CAN'T GET NO SATISFACTION: THE CONSEQUENCES OF *PISCIOTTA V. OLD NATIONAL BANCORP*, 499 F.3D 629 (7TH CIR. 2007) FOR POTENTIAL VICTIMS OF IDENTITY THEFT*

Amanda Blades**

I. INTRODUCTION

Pisciotta v. Old National Bancorp[1] represents the continuing trend in cases that have barred recovery of damages for plaintiffs whose personal and financial information has been compromised, but has not yet been used fraudulently. There is little doubt that electronic services provide benefits to both businesses and consumers. Online services provide businesses with a quick and inexpensive way to conduct business, while consumers have the convenience of obtaining service from home. However, identity theft has become more prevalent with the increased use of online services.[2] According to a recent study, there were approximately 15 million identity theft victims in 2006.[3] Given the frequency and the harm that can result, identity theft has proven to be a serious concern for many consumers.

With all of the problems caused by the electronic storage of personal information, the court should reconsider forcing potential victims of identify theft to wait in limbo until identity theft actually occurs before providing a remedy. Although the *Pisciotta* decision can be supported by the limited case law refusing to allow recovery for credit monitoring, the decision should be overturned due to compelling policy arguments that justify recovery. To illustrate this point, Section II of this casenote outlines the concerns facing consumers that engage in online business and briefly introduces readers to the *Pisciotta* decision. Section III then discusses the *Pisciotta* decision, including

---

* Best Legal Casenote (2008), Southern Illinois University Law Journal

** J.D., Southern Illinois University School of Law. Amanda would like to thank Professor R.J. Robertson for offering his time and expertise so generously. She would also like to thank her fiance, Garrett, for all the love and laughter. She would especially like to thank her parents, Charles and Rebecca, for their constant encouragement and support.

1. Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629 (7th Cir. 2007).
2. Gartner, Inc., http://www.gartner.com/it/page.jsp?id=501912 (last visited Mar. 19, 2009). Gartner, Inc. is an information technology (IT) research and advisory company.
3. *Id.*

facts and procedural history. Finally, Section IV contains an analysis of why the *Pisciotta* decision should be overturned, including several policy reasons for doing so, such as deterring negligence in storing sensitive information, preventing injustice to the consumer, and preventing loss by encouraging early detection of identity theft.

II. BACKGROUND

Identity thieves can obtain personal information in a number of ways, including stealing mail, wallets and purses, rummaging through the trash, etc.[4] However, "the weak links are found among the five or more million businesses that accept electronic payments from consumers," as well as the consumers.[5] In fact, electronic theft of personal financial information is the leading cause of certain types of fraud, including credit card and bank account fraud.[6] Consumers often entrust personal and financial information to an institution, such as a bank, in order to obtain online financial services. The bank will then store this personal information in a database for easy access. Problems arise when an unauthorized third party manages to access this information. The unauthorized person, using someone else's personal information, is then free to purchase goods and services on the credit of the other person, leaving the fraud victim to bear the costs of repairing the harm. Once the personal information is obtained, it can be used in many ways, including opening new credit card and bank accounts and obtaining loans, to name a few.[7] Additionally, personal information can be used to avoid criminal charges, requiring the identity theft victim to show up for court dates and possibly be arrested.[8]

As more businesses provide online services, there is an increased risk that consumers using these services will have their personal information accessed by an unauthorized third party. The Federal Trade Commission has made several recommendations for businesses to safeguard the personal information of their customers.[9] Even if businesses do take such measures, this does not

4. Federal Trade Commission, http://www.ftc.gov/bcp/edu/microsites/idtheft/ consumers/about-identity-theft.html (last visited Mar. 19, 2009) [hereinafter FTC].
5. Gartner, *supra* note 2.
6. *Id*.
7. FTC, *supra* note 4.
8. *Id*.
9. FTC, http://www.ftc.gov/infosecurity, (last visited Mar. 19, 2009).

guarantee that identity theft will not occur. In fact, identity theft has actually increased significantly from 2006 to 2007.[10]

Relief is possible for victims of identify theft or consumer fraud whose personal information has been used to their detriment. Identity theft is not recognized as an independent cause of action, but plaintiffs have been able to recover based on a theory of negligence.[11] However, courts have provided little protection for those whose personal information has been compromised, but has not yet been misused. The courts have refused to recognize the compromising of personal information as a cognizable injury without the actual fraudulent use of that information.

The problem faced by the court in *Pisciotta* is whether sensitive financial information must be used fraudulently by an unauthorized third party in order to constitute a compensable injury.[12] The court rejected the idea of imposing the costs of credit monitoring on the financial institution,[13] but some statistics indicate that the troubles associated with credit monitoring can become both costly and time consuming for the customers. According to a 2007 survey, victims of identity theft spent an average of 116 hours recovering from the effects of identify theft, and not everyone was able to correct negative credit records.[14] In addition to any immediate financial loss, victims reported additional secondary effects of the identity theft, including continuing calls from collection agencies, canceled credit cards, and effects on employment and tenancy.[15] Obviously, these problems are the result of an actual fraudulent use of personal information, but they are also the same concerns faced by those who are at an increased risk of identity theft. The 2007 survey revealed that 82% of identity theft victims became aware that they had been victimized due to adverse action, and in many cases, it took up to three months following the crime to discover the identity theft.[16] However, if a customer could have their credit monitored, the negative and long-lasting effects of identity theft could be prevented by allowing those at an increased risk of identity theft to recover the costs of credit monitoring for a reasonable amount of time.

---

10. Identity Theft Resource Center, http://www.idtheftcenter.org/artman2/publish/m_press/Identity_Theft_The_Aftermath_2007.shtml, (last visited Mar. 19, 2009) [hereinafter ITRC].
11. *See e.g.*, Murray v. Bank of Am., 580 S.E.2d 194 (S.C. Ct. App. 2003).
12. *Pisciotta*, 499 F.3d 629.
13. *Id*.
14. ITRC, *supra* note 10.
15. *Id*.
16. *Id*.

III. EXPOSITION OF THE CASE

A. The Facts

The defendant, Old National Bancorp (ONB), operated a website allowing potential customers to fill out online applications for banking services. ONB, an Indiana corporation, provides services to its home state, as well as to citizens of Illinois, Kentucky, and Ohio.[17] Due to the nature of the services provided, many of the applications required personal information, including social security numbers, financial account numbers, and other confidential information.[18] Mr. Pisciotta opened an online checking account in 2002 using ONB's website, although he closed the account two months later.[19] Mr. Mills, co-plaintiff in the case, also applied for an account online for his law firm in 2004, although he never actually used ONB's banking services.[20]

A hosting facility known as NCR maintained ONB's website.[21] In 2005, NCR informed ONB that there had been a security breach of the website.[22] Although the specific details remain undisclosed, a third-party found a way to hack[23] into ONB's website to access confidential information of ONB's customers.[24] Despite the breach, neither Mr. Pisciotta nor Mr. Mills had yet been the victim of identity theft as of the date the suit was filed.[25]

B. Procedural History

Mr. Pisciotta and Mr. Mills brought suit in the United States District Court for the Southern District of Indiana against both ONB and NCR.[26] The lawsuit was filed on behalf of both the plaintiffs and other customers of ONB affected by the security breach.[27] The complaint asserted claims of negligence against both defendants, a breach of implied contract claim against ONB, and

---

17. Brief of Appellee at 5, Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629 (7th Cir. 2007) (No. 06-3817).
18. Pisciotta, 499 F.3d at 631.
19. Brief of Appellants at 4, Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629 (7th Cir. 2007) (No. 06-3817).
20. *Id.*
21. *Pisciotta*, 499 F.3d at 632.
22. *Id.*
23. According to Merriam-Webster, hacking refers to acquiring access to a computer illegally. MERRIAM-WEBSTER'S COLLEGIATE DICTIONARY (11th ed. 2003).
24. *Pisciotta*, 499 F.3d at 632.
25. *Id.*
26. *Id.*
27. *Id.*

a breach of contract claim against NCR.[28] The plaintiffs alleged that they "have incurred expenses in order to prevent their confidential personal information from being used and will continue to incur expenses in the future."[29] The plaintiffs also sought other equitable relief, including a credit monitoring system to prevent the use of their confidential information by unauthorized individuals.[30]

NCR filed a motion for dismissal for failure to state a claim, which the district court granted.[31] The plaintiffs did not appeal the ruling.[32] The district court also granted ONB's motion for judgment on the pleadings.[33] The district court determined that the plaintiffs' allegation of possible economic harm in the future was too speculative, and therefore, they did not have a valid claim.[34] The district court also ruled that a breach of contract claim required an allegation of a compensable damage, which it found lacking in this case.[35]

Finally, the district court rejected the plaintiffs' suggestion for credit monitoring in the alternative to monetary damages.[36] The district court explored several cases from other district courts throughout the country that had considered credit monitoring as a possible remedy but ultimately rejected the idea as too speculative.[37] The plaintiffs filed a timely appeal as to the claims for negligence and breach of implied contract.[38]

C. Reasoning

The Seventh Circuit Court of Appeals began its review of the case by discussing whether the plaintiffs had standing pursuant to Article III of the U.S. Constitution, which requires injury-in-fact.[39] The cases relied upon by the district court determined that individuals whose personal information had been at risk for harm, but that no harm had yet occurred, did not meet the

---

28. *Id*.
29. Brief of Appellants at 10, Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629 (7th Cir. 2007) (No. 06-3817).
30. *Pisciotta*, 499 F.3d at 632.
31. *Id*.
32. *Id*.
33. *Id*.
34. *Id*.
35. *Id*.
36. *Id*. at 632-33.
37. *Id*. at 633. (citing Stollenwerk v. Tri-West Healthcare Alliance, 2005 WL 2465906 (D. Ariz. 2005); Guin v. Brazos Higher Educ. Serv., Inc., 2006 WL 288483 (D. Minn. 2006); Kahle v. Litton Loan Servicing LP, 486 F. Supp. 2d 705 (S.D. Ohio 2007); Forbes v. Wells Fargo Bank, 420 F. Supp. 2d 1018 (D. Minn. 2006)).
38. *Id*.
39. *Id*. at 634.

injury-in-fact requirement.[40] The Court of Appeals rejected this argument, instead adopting the view that the threat or increased threat of future harm sufficiently meets the injury-in-fact requirement.[41] The cases the court relied upon did not necessarily adopt the view that threats of future harm are compensable damages, but that they are sufficient to create injury-in-fact for standing purposes.[42]

Because the plaintiffs invoked diversity jurisdiction, the Court determined that it must apply substantive state law,[43] and more specifically, the Court must apply the law the way it believes the Indiana Supreme Court would apply the law.[44] Neither party identified any Indiana precedent that could be applied to the case, so the Court began its analysis with a recently enacted Indiana statute[45] pertaining to the subject-matter.[46] Specifically, the statute created responsibilities for private entities storing databases of personal information following a security breach.[47] The Act required the owner of a database that stores personal information to disclose the breach to the affected parties.[48] However, the statute did not obligate the database owner to take any further action.[49] The statute did not provide for a cause of action for the individual potentially affected by the security breach.

The plaintiffs argued that the passage of such a law recognizing the seriousness of compromising an individual's personal information indicates that the Indiana legislature considers a security breach to be a compensable injury.[50] However, the Court determined that the legislature would have made clear such an intent or recognized a private cause of action for those affected by the security breach, if that were the case.[51]

The plaintiffs argued that Indiana courts in the past have recognized the injury caused by the unauthorized access of personal information and presented two cases to support this position.[52] In the first case, *Indiana National Bank v. Chapman*,[53] a bank customer filed suit for breach of implied

---

40. *Id*.
41. *Id*.
42. *Id*.
43. Erie R.R. Co. v. Tompkins, 304 U.S. 64, 78 (1938).
44. *Pisciotta*, 499 F.3d at 635.
45. IND. CODE. ANN. § 24-4.9-3-1 (2009). The Court only used the statute as a reference, as the law had not become effective until after ONB's security breach.
46. *Pisciotta*, 499 F.3d at 636.
47. *Id*. at 637.
48. *Id*.
49. IND. CODE. ANN. § 24-4.9-3-1 (2009).
50. *Pisciotta*, 499 F.3d at 637.
51. *Id*.
52. *Id.* at 637-38.
53. Indiana Nat'l Bank v. Chapman, 482 N.E.2d 474 (Ind. Ct. App. 1985).

contract because the bank released the customer's personal information to a state policeman.[54] The appellate court determined that the bank was justified in releasing the information to a law enforcement official, but a bank impliedly contracts not to reveal personal information of its customer unless there is a public duty to do so.[55] Thus, the plaintiffs in the *Pisciotta* case correctly pointed to the fact that Indiana does recognize that bankers have a duty to prevent the unauthorized disclosure of their customers' personal information.[56]

The plaintiffs in the *Pisciotta* case also looked to *American Fletcher National Bank and Trust Co. v. Flick*.[57] In that case, the bank wrongfully dishonored a check by the customer who sought to recover for loss of credit and business standing.[58] The appellate court determined that wrongfully dishonoring a check creates a presumption that there will be harm to credit and business standing.[59] The court discussed the importance of a person's credit: "In the modern world the financial credit of a man is a much prized and valuable asset. Although laboriously built it is easily destroyed."[60] However, the court determined that only nominal damages would be appropriate given the lack of evidence.[61]

The court in *Pisciotta* rejected both cases presented by the plaintiffs as controlling authority regarding credit monitoring.[62] According to the court, the customers in *Indiana National Bank* and *American Fletcher National Bank* sought damages for present harm to their reputations.[63] The court determined that such an injury was a recoverable present harm, as opposed to an anticipated future harm sought in this case.[64]

The court considered the connection between compensable damages for medical monitoring and the award of damages sought by the plaintiffs for credit monitoring.[65] Following exposure to toxic substances, some jurisdictions allow recovery for the costs that will be incurred from monitoring the plaintiff's health due to the increased risk of health problems caused by the exposure.[66] The court did not specifically endorse the analogy, but

---

54. *Id.* at 476.
55. *Id*. at 482.
56. *Pisciotta*, 499 F.3d at 637-38.
57. Am. Fletcher Nat'l Bank & Trust Co. v. Flick, 252 N.E.2d 839 (Ind. Ct. App. 1969).
58. *Id*. at 840.
59. *Id*. at 845.
60. *Id*. (citing Weiner v. North Penn. Bank, Inc., 1916 WL 2998 at *3 (Pa. Super. Ct. 1916)).
61. *American Fletcher*, 252 N.E.2d at 846-47.
62. Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 638 (7th Cir. 2007).
63. *Id*.
64. *Id*.
65. *Id*. at 638-39.
66. *Id*. at 639.

acknowledged that it exists.[67] However, the court pointed out that Indiana is not among the jurisdictions that have allowed for recovery of medical monitoring.[68]

Finally, the court examined case law from other jurisdictions, including those cases relied upon by the district court when dismissing the case.[69] *Stollenwerk v. Tri-West Healthcare Alliance*[70] was the first decision regarding the recovery of credit monitoring costs. In that case, the plaintiffs sued Tri-West following a burglary in which computer systems containing their personal information were stolen.[71] The plaintiffs alleged that the defendant failed to adequately secure the premises, and sought recovery of money spent on credit monitoring services.[72] The court ultimately rejected the plaintiffs' claim for credit monitoring, but suggested that such a claim was possible, even stating the possible elements of such a claim.[73] The court recognized the analogy between credit monitoring and medical monitoring, but determined that they are distinguishable given the importance of health at risk in medical monitoring cases.[74] In the end, the plaintiffs' claim for credit monitoring was denied for failure to demonstrate a sufficient injury.[75]

Guin v. Brazos Higher Educ. Serv., Inc.[76] was determined by analyzing individually the general elements of a cause of action for negligence.[77] In that case, the plaintiff sued the defendant corporation for negligently allowing an employee to keep confidential information on a laptop, which was stolen.[78] The defendant conceded that, as a holder of personal information, there was a duty to adequately safeguard sensitive personal information.[79] However, the court determined that the defendant had exercised reasonable care and sufficiently protected the personal information.[80] The court also determined

---

67. *Id*.
68. *Id*.
69. Stollenwerk v. Tri-West Healthcare Alliance, 2005 WL 2465906 (D. Ariz. 2005); Guin v. Brazos Higher Educ. Serv., Inc., 2006 WL 288483 (D. Minn. 2006); Kahle v. Litton Loan Serv. LP, 486 F. Supp. 2d 705 (S.D. Ohio 2007); Forbes v. Wells Fargo Bank, 420 F. Supp. 2d 1018 (D. Minn. 2006).
70. Stollenwerk v. Tri-West Healthcare Alliance, 2005 WL 2465906 (D. Ariz. 2005).
71. *Id*. at *1.
72. *Id*.
73. *Id*. at *4.
74. *Id*.
75. *Id*.
76. Guin v. Brazos Higher Educ. Serv., Inc., 2006 WL 288483 (D. Minn. 2006).
77. A claim for negligence typically requires the plaintiff to prove four elements: 1) the defendant owed the plaintiff a duty of care; 2) that duty was breached by the defendant; 3) the breach caused an injury to the plaintiff; and 4) the breach was the proximate cause of the plaintiff's injury. *Id*. at *3.
78. *Guin*, 2006 WL 288483 at *1.
79. *Id*. at *3.
80. *Id*. at *4.

that the plaintiff had failed to demonstrate a recoverable injury, thus rejecting the notion of recovery for future harm not yet materialized.[81] Finally, the court stated that the general rule in negligence cases was that an intervening criminal act "break[s] the chain of causation."[82] In the end, the court concluded that the mere exposure of sensitive personal information does not create a cause of action.[83]

Similarly, the court in *Forbes v. Wells Fargo Bank*[84] also rejected the costs of credit monitoring as recoverable damages.[85] In *Forbes*, several bank customers sued Wells Fargo Bank when computers were stolen containing their personal information.[86] The decision was mainly based on the plaintiffs' failure to prove injury.[87] As the court stated, the money spent on credit monitoring was not recoverable because "[plaintiffs'] expenditure of time and money was not the result of any present injury, but rather the anticipation of future injury that has not yet materialized."[88] The court refused to deviate from the general rule that risk of future harm alone is not sufficient to constitute a cognizable injury and rejected the notion that money spent to monitor one's credit is itself an injury.

In *Kahle v. Litton Loan Servicing LP*,[89] the plaintiff sued her mortgage loan company when computer equipment was stolen containing her personal information.[90] The *Kahle* court relied on prior cases, such as *Stollenwerk*, *Forbes*, and *Guin*, to determine that the plaintiffs did not suffer a cognizable injury until the personal information was actually used to commit consumer fraud.[91] The decision was based mainly on past precedent without much in the way of an independent analysis of the issues.

The *Pisciotta* court concluded that even though the district court cases were not exactly factually identical, the courts that have addressed the credit monitoring issue took the position that a customer whose personal information has been exposed, but had not yet been used fraudulently, had not suffered a

81. *Id*. at *5-6.
82. *Id*. at *6 (citing Funchness v. Cecil Newman Corp., 632 N.W.2d 666, 674 (Minn. 2001)).
83. *Guin*, 2006 WL 288483.
84. Forbes v. Wells Fargo Bank,420 F.Supp.2d 1018 (D. Minn. 2006).
85. *Id*.
86. *Id*. at 1019.
87. *Id*. at 1020.
88. *Id*. at 1021.
89. Kahle v. Litton Loan Servicing LP, 486 F.Supp.2d 705 (S.D. Ohio 2007).
90. *Id*. at 706.
91. *Id*.

recoverable injury.[92] The court also considered another federal district court case, *Hendricks v. DSW Shoe Warehouse, Inc.*,[93] which did not rely on the prior decisions regarding security breaches of personal information, but instead determined that recovery would not be permitted because no statutes or cases within the state have allowed recovery for such an injury.[94] Similarly situated, the Seventh Circuit was also hesitant to impose liability absent state law. Finding the federal district court cases compelling, the court strengthened the stance against allowing recovery for consumers following a security breach, leaving them with only the option of waiting until identity theft occurs before granting any relief.[95]

IV. ANALYSIS

The general rule is that recovery is not allowed for damages which are speculative or uncertain.[96] Given the uncertainty of whether the exposure of personal information will eventually lead to consumer fraud, courts have been reluctant to allow plaintiffs to recover until the harm actually occurs. State legislatures have also been reluctant to impose costs on businesses following a security breach, generally only requiring that the business disclose the breach to the customers.[97] Future plaintiffs, therefore, do not have favorable precedent to rely upon thus far. In fact, the lack of statutory authority and limited case law on the issue of recovery for security breaches absent consumer fraud does not leave courts with much controlling law on the subject. However, potential identity theft victims can continue to pursue their claims, despite the lack of favorable precedent, by making compelling policy arguments and comparing their claims to those of medical monitoring plaintiffs.

A. *Stollenwerk v. Tri-West Healthcare Alliance*

The Seventh Circuit examined the leading cases regarding credit monitoring, all of which denied recovery, and the decision was consistent with

---

92. Pisciotta v. Old Nat'l Bancorp, 489 F.3d 629, 639 (7th Cir. 2007) *(discussing* Stollenwerk v. Tri-West Healthcare Alliance, 2005 WL 2465906 (D. Ariz. 2005); Guin v. Brazos Higher Educ. Serv., Inc., 2006 WL 288483 (D. Minn. 2006); Kahle v.`Litton Loan Servicing LP, 486 F.Supp.2d 705 (S.D. Ohio 2007)).

93. Hendricks v. DSW Shoe Warehouse, Inc., 444 F.Supp.2d 775 (W.D. Mich. 2006).

94. *Id.*

95. *Pisciotta*, 499 F.3d at 640.

96. Salaban v. East St. Louis & Interurban Water Co., 1 N.E.2d 731, 733 (Ill. App. Ct. 1936).

97. *See, e.g.*, IND. CODE. ANN. § 24-4.9-3-1 (2009).

those cases. However, most credit monitoring cases rely on *Stollenwerk* to deny recovery for credit monitoring, which might be a misapplication of the principles articulated in the case. A closer reading of *Stollenwerk* suggests that the decision may not have been intended to establish a blockade to the plaintiff's road to recovery for credit monitoring, but instead to point such plaintiffs in the right direction.

In *Stollenwerk*, defendant Tri-West was an agent of the federal government that managed the local health insurance program.[98] The computer systems contained the personal information of the beneficiaries of the program, including the plaintiffs.[99] When the premises was burglarized, the defendant's computer hard drives were stolen.[100] Plaintiffs sued Tri-West for negligence, seeking recovery of money spent on credit monitoring services.[101] Although the *Stollenwerk* court ultimately denied the plaintiffs' claim for credit monitoring, the decision does not seem to suggest that a credit monitoring claim would never be possible. On the contrary, the court even articulated the elements of such a cause of action, which closely resemble those of a medical monitoring claim. Determining that "the Court is not convinced that the negligent exposure of confidential personal information is entirely dissimilar from negligent exposure to toxic substances or unsafe products,"[102] the court articulated the following elements for establishing a claim for credit monitoring: 1) exposure of confidential personal information; 2) increased risk of identity theft because of that exposure; and 3) the need and effectiveness for credit monitoring to prevent identity theft.[103] Although the court granted summary judgment for the defendant because the plaintiffs did not establish that a sufficient injury had occurred, the court concluded that recovery may be possible if the potential plaintiff could establish the elements that the court articulated.[104]

Thus, the decision in *Stollenwerk* alludes to the fact that recovery of the costs of credit monitoring is possible, if the plaintiff can provide the court with sufficient reasons of why it would be an appropriate remedy. The decisions after *Stollenwerk*, including *Pisciotta*, follow that court's decision not to allow recovery for credit monitoring, but perhaps ignore the real importance of the case, which is the suggestion that credit monitoring should be permissible if the plaintiff can make the requisite showings.

---

98. *Stollenwerk*, 2005 WL 2465906 at *1.
99. *Id*.
100. *Id*.
101. *Id*.
102. *Id*. at *3.
103. *Id*. at *4.
104. *Id*.

B. Medical Monitoring

Credit monitoring is very similar to what is known as medical monitoring,[105] which is recognized in many jurisdictions as either an element of damages or an independent cause of action.[106] Medical monitoring is a claim in which the plaintiff seeks recovery for the costs of regularly administered medical exams to prevent against latent diseases caused by exposure to toxic substances known to cause medical problems.[107] "Medical monitoring is one of a growing number of non-traditional torts that have developed in the common law to compensate plaintiffs who have been exposed to various toxic substances."[108] Medical monitoring is non-traditional in that the physical injury caused by the exposure is latent, whereas traditional tort claims require a present, actual injury.[109] However, the court in *Paoli* clarified that the injury in medical monitoring claims is the cost of medical examinations to protect against those possible latent diseases.[110] Similarly, the injury in a credit monitoring claim would be the cost of credit monitoring service to guard against identity theft.

Although some jurisdictions do not even consider medical monitoring absent a present physical injury, there are a number of jurisdictions that do recognize medical monitoring as a cause of action or as an element of damages despite there being no present physical injury.[111] There are variations on the elements of the cause of action, but the basic elements of a medical monitoring claim were articulated in *Paoli Railroad*:

1. Plaintiff was significantly exposed to a proven hazardous substance through the negligent actions of the defendant.
2. As a proximate result of exposure, plaintiff suffers a significantly increased risk of contracting a serious latent disease.

---

105. *See generally*, Vincent R. Johnson, *Cybersecurity, Identity Theft, and the Limits of Tort Liability*, 57 SCLR 255, 307-308 (2005).
106. *See generally*, Joseph K. Hetrick & Allison M. Brown, *Cause of Action for Medical Monitoring Relating to the Use of Medical Devices and Prescription Drugs*, 34 COA2D 249, §§ 8-9 (2007).
107. *In re* Paoli R.R. Yard PCB Litig., 916 F.2d 829, 849 (3rd Cir. 1990).
108. *Id*.
109. *Id*. at 850.
110. *Id*. at 849.
111. Jurisdictions that recognize medical monitoring absent a present physical injury include: Arizona, California, Colorado, Connecticut, District of Columbia, Florida, Illinois, New Jersey, New York, Ohio, Pennsylvania, Utah, and West Virginia.

3. That increased risk makes periodic diagnostic medical examinations reasonably necessary.
4. Monitoring and testing procedures exist which make the early detection and treatment of the disease possible and beneficial.[112]

Additionally, some states require the plaintiffs to prove that the medical monitoring they seek differs from the medical testing that they would receive otherwise.[113] Recovery is not permissible for medical examinations in which the average person should submit to anyway, such as regular checkups.[114]

Plaintiffs pursing a claim for credit monitoring might find it difficult to show that the credit monitoring program they seek differs from what the average person should use. Consumers would be well-advised to regularly check the status of their credit report, and a credit monitoring service would be a good investment for anyone, especially those who conduct business online. It seems unlikely that the average person would spend money for preventative credit monitoring unless they believed that they were at an increased risk of identity theft, but it is unclear how many people actually pay for credit monitoring services and more research would be needed to determine this element.

Despite the failure of past plaintiffs to prove a cause of action for credit monitoring, there is still hope for future claims. The elements of a possible cause of action have been identified,[115] so there is a chance that future plaintiffs will be able to prove their claims. And, given the similarities between medical monitoring and credit monitoring, courts might be persuaded by some of the same policy arguments that have succeeded for medical monitoring claims.

C. Policy Concerns

Because Indiana does not allow recovery for medical monitoring,[116] it is logical that the court determined that allowing recovery for credit monitoring would be inconsistent with state law. Even though the *Pisciotta* decision is reasonable given the limited prior case law, there are several policy considerations that outweigh the concerns addressed by the courts regarding credit monitoring. There are a number of issues that could be troubling the

---

112. *Paoli*, 916 F.2d at 852.
113. Hetrick & Brown, *supra* note 106, at § 15.
114. Potter v. Firestone Tire & Rubber Co., 863 P.2d 795, 835 (Cal. 1993).
115. *Stollenwerk*, 2005 WL 2465906 at *4.
116. *See*, AlliedSignal, Inc. v. Ott, 785 N.E.2d 1068 (Ind. 2003).

courts, many of which are analogous to the concerns regarding medical monitoring.

One of the potential concerns is that allowing recovery for credit monitoring would open the door to too many potential plaintiffs. As online services become increasingly popular, there are more and more people who chose to conduct business over the Internet. Theoretically, if more people entrust their personal information into the hands of online businesses, each security breach will result in more affected consumers. By allowing recovery for nothing more than a security breach, every consumer following a security breach could become a potential plaintiff. However, recognizing a new cause of action does not necessarily lead to excessive litigation, because not every claim will be successful. When faced with this argument against allowing medical monitoring, the court in *Miranda v. Shell Oil Co.*[117] stated that allowing recovery "does not sweep away the burdens imposed on a plaintiff to prove each of the elements of his or her cause of action."[118]

Another possible concern is that the plaintiffs will not spend the money as it was intended. In *Ayers v. Jackson*,[119] the court upheld a lump sum award of damages for medical monitoring, wishing to leave the jury verdict undisturbed.[120] But, an informal survey of the plaintiffs following the judgment had some disturbing results. Out of the three people who responded, one bought a house and never saw a doctor again, and the other two did not see their doctors any more than usual.[121] However, this problem could be avoided by creating a court-administered fund, as opposed to a lump sum payment. The use of a court-administered fund was supported in *Ayers*, even concluding that a court-administered fund should be the general rule regarding medical monitoring awards.[122] A court-administered fund would eliminate the concern that plaintiffs would not use the money as it was intended. Also, "a [court-administered] fund would serve to limit the liability of the defendants to the amount of expenses actually incurred [by the plaintiff]."[123]

Additionally, courts may be concerned that awarding the costs of credit monitoring would be too speculative. If, for example, a plaintiff whose information is wrongfully accessed never actually becomes a victim of identity theft, the defendant would have paid damages for an injury that never occurred. The same issue has been addressed by the court in *Ayers* regarding

---

117. Miranda v. Shell Oil Co., 17 Cal. App. 4th 1651 (Cal. Ct. App. 1993).
118. *Id.* at 1660.
119. Ayers v. Jackson Tp., 525 A.2d 287 (N.J. 1987).
120. *Id.* at 315.
121. Hetrick & Brown, *supra* note 106, § 21, at 285.
122. *Ayers*, 525 A.2d. at 314.
123. *Id.*

the costs of medical monitoring. The court determined that "[t]he invasion for which redress is sought is the fact that plaintiffs have been advised to spend money for medical tests, a cost they would not have incurred absent their exposure to toxic chemicals."[124] Likewise, plaintiffs would not likely spend money on credit monitoring if they were not concerned about consumer fraud and identity theft as a result of the defendant's failure to safeguard their personal information. If the costs of credit monitoring are merely reimbursed through a court-administered fund, the defendant will only be paying for money actually spent on credit monitoring. The damages then would be easily calculated and not speculative at all.

Finally, there is likely a concern that paying credit monitoring costs for every customer whose information is compromised would create economic hardships on the defendants. In regards to medical monitoring, the U.S. Supreme Court in *Metro-North Commuter R.R. Co. v. Buckley*[125] feared that this would be a "costly" remedy and could use up financial resources that could be used for the severely injured.[126] This is certainly a possibility. A recent study by ID Analytics, Inc. analyzed four large data breaches,[127] two of which were identity-level breaches.[128] Of the two identity-level breaches, the misuse rate was about 1 in 1,000.[129] If the business can only be required to pay for the loss of that one person whose information is misused, it is possible that the business will spend less money than paying credit monitoring for all 1,000. Of course, this would all depend on the damages awarded to identity theft victims. In *Murray v. Bank of America*, the plaintiff was arrested in front of her son, spent 12 hours in jail, and was required to appear in court when she became a victim of identity theft due to the bank's negligence.[130] The jury awarded her $300,000.[131] Assuming ID Analytics' study is accurate regarding the misuse rate following a data breach, a business could pay for credit monitoring for all 1,000 consumers at a rate of $100 for three years for potentially the same cost of paying damages to one and avoid the hassles of litigation. Given the speed that identity thieves must work to avoid being

124. *Id.* at 304.
125. Metro-North Commuter R.R. Co. v. Buckley, 521 U.S. 424 (1997).
126. *Id*. at 442.
127. ID Analytics, Inc., National Data Breach Analysis Frequently Asked Questions, http://www.idanalytics.com/assets/pdf/National_DataBreach_FAQ.pdf (last visited Mar. 19, 2009). ID Analytics, Inc. specializes in identity risk management.
128. Identity-level breaches contain the most personally-identifiable information, such as names, addresses, and social security numbers. *Id.*
129. ID Analytics, *supra* note 127.
130. Murray v. Bank of Am., 580 S.E.2d 194, 197 (S.C. Ct. App. 2003).
131. *Id*.

caught, credit monitoring for even a few years would probably be sufficient to protect consumers.

Of course, the results of ID Analytics' study are not representative, given the small sample size. In fact, ID Analytics concluded that the misuse rate could increase drastically if the market for this information is allowed to become more efficient and organized, and that more research needs to be done in this area.[132] The lack of research about data breaches makes it difficult to determine conclusively whether paying credit monitoring costs for all consumers following a breach would actually cost or save the business money in the long run. Businesses are in the best position, as compared to the consumer, to conduct research and gather statistics, so perhaps the burden should shift to them to prove that credit monitoring would be a costly remedy.

There is reason to believe that a business would actually benefit from providing credit monitoring services following a security breach. First of all, credit monitoring services are relatively inexpensive. For example, Lifelock is a credit monitoring service that takes several preventative measures to guard against identity theft.[133] The service provided costs approximately $100 per year, and Lifelock guarantees its services, by insuring the consumer against identity theft for up to one million dollars.[134] Thus, businesses could be assured that by paying a small fee per consumer, they will not be required to pay a large amount in the future if any of the consumers become identity theft victims or spend time litigating over their liability.

Another way for a business to benefit from paying credit monitoring would be to pass the additional costs on to the consumers. If, for example, the business adds a small additional fee for using online services, the money can be set aside to pay future credit monitoring costs, if necessary. If sensitive information is compromised, the company can use the funds acquired from this additional fee to pay the expenses of credit monitoring. If a security breach does not occur, the business has additional profits. As an added bonus, the business gains credibility for attending to the needs of the consumers by protecting their credit on their own accord.

---

132. ID Analytics, *supra* note 127.

133. Lifelock, http://www.lifelock.com (last visited Mar. 19, 2009).

134. Lifelock, http://www.lifelock.com/our-guarantee?aplisting=2 (last visited Mar. 19, 2009).

D. Additional Reasons to Reconsider

When justifying medical monitoring, the court in *Redland Soccer Club, Inc. v. Dept. of the Army and Dept. of Defense of the U.S.*[135] determined that there were several important reasons for allowing the cause of action, including promoting early detection, deterrence, and preventing injustice.[136] If businesses were required to pay for credit monitoring services, these same policy concerns would be addressed. By providing credit monitoring, identity theft would be prevented before it occurs. According to statistical information, 70% of identity theft victims spent up to one year trying to reverse the effects of identity theft,[137] and the average loss for each victim was over $3,000.[138] In addition to the direct monetary loss and time spent trying to recover for such loss, there are additional secondary effects of identity theft, including emotional distress, harm to reputation, privacy concerns, and other noneconomic costs. In a 2007 survey, 53% of victims have reported continuing calls from collection agencies, 27% have had their credit cards canceled, and 18% reported effects on their ability to find employment.[139] Therefore, it is clearly in the best interest of both the business and the consumer that the injury is prevented before it occurs rather than trying to compensate the plaintiff after the fact, given the irreversible harm that can result from identity theft. Providing a credit monitoring service that fosters early detection of attempted identity theft will not only save the business from the potentially overwhelming costs of consumer fraud, but it will also save the potential victim from emotional distress, ruined credit, inability to acquire loans, embarrassment, and other serious concerns.

Imposing liability on companies who fail to adequately safeguard their customer's personal information would deter carelessness and provide an incentive to ensure sufficient protection of sensitive information. Businesses are more likely to carefully defend against security breaches if they must incur the expense of failing to guard against such risks. Furthermore, the business is in the best position to guard against such risks as compared to the consumer. Money talks, and when it does, most businesses will listen. Thus, if companies are held responsible for failure to properly safeguard their

135. Redland Soccer Club, Inc. v. Dep't of the Army and Dep't of Def. of the U.S., 548 Pa. 178 (Pa. 1997).
136. *Id*. at 194.
137. ITRC, *supra* note 10.
138. Gartner, *supra* note 2.
139. *Id*.

customer's personal information, they will most likely take every step necessary to ensure that security breaches do not occur.

Finally, forcing the businesses to pay credit monitoring fees would prevent the injustice of requiring the economically disadvantaged consumer from paying fees caused by the defendant's negligence.[140] Every citizen is entitled to a free yearly credit report from the major credit reporting companies: Equifax, Experian, and TransUnion.[141] The consumer also has the option to place a fraud alert on their credit file, after which the creditor should contact the consumer before opening a new account.[142] Even if a consumer is aware of this option, the fraud alert lasts only 90 days and creditors sometimes ignore them.[143] However, the costs of a preventative service, such as Lifelock, could be too costly for the economically disadvantaged consumer, whereas the cost would be nominal to a business. As the court in *Ayers* suggested, while some individuals will seek monitoring regardless of whether the costs will be refunded, others may be deterred from seeking such services if they know that they will not be reimbursed.[144] In all fairness, businesses should consider paying credit monitoring fees following a security breach with or without a court order.

V. CONCLUSION

Although a person's credit score is not as important as his or her health and well-being, the numerous problems that stem from identity theft and consumer fraud caused by the failure to adequately safeguard personal information should persuade the courts to consider what is in the best interest for society. As a matter of public policy, businesses that store personal information should be required to front the costs of credit monitoring following a security breach. Some courts have determined that creating a new cause of action for credit monitoring is a job best left to the legislature.[145] Consumers would certainly welcome such legislation, but they have no other choice but to turn to the court when the legislature is not acting on their behalf.

---

140. *Redland*, 548 Pa. at 194.
141. AnnualCreditReport.com, http://www.annualcreditreport.com (last visited Mar. 19, 2009). *See*, 15 U.S.C. §1681j(a)(1)(a) (2009).
142. Fight Identity Theft, http://www.fightidentitytheft.com/flag.html (last visited Mar. 19, 2009).
143. *Id*.
144. Ayers v. Jackson Tp., 106 N.J. 557, 604 (N.J. 1987).
145. *See e.g.* Badillo v. Am. Brands, Inc., 117 Nev. 34, 40-41 (Nev. 2001).