregarded the economic loss doctrine, which limits economic recovery in negligence actions. Through this analysis, we recognize that a favorable result for the plaintiffs was possible in theory, but not in practice. Plaintiffs therefore need to look to new legislation, as discussed in Part IV, in order to recover credit monitoring damages in these situations.

A. Analogizing to Toxic Tort Liability

An interesting argument that the plaintiffs in *Pisciotta* failed to make, but that the Seventh Circuit raised on its own, was whether an injury could be found by analogizing data breach liability to toxic tort liability.[137] Multiple state and federal courts have allowed victims of toxic exposure, without proof of further injury caused by the exposure, to recover medical monitoring damages.[138] If the analogy between

[137] *Id*. at 638-39.

[138] Johnson, *supra* note 58, at 307-08 (citing Carey v. Kerr-McGee Chem. Corp., 999 F. Supp. 1109, 1119 (N.D. Ill. 1998); Witherspoon v. Philip Morris, Inc., 964 F. Supp. 455, 467 (D.D.C. 1997); Redland Soccer Club, Inc. v. Dep't of the Army, 696 A.2d 137, 145 (Pa. 1997);Potter v. Firestone Tire & Rubber Co., 836 P.2d 795, 824-25 (Cal. 1993)). *See also*, In re Paoli R. Yard PCB Litig., 916 F.2d 829 (3d Cir. 1990); Friends for All Children, Inc. v. Lockheed Aircraft Corp., 746 F.2d 816 (D.C. Cir. 1984); Patton v. Gen. Signal Corp., 984 F. Supp. 666 (W.D.

toxic exposure and exposure of personal information to identity theft is accepted, it follows that these courts could also allow for the recovery of credit monitoring damages.

The analogy is as follows: a consumer who loses personal information due to a database security breach is like a person who suffers exposure to a toxic substance in that both risk greater harm to their person as a result of this occurrence.[139] In the case of toxic exposure, the exposed party has increased chances of having a disease, while in the case of a database security breach, the exposed consumer has increased chances of falling victim to identity theft and fraud.[140] In either case, the victim of the exposure is in the best position to mitigate future harm by, in the least, monitoring the risk of the future harm.[141]

In theory, because there was no Indiana authority on awarding credit monitoring damages, the Seventh Circuit could have looked at other jurisdictions, including those that have accepted medical monitoring damages, and used this authority to support a finding for credit monitoring damages under Indiana law. The Supreme Court of Indiana, however, had spoken to the issue of awarding damages in a toxic exposure case.[142] The Supreme Court of Indiana ruled in *Allied Signal, Inc. v. Ott* that "no compensable injury occurs at the time of [toxic] exposure."[143] Therefore, the Seventh Circuit was constrained to this ruling. Although other states have allowed medical monitoring

N.Y. 1997); Gibbs v. E.I. DuPont De Nemours & Co., 876 F. Supp. 475 (W.D. N.Y. 1995); Bocook v. Ashland Oil, Inc., 819 F. Supp 530 (S.D. W. Va. 1993); Bower v. Westinghouse Electric Corp., 522 S.E. 2d 424, 431 (W. Va. 1999); Bourgeois v. A.P. Green Indus., Inc., 716 So.2d 355 (La. 1998); Simmons v. Pacor, Inc., 674 A.2d 232 (Pa. 1996); Hansen v. Mountain Fuel Supply Co., 858 P.2d 970 (Utah 1993); Theer v. Philip Carey Co., 628 A. 2d 724, 733 (N.J. 1993); Ayers v. Jackson Twp., 525 A.2d 287 (N.J. 1987); Burns v. Jaquays Mining Corp., 752 P.2d 28 (Ariz. App. 1987).

[139] Johnson, *supra* note 58, at 308.

[140] *Id*.

[141] *Id*.

[142] *Pisciotta*, 499 F.3d at 639 (citing Allied Signal, Inc. v. Ott, 785 N.E.2d 1068 (Ind. 2003)).

[143] *Id*. (citing *Allied Signal*, 785 N.E.2d at 1075).

damages, Indiana is not one of them.[144] Therefore, even if the Seventh Circuit found the analogy to be apt, which it did not take a position on, it would be forced to conclude that credit monitoring damages were not available following a database security breach, just as medical monitoring damages were not available following toxic exposure.[145]

Still, this leaves the door open for actions seeking credit monitoring damages brought to the Seventh Circuit under other states' laws. For example, it remains largely unsettled in Illinois whether medical monitoring damages are available without physical injury.[146] Therefore, it is possible, though still rather unlikely, that the Seventh Circuit could recognize credit monitoring damages in a case brought under Illinois law, if the court accepted the analogy to medical monitoring damages.

B. Economic Loss Doctrine

The plaintiffs in *Pisciotta* also could have made the argument that the standard for proving compensable injury should have been broadened in the context of a database security breach because the economic loss doctrine, which effectively narrows the standard, is not implicated in this context. The economic loss doctrine states that in order for a plaintiff to recover economic losses resulting from a defendant's negligence, the plaintiff must have suffered physical harm to his or her person or property.[147] This doctrine, although having its roots in product liability, is applicable in most negligence cases and may effectively limit recovery in tort cases involving internet security, as implicitly illustrated in *Pisciotta*. The concept of physical harm to

[144] *Id*.

[145] *Id*. at 639 n.10.

[146] Guillory v. Am. Tobacco Co., No. 97 C 8641, 2001 U.S. Dist. LEXIS 3353 (N.D. Ill. Mar. 20, 2001); Carey v. Kerr-McGee Chem. LLC, No. 96 C 8583, 1999 U.S. Dist. LEXIS 16232 (N.D. Ill. Oct. 4, 1999); Campbell v. A.C. Equip. Servs. Corp., Inc., 610 N.E.2d 745, 751 (Ill. App. Ct. 1993).

[147] *See* E. River S.S. Corp. v. Transamerica Delaval, Inc., 476 U.S. 858 (1986); Seely v. White Motor Co., 403 P.2d 145 (Cal. 1965) (Chief Justice Roger Traynor is credited with first articulating the doctrine in this landmark decision).

one's person or property is a questionable one though in the context of cybertorts, and it is for this reason that we need to evaluate the purpose and value of the economic loss doctrine in this context.

The economic loss doctrine has three significant functions: 1) to protect a defendant from a disproportionately wide range of liability,[148] 2) to ensure that damages are proven with certainty, and 3) to define a doctrinal boundary between tort and contract law.[149] If one looks only at the damages requested in *Pisciotta*, the costs of credit monitoring, one realizes that the functions of the economic loss doctrine are not met. The doctrine is thus an unnecessary limitation on recovery in this context.

First, the scope of liability in *Pisciotta* is not in question. Limiting the scope of a defendant's liability is certainly crucial in tort law, considering that "acts of negligence often have extremely broad adverse economic consequences."[150] This is also the reason why most jurisdictions require proof of proximate causation in a negligence action. A defendant otherwise could be sued by parties having almost no relation to the negligent act. In *Pisciotta*, however, the plaintiffs were all customers or potential customers of ONB who had provided ONB with personal information.[151] It was consequently the information of these plaintiffs that was stolen through the security breach of ONB's database.[152] As such, the liability of the defendant is restricted to ONB's customers.

Second, the plaintiffs in *Pisciotta* could prove their requested damages with certainty. This is not a situation where the court must calculate lost economic opportunity, a situation that the economic loss doctrine most directly addresses under this function. By requiring that damages be proven with reasonable certainty, the economic loss doctrine not only ensures that defendants not pay for speculative

[148] *See* Robert L. Rabin, *Tort Recovery for Negligently Inflicted Economic Loss: A Reassessment*, 37 STAN. L. REV. 1513, 1533 (1985).

[149] Johnson, *supra* note 58, at 296.

[150] *Id*. at 296-97.

[151] Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 631 (7th Cir. 2007).

[152] *Id*.

amounts, it also "promotes judicious use of limited judicial resources, ensuring that those scarce assets are not squandered on the burdensome, and perhaps dubious, task of trying to quantify endless economic losses that may, in truth, not be provable with reasonable precision."[153] In *Pisciotta*, however, the plaintiffs would merely need to present receipts or online invoices showing the cost of past and, to the extent reasonable, future credit monitoring services they used or would use following the security breach of ONB's database. One can go to the website of almost any credit monitoring service provider and find the price for services, which generally range from ten to fifteen dollars per individual per month.[154] Therefore, damages could be limited to this amount, protecting ONB from paying mere speculative amounts.

Lastly, as argued by Professor Vincent Johnson, providing a plaintiff with the costs of credit monitoring after a database security breach, as requested in *Pisciotta*, would not pose a problem in delineating between tort and contract law.[155] Professor Johnson explains that the protection of personal information in databases should not be an area of bargaining between consumers and database owners.[156] The majority of states, through their data breach notification statutes, seem to support this idea.[157] Even though database owners may have privacy policies that must be accepted by consumers, consumers should not be able to contract out of their right to sue for credit monitoring costs through these policies. Furthermore, plaintiffs arguing breach of contract in these situations would likely be unable to recover credit monitoring costs if they were not expressly contracted for, because they would be considered consequential damages, which are generally difficult to recover if not contemplated

[153] Johnson, *supra* note 58, at 297-98 (citing Vincent R. Johnson & Alan Gunn, STUDIES IN AMERICAN TORT LAW 7, 9 (3d ed. 2005)).

[154] *See, e.g.*, http://www.equifax.com/credit-product-list/; http://www.truecredit.com; http://www.identityguard.com.

[155] Johnson, *supra* note 58, at 300-01.

[156] *Id*.

[157] *Id*.

at the time of contract formation.[158] Rather, tort law is better equipped to provide for recovery of the cost of credit monitoring, where compensation would depend on the reasonableness of these costs in the context of each case.[159]

In all, the plaintiffs in *Pisciotta* could have argued that courts should not be limited by the economic loss doctrine when deciding whether plaintiffs have suffered the requisite compensable injury in a data security breach case where the consequent damages are the cost of credit monitoring, because the functions of the economic loss doctrine are not implicated in this context. Nonetheless, considering that the Seventh Circuit traditionally has espoused the economic loss doctrine, with Judge Posner as one of its strongest advocates,[160] this argument would not ensure the plaintiffs in *Pisciotta* recovery of credit monitoring costs.

IV. WHERE DO CONSUMERS GO FROM HERE?

Following *Pisciotta*, it is clear that the Seventh Circuit is not willing to find a common law cause of action under tort law, at least in Indiana, to provide credit monitoring costs to consumers who have lost personal information due to a database security breach. The court noted in *Pisciotta* that allowing for recovery of credit monitoring costs after a security breach would constitute a "substantive innovation" in state law, and the court justifiably refused to do this.[161] In the short time since *Pisciotta* was decided, it has already been followed by a district court in the Fifth Circuit,[162] having ruled that consumers need to prove more than wrongful access to their personal information to

[158] *Id*. at 301 n.307.

[159] *Id*. at 301.

[160] *See* Miller v. U.S. Steel Corp., 902 F.2d 573 (7th Cir. 1990); Rardin v. T & D Mach. Handling, Inc., 890 F.2d 24 (7th Cir. 1989). *See also* Thomas J. Miles, *Posner on Economic Loss in Tort: EVRA Corp v Swiss Bank*, 74 U. CHI. L. REV. 1813 (2007); Richard A. Posner, *Common-Law Economic Torts: An Economic and Legal Analysis*, 48 ARIZ. L. REV. 735 (2006).

[161] Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 640 (7th Cir. 2007).

[162] Ponder v. Pfizer, Inc., 522 F. Supp. 2d 793 (M.D. La. 2007).

recover under tort law, and that credit monitoring costs are thus not compensable damages.[163] As noted above, there are also other district courts, including in Ohio,[164] Minnesota,[165] Arizona,[166] and Michigan[167] which decided, prior to *Pisciotta*, that credit monitoring costs are not recoverable after a database security breach. Although there is thus reason to believe that consumers in many states will not be able to recover credit monitoring costs through common law when the consumers' personal information is wrongfully accessed, the issue remains whether consumers should be able to recover credit monitoring costs despite the court decisions. If so, their best prospect for recovery is through new legislation.

A. Why Require Credit Monitoring Services?

Legislatures should require that database owners offer credit monitoring services to all consumers whose personal information has been wrongfully accessed due to a database security breach. This would be advantageous to database owners as well as consumers.

In 2007, the average cost to a database owner following a database security breach by a third-party hacker was $231 per compromised record (this cost is even greater for financial institutions where consumers have higher expectations of security).[168] The cost of lost business due to customer turnover accounted for about 56% of this total cost, and the cost of providing credit monitoring accounted for only 1%.[169] One must note that even though a database owner may

[163] *Id.* at 797.

[164] Kahle v. Litton Loan Servicing, LP, 486 F. Supp. 2d 705 (S.D. Ohio 2007).

[165] Guin v. Brazos Higher Educ. Serv. Corp., Inc., No. 05-668, 2006 U.S. Dist. LEXIS 4846 (D. Minn. Feb. 7, 2006).

[166] Stollenwerk v. Tri-West Healthcare Alliance, No. 03-0185, 2005 U.S. Dist. LEXIS 41054 (D. Ariz. Sept. 8, 2005).

[167] Hendricks v. DSW Shoe Warehouse, 444 F. Supp. 2d 775 (W.D. Mich. 2006).

[168] 2007 Annual Study: U.S. Cost of a Data Breach (study by the Ponemon Institute, LLC) (Nov. 2007).

[169] *Id*.

offer credit monitoring services, only about five to thirty percent of the affected consumers actually exercises this offer, which translates to the database owner's cost.[170] Therefore, a database owner's greatest concern following a security breach is the loss of customers.

By requiring that database owners provide credit monitoring services, consumers may be more sympathetic to the database owners (particularly in the case of a breach by a third-party hacker) and thus give a second thought to transferring their business. Furthermore, by offering credit monitoring services, database owners could potentially save future legal costs related to a security breach. Many companies already voluntarily provide affected consumers with credit monitoring after database security breaches, recognizing the potential liability if such monitoring does not take place.[171] After all, credit monitoring decreases affected consumers' risks of falling victim to identity theft and other fraud. Providing for credit monitoring services, though less of a cost than other potential liability, would still be a considerable expense for database owners, and therefore would also create an incentive for these owners to increase database security. With this increase in security, database owners will likely see an increase in their online business because consumers will feel that their personal information is being better protected.

For affected consumers, such legislation would at least provide compensation for out-of-pocket expenses. As seen in *Pisciotta*, consumers face an up-hill battle in protecting information privacy through common law. Unless they are victims of identity theft or other actual fraud, consumers will have significant difficulty receiving even those out-of-pocket expenses through a negligence or breach of contract action considering, among other difficulties, the high standard of proving a compensable injury. Affected consumers of a database security breach may also find it difficult in a negligence action, for

[170] Bob Sullivan, *Few Takers for Free Credit Monitoring*, MSNBC (April 20, 2006) *available at* http://redtape.msnbc.com/2006/04/few_takers_for_.html.

[171] John B. Kennedy & Anne E. Kennedy, *What Went Wrong? What Went Right? Corporate Responses to Privacy and Security Breaches*, PLI: Patents, Copyrights, Trademarks, and literary Property Course Handbook Series, 61-62 (2007).

example, to prove proximate causation, because the intentionally tortious or criminal conduct of a hacker may break the chain of causation, thus absolving the database owner of liability.[172] As stated above, requiring database owners to provide credit monitoring services following a database breach will also likely improve database security, which surely is advantageous for consumers providing personal information online.

B. Other Proposed Legislation

Professor Vincent Johnson proposes legislation which would allow consumers to recover credit monitoring costs when their personal information is wrongfully accessed, provided that these credit monitoring costs are a limitation on a database owner's liability.[173] The fact that most states have enacted security breach notification statutes illustrates that there is a recognized privacy interest in the personal information provided to the database owners.[174] In practice, however, the notification statutes provide limited protection, because many of these statutes do not ensure that affected consumers receive the most expedient notice which is crucial in minimizing harm following a security breach.[175] Database owners are generally only obligated to notify consumers of a database breach upon actual discovery or notification of the breach, when in reality they may be able to discover the breach earlier, yet have no incentive to do so.[176] By introducing credit monitoring costs as a statutory remedy and a limitation on liability, database owners will have an incentive to discover security breaches as early as possible so as to shift liability to the consumer as early as possible.[177] Once a database owner notifies an affected

[172] Johnson, *supra* note 58, at 309 (citing Restatement (Second) of Torts 448 (1965)).

[173] *Id*. at 306.

[174] *Id*.

[175] *Id*. at 306-07. *See, e.g.*, CAL. CIV. CODE § 1798.29(a) (2003).

[176] Johnson, *supra* note 58, at 306.

[177] *Id*. at 307.

consumer of a security breach, the database owner would only be liable for credit monitoring costs from that point and for no other liabilities resulting from the security breach.

The advantages for database owners and for consumers are, for the most part, the same as those from legislation without a cap on liability. For database owners, however, limiting liability to credit monitoring costs is even more advantageous than simply requiring credit monitoring costs because it would necessarily prevent devastating liability from subsequent legal actions.[178] Without this cap, their risk of liability is merely decreased.

Consumers, on the other hand, do face the disadvantage of not being able to bring a negligence claim against the database owner once they have actually suffered financial injury through identity theft or fraud. On the whole, however, the majority of affected consumers will not fall victim to identity theft or fraud, and would prefer some redress following a security breach than none. Furthermore, with free credit monitoring services, consumers should be less likely to fall victim to identity theft in the first place, consequently lessening this disadvantage.

CONCLUSION

Pisciotta is a fascinating case because it highlights the difficulties plaintiffs face when the law does not necessarily keep up with the advancement of technology. Indeed, *Pisciotta* presented the Seventh Circuit with an issue it had never faced: whether the costs of credit monitoring spent by consumers whose personal information was wrongfully accessed through a database security breach, but who were not victims of identity theft or fraud, are compensable damages and thus recoverable under a negligence or breach of contract action. The Seventh Circuit was unwilling to extend the definition of compensable damages to the costs of credit monitoring in this situation, and definitively refused to create a common law cause of action for such damages.

[178] *Id*. at 309.

Following *Pisciotta* then, individuals in Indiana whose personal information is wrongfully accessed because of a database security breach effectively have no avenue of redress unless they fall victim to identity theft or other fraud. Although this is a rather narrow reading of *Pisciotta*, it can easily be broadened to encompass other states in the Seventh Circuit and even beyond the Seventh Circuit because of the similar state of the law regarding database security breaches. Most states have security breach notification laws, but do not require database owners to provide affected consumers with credit monitoring services. If other circuits follow the Seventh Circuit in refusing credit monitoring damages, there will not only be lack of redress through regulation, but lack of redress through the common law. Consumers therefore need to rely on their legislators to create statutory credit monitoring damages, if they are to receive them at all.