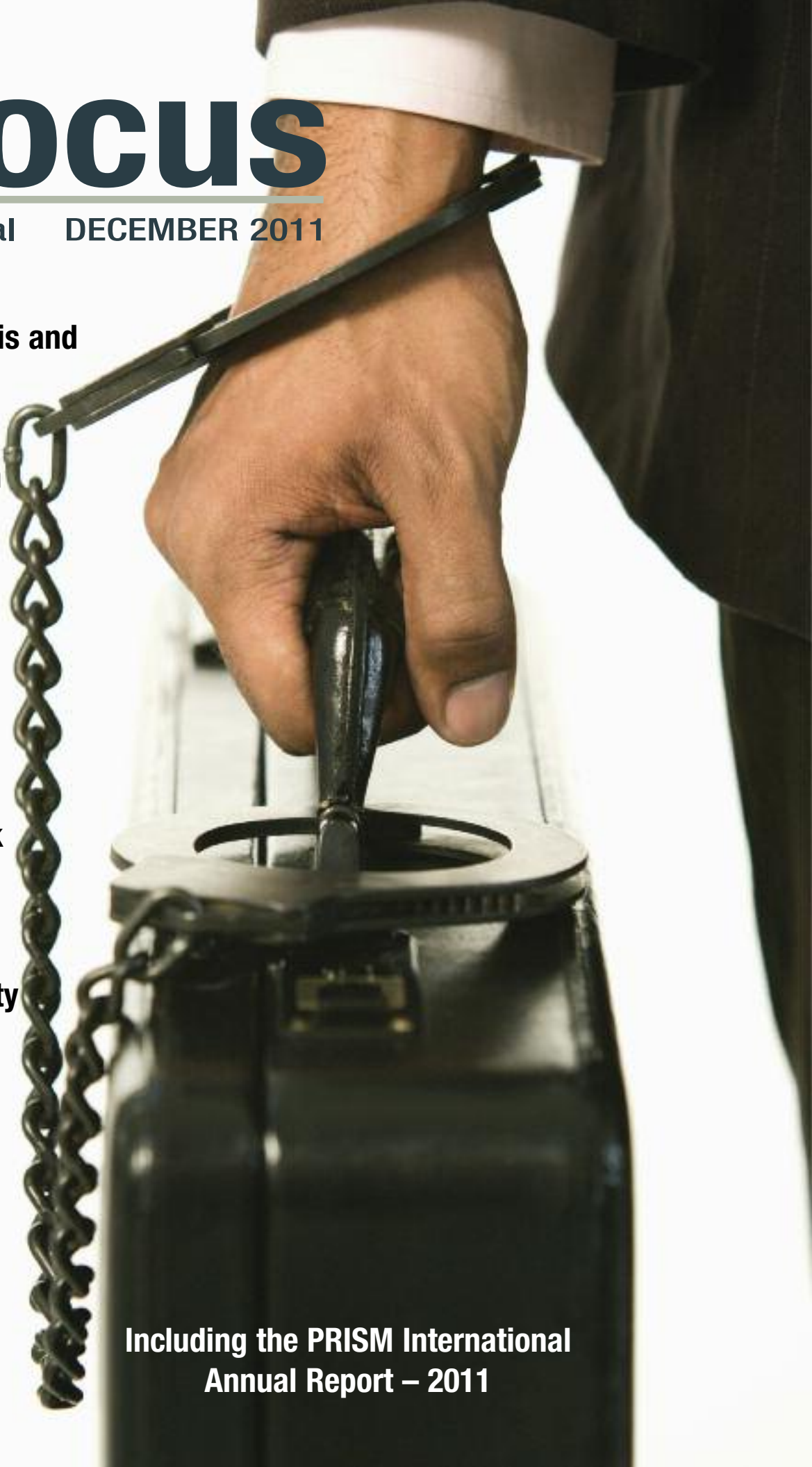
inFocus

Quarterly Journal DECEMBER 2011



Wikileaks, Tsunamis and Revolutions

Data Security Breach Notification Requirements in the United States: What You Need to Know

Data Breaches and Litigation: It's the American Way

Insurance and Risk Management for Breach of Data Privacy and Information Security

Including the PRISM International Annual Report – 2011

Data Breaches and Litigation: IT'S THE AMERICAN WAY

Larry L. Varn, Esq.[1]

I. Introduction

According to Gartner, Inc., a Stamford, Connecticut-based information technology research and advisory firm, approximately 7.5 per cent of adults in the United States lost money as a result of some sort of financial fraud in 2008, in large part because of data breaches.[2] The non-profit Privacy Rights Clearing-house has reported that between April 2005 and November, 2011, more than 542 million records have been breached or compromised from 2,761 data breaches that were made public. Data breaches have involved financial information such as banking or credit card details, personally identifiable information such as names, addresses and social security numbers (PII), personal health information (PHI), trade secrets or intellectual property of businesses, or confidential government information. Data breaches have resulted from inadvertent or accidental incidents, such as the loss or theft (for other purposes) of digital or hardcopy media, including laptops, computer tapes, hard drives, flash drives and medical or financial records, sophistical criminal activities commonly known as "hacking", the inadvertent transfer of information to individuals or entities who are not authorized to receive or view it, or the deliberate transfer of such information to a potentially adverse party, such as a competing business or foreign nation.

Well-publicized incidents are now legion, and include:

- In April 2011, Sony announced a massive data breach arising from theft by hackers of the Sony Playstation® Network, Sony Entertainment Online and Sony Pictures resulting in the compromise of the credit and debit card data of up to 100 million users involving more than 12 million cards. Sony estimated that breach remediation measures alone would cost it at least $171 million, and no fewer than 55 putative class actions were filed against Sony in the United States and another three such actions were filed in Canada.[3]
- In January 2009, Heartland Payment Systems announced that it had been the victim of a criminal security breach, possibly as part of a "global cyber fraud operation". Estimates were made that up to 100 million cards from more than 650 financial services institutions were compromised.
- In March 2008, Hannaford Brothers Co., a national grocery chain based in Maine, announced that the security of its information technology (IT) systems had been breached, leading to the theft of as many as 4.2 million debit card and credit card numbers belonging to individuals who had made purchases at more than 270 of its stores. Hannaford also announced that it had already received reports of approximately 1,800 cases of fraud resulting from the theft of those numbers, with authorized charges originating around the globe, including Spain and France. Twenty-six (26) separate lawsuits followed which were consolidated in federal court in Maine.
- In January 2007, TJX Companies, Inc., a retailer operating major chains such as TJ Maxx and Marshalls, announced the theft by hacking of more than 45 million individual records from its computer system. The scheme ultimately led to criminal charges against 11 individuals and resulted in several class action lawsuits.

II. A "Burgeoning Area" of Litigation

Given these statistics and events – not to mention thousands of other less-publicized incidents – it should come as no surprise that data breaches have led to multitudinous, complex and expensive litigations, many in the form of putative class actions. I am sure that the celebrated and respected English jurist Lord Denning would have predicted cases of this type when he remarked nearly 30 years ago: "As a moth

[1] The author is a litigation partner at Pierce Atwood LLP, a leading regional law firm with offices in Boston, MA, Portland and Augusta, ME, Portsmouth, NH, Providence, RI, Washington, DC, and Stockholm, Sweden, and has over 25 years of experience in complex corporate litigation, crisis management and litigation advisory services.

[2] See www.gartner.com/it/page.jsp?id=906312. Gartner surveyed nearly 5,000 U.S. adults in September 2008 and reported that payment card fraud, that is to say, credit, debit and ATM card fraud, was the method most actively used by crooks to steal money. Unfortunately, conviction rates are quite low, as less than one-third of victims reported the crimes to law enforcement and only about 5 per cent reported them to the Federal Trade Commission. Accordingly, the chances of a criminal getting arrested and convicted for identity-theft related fraud are less than one half of one per cent. Additional information is available in the Gartner report "2008 Data Breaches and Financial Crimes Scare Consumers Away", which may be found at http://www.gartner.com/ DisplayDocument?ref=g_search&id=902212@subref=simplesearch.

[3] *See J. Jean and R. Wrightson*, Outside Counsel: Insurance for Information Stolen in Security Breaches, *New York Law Journal* v. 246, No. 77 (Oct. 20, 2011). Although beyond the scope of this article, it is noteworthy that the Sony data breach, perhaps one of the largest since records have been kept, has also resulted in litigation between Sony and the issuer of its commercial general liability (CGL) primary and excess policies over coverage for Sony's insurance claim. *See id.; see also Zurich American Insurance Company, et al. v. Sony Corporation of America, et al.*, Complaint for Declaratory Judgment (Sup. Ct. of N.Y., N.Y. County, July 20, 2011). Sony was not alone in reporting massive data breaches in 2011. Many well-known institutions, including NASDAQ, Epsilon, Dropbox and even the Pentagon, reported substantial data breaches, both accidental and criminal, leading some commentators to label 2011 "The Year of the Breach". See K. Vasiloff and C. Phan, 2011 – *The Year of the Breach*, Insurance Law 360 (Aug. 8, 2011).

is drawn to the light, so is a litigant drawn to the United States. If he can only get his case into their courts, he stands to win a fortune."[4] These claims are thus part of what one judge has dubbed a "burgeoning area of law"[5] and another has explained:

> Database breaches appear to provide the basis for a new breed of lawsuits, and especially class action lawsuits, in which plaintiffs allege, as here, that the database handlers' negligence in developing and maintaining security measures have resulted in otherwise personal and confidential information being compromised, thereby increasing the risk of identity theft for those individuals whose information was so compromised. The remedies sought in these actions vary, but generally include costs for credit monitoring, costs for closing and opening financial accounts, and damaged for emotional distress.[6]

In addition to being a new area of law, claims arising from data security breaches are almost always brought in federal court.[7] To date, however, although the response and remediation costs resulting from data breaches can be very substantial, and the media scrutiny can be unforgiving, the ensuing lawsuits by affected (or potentially affected) consumers have fared very poorly, particularly in those cases where the plaintiffs cannot establish any actual misuse of information or any actual, quantifiable monetary damages but claim only such items as "an increased risk of harm", anxiety, increased apprehension and general aggravation. It is only in those cases where plaintiffs have been able to establish actual, fraudulent misuse of the compromised information that they have had any meaningful success in recovering their actual, provable damages, or where they have incurred actual costs or expenses in response to a credible threat of identity theft.

In determining whether to allow a claim in this area – generally grounded in theories of negligence or breach of express or implied contract – to go forward, our federal courts are required to answer two questions. First, do these claims involve a sufficient injury-in-fact to confer standing to sue in federal court under Article III of the United States Constitution? It is only if this question is answered in the affirmative that the court must then ask: do these claims involve compensable damages under the governing state's law? [8]

[4] *Smith Kline & French Labs Ltd. V. Bloch*, 1 W.L.R. 730 (C.A. 1982).

[5] *Allison v. Aetna*, 2010 WL 3719243, *4 (E.D. Pa. Mar. 9, 2010).

[6] *Amburgy v. Express Scripts, Inc*., 2009 wl 4067218, AT *1 (E.D. Mo. Nov. 23, 2009).

[7] One federal judge noted that: "[A]ll or nearly all of the precedent bearing on Plaintiffs' novel [data security] claims comes from federal courts interpreting state law. This court assumes that this is so because claims like Plaintiffs' are typically brought on behalf of a putative class, and the Class Action Fairness Act diverts most such cases to federal courts. *Krottner v. Starbucks Corp*., 2009 WL 7382290, *7 (W.D. Wash. Aug. 14, 2009).

[8] *Pisciotta v. Old National Bancorp*, 499 F.3rd 620 (7th Cir. 2007).

III. "Standing" Under Article III of the U.S. Constitution

Article III, Section 2 of the Constitution "limits the federal judicial power to the resolution of 'cases and controversies'". One well-settled element of the "case or controversy"[9] requirement is that a plaintiff must establish "standing" to sue, as to which the Supreme Court has held that "the 'irreducible constitutional minimum' of standing under Article III requires a plaintiff to establish three elements an injury in fact..., a causal connection between the injury and the conduct complained of, and substantial likelihood of remedy".[10] The first requirement – injury in fact – has been defined by our federal courts as "an invasion of a legally protected interest that is (a) concrete and particularized, and (b) actual or imminent, *not conjectural or hypothetical*."[11]

At least until and through a part of 2007, federal district courts consistently held that plaintiffs lacked standing under Article III to bring negligence or breach of contract claims as a result of the compromise of personal information and thus routinely dismissed those cases in their early stages.[12] However, later that year the United States Court of Appeals for the Seventh Circuit, which covers the states of Illinois, Wisconsin and Indiana, sparked at least a partial shift in the approach of the federal judiciary to the standing question. The case was *Pisciotta v. Old National Bancorp*,[13] and it arose out of claims that a non-party computer "hacker" was able to obtain access to the confidential information of "tens of thousands" of Old National site users. Notably, plaintiffs did not allege that anyone had been an actual victim of identity theft. Nevertheless, while noting that federal courts up to thatpoint had found no standing in situations, the Court of Appeals for the Seventh Circuit wrote that:

> We are not persuaded by the reasoning of these cases. As many ofour sister circuits have noted, the injury-in-fact requirement can 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. We concur in this view. Once the plaintiffs' allegations establish at least this level of injury, the fact that the plaintiffs anticipate that some greater potential harm might follow the defendant's act does not affect the standing inquiry.[14]

Accordingly, the Seventh Circuit found that the *Pisciotta* plaintiffs satisfied the constitutional requirement of standing to bring their claims in federal court, thus signaling a shift, albeit a very modest one, from the previous decisions on the subject.

Since *Pisciotta*, the federal courts in data breach cases have split on the thorny issue of standing to sue. On one side of the issue, in *Amburgy v. Express Scripts, Inc*.,[15] decided by a federal court in Missouri in 2009, the plaintiff, who alleged that inadequate security allowed unauthorized individuals to access a database containing personal information and threatened to publicize it if the defendant did not pay them a certain amount of money, was found to lack standing under Article III. Similarly, in *Hinton v. Heartland Payment Systems, Inc*.,[16] decided by a federal court in New Jersey the same year, the court held that the plaintiff, who claimed that his credit information was compromised in an electronic data breach but who did not allege any actual misuse, lacked standing because he had not alleged an actual injury-in-fact.[17] More recently, a federal district court in New York City, in dismissing a data breach case for lack of standing, stated that "Plaintiffs lack standing because their claims are future-oriented, hypothetical, and conjectural. There is no "case or controversy."[18]

On the other hand, several lower federal courts have followed the logic and holding of Pisciotta and declined to dismiss cases arising out of data breaches solely on standing grounds. For example, in *McLoughlin v. People's United Bank, Inc*.,[19] decided by a federal court in Connecticut, the court held that the plaintiff, who claimed that unencrypted backup tapes containing her PII and personal financial information that were managed by Bank of New York Mellon were either lost or stolen but did not allege actual misuse of her information, nevertheless had standing to *pursue her claims. Similarly, in Caudle v. Towers, Perrin, Forster & Crosby, Inc*.,[20] a New York federal court held that plaintiff, who alleged that a laptop containing his personal information was

9 *Interfaith Cmty. Org. v. Honeywell Int'l., Inc*., 399 F.3rd 248, 254 (3rd Cir. 2005).

10 *Pa. Prison Society v. Cortes*, 508 F.2rd 156, 160-61 (3rd Cir. 2007), citing Lujan v. Defenders of Wildlife, 504 U.S. 555, 560-61 (1992).

11 *Danvers Motor Co. v. Ford Motor Co*., 432 F.3rd 286, 290-91 (3rd Cir. 1005)(emphasis added).

12 *See, e.g., Randolph v. ING Life Ins. and Annuity Co*., 486 F. Supp. 2d 1, 4, 7-8 (D.D.C. 2007) (plaintiff, who alleged that a laptop containing her personal information was stolen but did not allege any misuse, lacked standing under Article III); *Bell v. Acxiom, Corp*., 2006 WL 2850042, at *1 (E.D. Ark. Oct. 3, 2006) (plaintiff, who alleged that a database containing her personal information was compromised and that information was illegally sold to a marketing company, lacked standing under Article III); *Key v. DSW, Inc*., 454 F. Supp. 2d 684, 685-686, 690 (S.D. Ohio 2006) (plaintiff, who alleged that her information had been accessed by an unauthorized individual but did not allege misuse, lacked standing under Article III); *Giordano v. Wachovia Sec., LLC*, 2006 WL 2177036, at *4-5 (D.N.J. July 31, 2006) (plaintiff, who claimed that defendant lost hardcopy of her personal information but did not allege that information was stolen or in the possession of someone who might misuse it, lacked standing under Article III). One exception, albeit a small one, to this seemingly unbroken line of anti-plaintiff decisions was *Stollenwerk v. Tri-West Healthcare Alliance*, 254 Fed. Appx. 664 (9th Cir. 2007). *Stollenwerk* arose from the theft of computer servers with customer's personal information during a burglary. Plaintiffs claimed that Tri-West failed to adequately secure the computers. The district court granted summary judgment in favor of Tri-West. On appeal, the Court of Appeals for the Ninth Circuit affirmed as to two of the three plaintiffs, who did not present any evidence of actual harm as a result of the disclosure of their information, but reversed as to one plaintiff who claimed to have suffered actual identity theft, finding that it was possible a jury could find a causal connection between the burglary and the identity theft. However, upon remand the district court denied the plaintiffs' motion for class certification, finding that the issues required an analysis of the facts unique to each potential member of the plaintiff class.

13 499 F.3rd 629 (7th Cir. 2007).

14 *Id*. at 634.

15 671 F. Supp. 2d 2046, 1053 (E.D. Mo. 2009).

16 2006 WL 2177036, at *1 (D.N.J. Mar. 16, 2009).

17 See also *Belle Chase Automatic Care, Inc. v. Advance Auto Parts, Inc*., 2009 WL 799760 at *4 (E.D. La. March 24, 2009) (plaintiff failed to state a claim because they did "not allege that any third party accessed their data and stole their identities, or that any other concrete financial loss resulted from the alleged negligence").

18 *Hammond v. The Bank of New York Mellon Corp*., 2010 WL 2643307 (June 25, 2010).

19 2009 WL 2843269, at *1, 4 (D. Conn. Aug. 31, 2009).

20 580 F. Supp. 2d 273, 275, 280 (S.D.N.Y. 2008).

stolen but who did not allege actual misuse of that information, had standing to litigate his claims.[21]

Because of the post-*Pisciotta* split, there now seems to be ample authority to support either side of the standing argument. Whether a plaintiff in a data breach case is found to have alleged a sufficient injury-in-fact to confer standing may well depend on the circuit in which the case is brought. For example, district courts in the Third Circuit, which covers the states of Pennsylvania and New Jersey, continue to routinely find that plaintiffs in data breach cases do not have standing under Article III.[22] On the other hand, the Court of Appeals for the Ninth Circuit, which covers the states of Washington, Oregon, Idaho, Montana, California, Nevada and Arizona, has recently endorsed the *Pisciotta* court's conclusion that plaintiffs in data breach cases generally do allege a sufficient injury-in-fact to confer standing.[23]

IV. Compensable Damages Under State Law

Just because a plaintiff has constitutional standing to sue, however, does not mean that the plaintiff has "standing to succeed" on the ultimate merits of the claims. As the Court of Appeals for the Ninth Circuit in *Krottner*, which involved the theft of a laptop, went on to explain:

> The court's conclusion that Plaintiffs have Article III standing does little to determine whether they have an injury that Washington law recognizes. An injury-in-fact serves merely as a license to sue in federal court. To recover for that injury, Plaintiffs must identify a legal theory that permits compensation for their injury. [24]

The *Krottner* court also reflected the reluctance of federal district courts to enlarge a substantive state law right of recovery.

> Whether the Washington Supreme Court would recognize Plaintiffs' theory of relief or not…it would only do so after a careful analysis of state policy and precedent, rendering legal judgments for which it can ultimately be held accountable by the people of Washington. This court has neither nine justices to independently consider Plaintiffs' claims nor direct accountability to the people of Washington. For similar reasons, many federal appellate courts demand restraint when considering novel state law claims that expand liability..[25]

As a consequence, until this year, it appears that nearly every federal court which has found standing to sue in a data breach case, including the court in *Pisciotta* itself, has nonetheless concluded that the claims were not actionable under the applicable state's law of contract or tort..[26]

The questions posed by these cases are of more than academic or theoretical interest to the RIMS industry. On September 19, 2007, a container of backup tapes belonging to the Louisiana Office of Student Financial Assistance (LOSFA) was inadvertently lost while in transit on a van operated by Iron Mountain. LOSFA claimed that the lost media contained personal information on many thousands of individuals participating in or considered for participation in programs for financial assistance and certain scholarship programs of higher education. Three putative class action lawsuits advancing various theories of negligence and other claims ensued, which were consolidated before a single judge in New Orleans. In essence, the plaintiffs alleged injuries in the form of invasion of privacy, identity theft, fear of identity theft, nuisance, anxiety, emotional distress, the need to close bank accounts and the need to register with fraud alert programs. In granting Iron Mountain's motion for summary judgment dismissing all claims against it, the federal court held that "the mere possibility that personal information may be at increased risk does not constitute actual injury sufficient to maintain a claim for negligence under the current state of Louisiana law". The court went on to find that "it is undisputed that no personal data has been compromised and plaintiffs have failed to offer evidence that any third party has gained access to the data". Accordingly, the court concluded that plaintiffs' alleged damages are "purely speculative" and thus they "lack the ability to prove an essential element of their negligence claim".[27]

V. The Hannaford Bros. Litigation Aftermath

The *Hannaford Bros*. litigation arose out of the criminal misappropriation of millions of credit and debit card numbers, expiration dates and security codes from the electronic payment processing system of a Maine-based national supermarket chain.

In late February, 2008, Visa notified Hannaford that its system had been breached. Hannaford discovered the means of access on March 8, 2008 and contained the breach on March 10, 2008. On the same day Hannaford gave notice to certain financial institutions and within a week later publicly announced that between

21 Despite finding standing, however, the court held that the plaintiff could not sustain a claim under New York law for negligence or breach of fiduciary duty. *See also Am. Fed'n of Gov't Employees v. Hawley,* 543 F. Supp. 2d 44, 45-46, 50-51 (D.D.C. 2008) (plaintiff, who alleged that hard drive containing personal information was lost but did not allege misuse, had standing, although the holding was in part based on The Privacy Act of 1974).

22 See, e.g., Reilly v. Ceridien Corp., 2011 WL 735512 (D.N.J. Feb. 22, 2011).

23 See Krottner v. Starbucks Corp., 406 Fed. Appx. 129 (9th Cir. 2010).

24 *Id*., 2009 WL 7382290 at *6, citing *Doe v. Chao,* 540 U.S. 614, 641 (2004) (noting that a plaintiff with Article III standing has "standing to sue, but not [necessarily] to succeed") (Ginsburg, J., dissenting).

25 2009 WL 7382290 at *21. See also *Pisciotta*, 499 F.3d at 635-636 (noting the court's reticence to expand Indiana law to recognize an enhanced risk of identity theft as a compensable injury); *Insolia v. Philip Morris Inc*., 216 F.3d 596, 607 (7th Cir. 2000) ("[f]ederal courts are loathe to fiddle around with state law. Though district courts may try to determine how state courts would rule on an unclear area of state law, district courts are encouraged to dismiss actions based on novel state claims").

26 *See, e.g., In re Hannaford Bros. Co. Customer Data Sec. Breach Litig*., 2010 Me. 93; 4 A.3d 492 (2010); *Pinero v. Jackson Hewitt Tax Serv., Inc.,* 594 F. Supp. 2d 710, 714-23 (E.D. La. 2009) (rejecting, inter alia, Louisiana and contract claims); *Cherny v. Emigrant Bank*, 604 F. Supp. 2d 605, 608-09 (S.D.N.Y. 2009); *Randolph v. ING Life Ins. & Annuity Co*., 973 A.2d 702, 708 (finding that monitoring costs were not compensable); *Shafran v. Harley-Davidson, Inc*., 2008 U.S. Dist. LEXIS 22494, at *8 (S.D.N.Y. Mar. 24, 2008); *Hendricks v. DSW Shoe Warehouse, Inc*., 444 F. Supp. 2d 775, 783 (W.D. Mich. 2006) ("[t]here is no existing Michigan statutory or case law authority to support plaintiff's position that the purchase of credit monitoring constitutes either actual damages or a cognizable loss."). One noteworthy exception is the decision of the Court of Appeals for the First Circuit in *In re TJX Companies Retail Security Breach Litigation,* 564 F.3rd 489 (1st Cir. 2009), in which the court allowed a bank seeking to represent a putative class to pursue a claim under the Massachusetts unfair trade practices statute against TJX and the bank that processed debit and credit card transactions on its behalf for damages sustained as a result of the data breach, including reimbursement of fraudulent charges. This ruling set the stage for a well-publicized $40.9 million settlement by TJX with the affected banks. *See USA Today* (11/30/2007)("TJX, Visa Reach $40.9 Million Settlement for Data Breach").

27 *Melancon v. Louisiana Office of Student Financial Assistance*, 567 F. Supp. 2d 873 (E.D. La. 2008).

December 7, 2007 and March 10, 2008, the security of its information technology system had been breached, leading to the theft of as many as 4.2 million debit card and credit card numbers belonging to individuals who had made purchases at more than 270 of its stores. Hannaford also announced "that it had already received reports of approximately 1,800 cases of fraud resulting from the theft of those numbers". The unauthorized charges originated across the globe, including New York, Spain and France.

Following Hannaford's announcement, some financial institutions immediately cancelled customers' debit and credit cards and issued new cards. Others did not, telling the cardholder they wished to wait for evidence of authorized activity before taking action. Plaintiffs claimed that some institutions, in response to customers' requests for new cards, charged fees for replacement cards and some plaintiffs also purchased identity theft insurance and credit monitoring services to protect themselves against possible consequences of the breach.

Twenty-six (26) separate suits against Hannaford arising out of the data breach were consolidated before a federal judge in Maine. In the consolidated complaint, plaintiffs alleged no fewer than seven causes of action, including breach of implied contract, breach of implied warranty, breach of duty of a confidential relationship, failure to advise customers of the theft of their data, strict liability, negligence, and violation of the Maine consumer unfair trade practices statute. Plaintiffs sought damages as well as injunctive relief in the form of credit monitoring and notification. The damages sought included the cost of replacement card fees, fees for accounts overdrawn by fraudulent charges, fees for altering pre-authorized payment arrangements, loss of accumulated reward points, inability to earn reward points during the transition to a new card, emotional distress, time and effort spent reversing unauthorized charges and protecting against further fraud, and the cost of purchase of identity theft and card protection insurance and credit monitoring services.

In a lengthy decision, the district court in Maine dismissed the claims of 20 of the 21 named plaintiffs.[28] The district court also dismissed nearly all of the substantive claims, concluding that the plaintiffs had not alleged facts stating a basis for those claims under Maine law. As to the surviving claims, the court divided the plaintiffs into three categories – the first comprised of those who did not have any fraudulent charges posted to their accounts, the second comprised of a single plaintiff whose fraudulent charges had not been reimbursed, and the third composed of plaintiffs whose fraudulent charges had been reimbursed – and concluded that only the single plaintiff in the second category could recover for her actual financial losses, dismissing the rest as not recoverable or as being "too remote, not reasonably foreseeable, and/or speculative". After this ruling, the plaintiffs moved, and the district agreed, to certify several questions of Maine state law to the Maine Supreme Judicial Court, which essentially adopted the reasoning of the federal district court. Judgment was then entered for Hannaford on all claims, and plaintiffs appealed to the Court of Appeals for the First Circuit, which covers Maine, New Hampshire, Massachusetts, Rhode Island and Puerto Rico.

The Court of Appeals issued its decision on October 20, 2011, affirming the vast majority of the district court's decision in favor of Hannaford but reversing in part, finding that implied contract and negligence were viable theories of recovery. As to damages, the First Circuit found that "a plaintiff may recover for costs and harms incurred during a reasonable effort to mitigate" damages from the data breach. To recover such damages, however, the plaintiffs needed to establish an actual injury such as money lost or spent as opposed to only time and effort. Importantly, however, the First Circuit affirmed the district court's decision dismissing the Maine unfair trade practices law claim, with its fee-shifting petition, thus relegating the case from a potential multi-million dollar exposure to one involving only a very few idiosyncratic and minor individual claims with no meaningful hope of certification as a class action or an award of plaintiffs' class action counsel fees. Thus, despite a superficial change in the decided cases prior to 2011, in reality the Hannaford Bros. decision has not made any substantive adjustment in the overall reluctance of the federal courts to open the floodgates to private litigation arising from data breaches, no matter how large or widely publicized.[29]

VI. Conclusions and Lessons

To date plaintiffs in data breach cases have met with very little success in recovering damages from the unauthorized loss or compromise of PII, PHI and other confidential information except in those few instances where the affected individuals have either suffered actual identity theft or incurred expenses in response to a credible threat of financial fraud. It would be premature, however, to conclude that the threat from such matters has passed. Many such cases continue to wind their way through the federal and state courts and additional incidents of data breaches continue to be reported. Attempts by plaintiffs to analogize certain casts, such as credit monitoring fees or identity theft insurance premiums, to medical testing and monitoring costs in response to an environmental exposure, have evinced some sympathy. In addition, proposals to codify private causes of action for data breaches are routinely introduced before legislative bodies. Finally, it should also be noted that both federal and state regulators have authority under both federal and state laws and regulations to seek relief to compel the implementation of reasonable data security processes and to seek fines and penalties for failure to comply with regulatory or industry standards for the protection of PII. Accordingly, although the financial threat from civil litigation resulting from data breaches still remains modest, there remain important reasons to adhere to and document compliance with applicable laws and standards and to comply strictly with the applicable statutory and regulatory frameworks in response to a data breach.

28 *In re Hannaford*, 613 F. Supp. 2d 108 (D. Me. 2009).

29 One unusual case still winding its way through the system resulted from the illicit hacking into the systems of RockYou, a publisher and developer of online services and applications for use with social networking sites such as Facebook and MySpace. In that case, plaintiffs advanced what a California federal court characterized as a "novel theory", namely that their PII constitutes "valuable property that is exchanged not only for defendant's products and services, but also in exchange for defendant's promise to employ commercially reasonable methods to safeguard the PII that is exchanged". Although the court declined to hold that plaintiff had failed to allege an injury in fact sufficient to support constitutional Article III standing, the district judge expressed "doubts about plaintiff's ultimate ability to prove his damages theory" and stated that if plaintiff could not demonstrate "tangible harm via the unauthorized disclosure of [PII], the court will dismiss plaintiff's claims for lack of standing at the dispositive motion stage". *Claridge v. RockYou, Inc.*, No. C 09-6032 PJM (N.D. Cal. Apr. 11, 2011). Just recently, however, it was announced that the case had been settled. Under the terms of the settlement, the plaintiff received $2,000 and his counsel received $290,000 from RockYou. Baker Hostetler *Data Privacy Monitor* (Nov. 21, 2011)(http://dataprivacymonitor.com).