NOTE

PREVENTING DATA BREACHES: ALTERNATIVE APPROACHES TO DETER NEGLIGENT HANDLING OF CONSUMER DATA

Jacob W. Schneider[*]

I. INTRODUCTION

Armed with a telescope-shaped antenna and a laptop, hackers, operating from a distance, intercepted data floating across T.J. Maxx's ("TJX") wireless

[*] J.D., Boston University School of Law, 2009; B.S. Computer Science, Trinity College (Hartford, CT), 2004.

network in Saint Paul, Minnesota.[1] The data they caught held the key to TJX's customer database and, with it, a treasure trove of credit card numbers and other customer information.[2] Eighteen months later, the retailer finally discovered the breach – but the damage was already done.[3] By then, the hackers had stolen information from over 94 million customer accounts.[4] It was the largest data breach in United States history.[5]

While the ringleader of the illicit operation lies behind bars,[6] both consumers and banks have filed negligence class action suits against TJX.[7] These parties alleged that TJX breached its duty to keep consumer and bank information protected from hackers.[8] To date, judges have been quick to dismiss data breach negligence suits because consumer class plaintiffs have difficulty showing injuries appropriate for legal relief.[9] Typically, only a small number of stolen accounts are ever subject to fraudulent purchases.[10] Attempts

[1] Bill Brenner, *TJX breach tied to Wi-Fi exploits*, SEARCHSECURITY.COM, May 7, 2007, http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1254020,00.html.

[2] *Id.*

[3] *Id.*

[4] Ross Kerber, *Court filing in TJX Breach: 94 million accounts were affected, banks say*, THE BOSTON GLOBE, Oct. 24, 2007, at A1, *available at* http://www.boston.com/business/globe/articles/2007/10/24/court_filing_in_tjx_breach_doubles_toll.

[5] *Id.*

[6] News Release, Office of the Attorney General of Florida, *Ringleader of ID Theft Operation Sentenced to 5 Years in Prison*, Sept. 13, 2007, http://myfloridalegal.com/__852562220065EE67.nsf/0/3D930E6715D0935D85257355005143E9.

[7] Rebecca Herold, *PCI DSS and GLBA Compliance & Privacy Breach: Lawsuits Filed Against TJX*, REALTIME COMMUNITY, http://www.realtime-itcompliance.com/identity_theft/2007/02/pci_dss_and_glba_compliance_pr.htm (last visited Feb. 20, 2009) (providing a timeline of litigation against TJX for the security breach and resultant personal data exposure).

[8] *Id.*

[9] *See* Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 639 (7th Cir. 2007) ("Without more than allegations of increased risk of future identity theft, the plaintiffs have not suffered a harm that the law is prepared to remedy."); Forbes v. Wells Fargo Bank, N.A., 420 F. Supp. 2d 1018, 1020-21 (D. Minn. 2006) ("Moreover, they overlook the fact that their expenditure of time and money was not the result of any present injury, but rather the anticipation of future injury that has not materialized. In other words, the plaintiffs' injuries are solely the result of a perceived risk of future harm. Plaintiffs have shown no present injury or reasonably certain future injury to support damages for any alleged increased risk of harm.").

[10] Steve Lohr, *Surging Losses, but Few Victims in Data Breaches*, N.Y. TIMES, Sept. 27, 2006, at G1, *available at* http://www.nytimes.com/2006/09/27/technology/circuits/27lost.html ("Regardless of the data breach, a rise in financial fraud has not surfaced. Visa and MasterCard report that about 2 percent of the card accounts lost or stolen in the last 18 months have been used to make

to obtain relief for anticipated losses or to secure reimbursement for future credit monitoring fees have met judicial resistance.[11] Financial institutions, seeking to recoup losses from fraudulent activity and reissuing credit cards, have met similar resistance.[12]

What these decisions fail to recognize is that when hackers obtain confidential account information they can get more than just a credit card number.[13] The hackers can obtain other personal information used to impersonate their victims.[14] For instance, hackers may use this information to apply for new credit cards,[15] manipulate online auctions,[16] or even make unauthorized stock trades.[17] Identity thieves can attack consumers on many different fronts and subject them to much more than just fraudulent credit card charges.

More importantly, since these suits fail, little effectively compels retailers to adopt stronger security safeguards. In recent years, the risk of identity theft has

---

fraudulent purchases. That is within the range of the 1.5 percent and 4 percent of consumers who reported being victims of financial fraud or identity theft, surveys say.").

[11] *See Pisciotta*, 499 F.3d at 638-40; *Forbes*, 420 F. Supp. 2d at 1019-21.

[12] Kirk J. Nahra, *Plaintiffs in Creative Privacy Litigation Still Face an Uphill Struggle*, PRIVACY IN FOCUS NEWSLETTER (Wiley Rein, LLP, New York, N.Y.), May 2006, *available at* http://www.wileyrein.com/publication_newsletters.cfm?id=10&publication_ID=12623. *See* Banknorth, N.A. v. BJ's Wholesale Club, Inc., 442 F. Supp. 2d 206, 211-14 (M.D. Pa. 2006) (dismissing the case on summary judgment under the economic loss rule); Sovereign Bank v. BJ's Wholesale Club, Inc., 395 F. Supp. 2d 183, 195 (M.D. Pa 2005) ("Sovereign should not be allowed to upset the expectations of the parties to the VISA system by injecting the uncertainty of tort law into the system.").

[13] Some customers "were robbed of their driver's license numbers and other personal information." *See* Brenner, *supra* note 1.

[14] *Id.*

[15] Peter Brownfeld, *Identity Theft Worries Consumer Advocates*, FOXNEWS.COM, Feb. 10, 2004, http://www.foxnews.com/story/0,2933,110923,00.html ("Identity thieves then use stolen Social Security numbers, addresses and phone numbers to apply for credit cards and change billing addresses. In many cases, victims never even know they are being taken until they apply for a loan and find their credit has been destroyed.").

[16] Caroline McCarthy, *Study: Identity Theft Keeps Climbing*, CNET NEWS, Mar. 6, 2007, http://www.news.com/Study-Identity-theft-keeps-climbing/2100-1029_3-6164765.html ("'Hackers are exploiting Internet auctions, non-regulated money transmittal systems, the ability to impersonate lottery and sweepstake contests, and other types of imaginative scams,' Gartner analyst Avivah Litan said in a statement.").

[17] Ellen Nakashima, *Hackers Zero In on Online Stock Accounts*, WASHINGTON POST, Oct. 24, 2006, at A01, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2006/10/23/AR2006102301257.html; BUSINESS WEEK ONLINE, *Invasion of the Stock Hackers*, Nov. 3, 2005, http://www.businessweek.com/technology/content/nov2005/tc20051103_565150.htm; Judith Burns, *Offshore Hackers Changed with Fraud, Identity Theft*, MARKETWATCH.COM, Mar. 12, 2007, http://www.marketwatch.com/news/story/offshore-hackers-charged-fraud-identity/story.aspx?guid=%7BD71B9BA1-269C-423E-990B-58C2FCE6DD44%7D.

grown annually at a rapid rate.[18] Between 2003 and 2006, the United States saw a fifty percent increase in the number of identity theft victims.[19] Today, identity theft affects about fifteen million Americans each year.[20]

In Part II, this Note will discuss how existing legal mechanisms have failed to deter the negligent handling of personal information. Part II.A will show how statutory notification laws, standing alone, do not establish the proper incentives to compel retailers to adopt cutting-edge security procedures. Part II.B will describe how traditional tort negligence suits, brought on behalf of both consumers and banks, have failed to hold breached retailers accountable. Part III will discuss two new potential statutory actions (one brought by consumers, the other by states), aimed at deterring negligent handling of data. It will explore the proper amount of damages to impose upon a breached retailer, as well as the requisite level of security precautions necessary to avoid liability for the breach. Finally, Part IV will advocate for state-level legislation to establish these new civil actions against retailers – setting the standard of care according to industry custom and the measure of damages by statute.

II. FAILING TO PREVENT FUTURE BREACHES: INEFFECTUAL NOTIFICATION LAWS AND DISMISSED NEGLIGENCE SUITS

Currently, there are two legal mechanisms available to deter a retailer's negligent handling of a consumer's personal information: state statutory notification laws and private civil tort actions. Neither effectively deters negligent behavior nor encourages reasonable care on the part of data handlers.

A. Ineffectual Statutory Notification Laws

With data breach incidents on the rise,[21] forty-four states have enacted notification statutes. [22] Notification statutes require retailers to publicly acknowledge data breaches, alerting affected parties to take appropriate precautions.[23]

California's notification statute, the Security Breach Information Act ("SBIA"),[24] was the first notification statute in the nation.[25] Many states have

---

[18] *Gartner Says Number of Identity Theft Victims Has Increased More than 50 Percent Since 2003*, GARTNER, Mar. 6, 2007, http://www.gartner.com/it/page.jsp?id=501912

[19] The average loss resulting from identity theft grew from $1,408 in 2003 to $3,257 in 2006. *Id.*

[20] *Id.*

[21] *Id.*

[22] National Conference of State Legislatures, State Security Breach Notification Laws, http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm (last visited Feb. 19, 2009).

[23] *Id.*

[24] CAL. CIV. CODE § 1798.82 (West 2007).

[25] Vincent R. Johnson, *Cybersecurity, Indentity Theft, and the Limits of Tort Liability*, 57 S.C. L. REV. 255, 264 (2005).

used the SBIA as a template for their own legislation.[26] As a result, the SBIA provides a good example of notification laws throughout the United States.[27] The SBIA requires California businesses to "disclose any [known] breach . . . of the security of the system. . . to any resident of California whose unencrypted personal information was . . . acquired by an unauthorized person."[28] The SBIA makes exceptions to the notification requirements when the lost data was encrypted (as opposed to plain-text) or to assist law enforcement.[29] Under the SBIA, a written letter to those affected by the breach may satisfy the statutory notice requirement.[30] Notice via email, a website posting, or statewide media is acceptable when the price of notice exceeds $250,000, the breach affects at least 500,000 people, or the business does not have sufficient contact information for those affected.[31]

Most state statutory notification laws follow this model, though some contain minor deviations.[32] For example, Georgia, Minnesota, and Texas require notification to consumer reporting agencies.[33] Florida imposes heavy fines on businesses that fail to promptly report a breach.[34] Arizona, Montana, and Nevada require businesses to take added precautions when disposing of personal information.[35]

Although quickly informing consumers of data breaches, thus allowing them to take proper precautionary measures, is an important step towards protection, notification laws do little to deter the underlying negligent conduct. Although public notification can damage a retailer's reputation or result in an influx of litigation on behalf of customers and financial institutions, these consequences inadequately deter negligent behavior.

1. Damage to Reputation

Studies have shown that notification laws can have a negative impact on a retailer's brand name.[36] Presumably, after the retailer publicly admits losing

[26] *Id.*

[27] *Id.*

[28] CAL. CIV. CODE § 1798.82(a) (West Supp. 2009).

[29] *See id.* at § 1798.82(a), (c) (allowing for delayed notification if it otherwise would impede a criminal investigation).

[30] *Id.* at § 1798.82(g)(1).

[31] *Id.* at § 1798.82(g)(3).

[32] Johnson, *supra* note 25, at 264.

[33] *See* GA. CODE ANN. § 10-1-912(d) (LexisNexis 2008); MINN. STAT. § 325E.61 subd. 2 (West 2008); TEX. BUS. & COM. CODE ANN. § 48.103(h) (Vernon 2008).

[34] *See* FLA. STAT. ANN. § 817.5681(1)(b), (2)(b) (West 2008).

[35] *See* ARIZ. REV. STAT. ANN. § 44-7601 (West 2008); MONT. CODE ANN. § 30-14-1703 (West 2007); NEV. REV. STAT. § 603A.200 (2007).

[36] SAMUELSON LAW, TECHNOLOGY & PUBLIC POLICY CLINIC, UNIVERSITY OF CALIFORNIA-BERKELEY SCHOOL OF LAW, SECURITY BREACH NOTIFICATION LAWS: VIEWS FROM CHIEF SECURITY OFFICERS 16 (2007), *available at*

personal information in a large-scale attack, consumers would be less likely to continue patronizing the merchant.[37] A February 2007 survey found that 75% of debit card holders said they would not shop at a retailer after a data breach became public[38] and 84% of those polled said they would prefer retailers with stronger data security reputations.[39] Reality, however, demonstrates the contrary result. Well after public notification of the break-in, consumers continue to shop enthusiastically at the retailer hit with the largest and most publicly discussed data breach incident in United States history: T.J. Maxx.[40] One reason for this is that consumers, like courts, may be weighing the generally low likelihood of harm resulting from data breaches.[41] The problem is exacerbated because consumers rarely have good information regarding the sophistication and effectiveness of a retailer's security systems.[42] Nevertheless, while there is a blight on TJX's reputation, it does not appear to have affected its bottom line.[43]

The facts underlying some data breach cases may shield some retailers from serious reputation damage. Often, retailers outsource their information infrastructure to third-party data warehouses or web-hosting companies.[44] For example, in a case summarized below,[45] Old National Bancorp employed NCR

http://www.law.berkeley.edu/clinics/samuelson/cso_study.pdf ("Of those security professionals surveyed in CSO Magazine's latest E-Crime survey, 23% of security professionals who have experienced negative security events cited harm to the organization's reputation as a loss resulting from an electronic crime suffered by the organization.").

[37] *Id.*

[38] Larry Greenemeier, *The TJX Effect: Details of the Largest Breach of Customer Data are Starting to Come to Light*, INFORMATIONWEEK, Aug. 11, 2007, http://www.informationweek.com/story/showArticle.jhtml?articleID=201400171 (citing a Javelin Strategy & Research survey).

[39] *Id.*

[40] Chris Reidy, *Sales up at TJX*, Apr. 12, 2007, http://www.boston.com/business/ticker/2007/04/sales_up_at_tjx.html ("The loss of millions of customer credit- and debit-card records seems to be having little impact on the sales of TJX Cos." Sales for the retailer were up 11% from the previous year.); Greenemeier, *supra* note 38 ("Financial analysts continue to raise their expectations for the company's stock price, as first-quarter 2008 sales were up about 6% compared with the year-earlier quarter, to $4.1 billion. Net income was down less than 2% from a year ago, to $162.1 million—not bad considering the $20 million charge TJX had to take.").

[41] *See* Lohr, *supra* note 10.

[42] Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913, 947 (2007) (". . . [A] consumer generally has good information about price . . ., but bad information about non-price terms (such as the full range of investment by a company in data security and whether such investment is likely to be effective).").

[43] *See* Reidy, *supra* note 40.

[44] *See generally Pisciotta*, 499 F.3d 629.

[45] The *Old National Bancorp* case is discussed in detail, *infra* Part II.B.1.

to host its website, and the breach occurred under NCR's supervision.[46] Retailers can affect public relations by either blaming their hosting companies for their lax security or sharing the blame with them, thus significantly diffusing public criticism.[47] Even if the retailer's brand name suffers substantial damage from statutory notification and the resulting negative publicity, there is no guarantee that this will reduce the retailer's profitability.[48] As a result, in many instances, public notification statutes only have a slight deterrent effect upon retailers.[49]

2. Threats of Litigation

Public notification of data breaches alerts consumers and financial institutions, prompting both to prepare for litigation against the retailer.[50] While no business ever wants to face litigation, as it stands today, compromised retailers can feel confident that they face no serious threat of legal liability.[51] Retailers will typically face class action suits comprised of two

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

[47] This, however, might not be the best tactic. One 2006 study by the Ponemon Institute found that customers generally feel betrayed upon discovering that their retailers outsource their personal information to third-party data warehouses. *Customers unlikely to forgive data leaks from third-party contractors*, INFOWATCH, Oct. 31, 2006, http://www.infowatch.com/threats?chapter=162971949&id=204558358.

[48] *See generally* Reidy, *supra* note 40.

[49] Larry Walsh, *Security Breach Costs TJX Surprisingly Little*, BASELINE SECURITY, Dec. 21, 2007, http://blog.baselinemag.com/security/content001/data_breaches/tjxs_unblemished_reputation_disproves_security_assumption.html ("Reputation was always supposed to be the biggest damage, but the TJX experience is disproving that. . . . If you look back at some of the bigger security breaches of the past few years—Kaiser Permenente, Bank of America, Wells Fargo, ChoicePoint—none of the affected companies have suffered lasting reputational loss to their security breaches. . . . While the cost of correcting the reasons behind a security breach will likely continue to climb, it's hard to imagine that reputational cost will have any impact, thanks to our short attention spans.").

[50] Jackson Lewis, *Massachusetts Identity Theft Law Creates Data Breach Notification, Protection and Destruction Requirements*, JACKSON LEWIS, Aug. 23, 2007, http://www.jacksonlewis.com/legalupdates/article.cfm?aid=1184 (discussing the new Massachusetts data breach notification law, "While this measure may be good news for Massachusetts residents, the law significantly increases businesses' exposure to civil actions by individuals and the Massachusetts attorney general with regard to the security of their business and employment records. Exposure to litigation and penalties is enhanced for those businesses with large numbers of employees and operations in Massachusetts and other states, especially in view of some of the unique features of the Massachusetts law . . .").

[51] Jaikumar Vijayan, *Are Data Breach Lawsuits Just Tilting at Windmills?*, CIO, Aug. 27, 2007, http://www.cio.com/article/133250/Are_Data_Breach_Lawsuits_Just_Tilting_at_Windmills_ (quoting Christopher Pierson, partner at Lewis and Roca, "'Lawsuits brought under traditional negligence norms will not be successful. Courts are just not going to award

groups: consumers and banks seeking to recoup losses due to reissuing credit cards and fraudulent purchases.[52] Cases brought by either party have been unsuccessful.[53]

B. Failure of Recent Tort Actions

Usually, two groups bring suit against institutions for failure to protect personal information: disgruntled consumers who fear fraudulent charges and banks seeking to recoup credit card reissuing costs, as well as funds used for fraudulent purchases.[54] Both have been unsuccessful.[55]

1. Failure of the Consumer Suits

Consumers, banded together by class actions, have great difficulty bringing a successful negligence action against retailers who have compromised their personal data.[56] It is standard hornbook knowledge that a successful negligence suit involves four elements: (1) duty; (2) breach of that duty; (3) injury caused by the breach; and (4) damage to the plaintiff.[57] Although class plaintiffs can usually establish the first three elements,[58] proving actual damages remains a stumbling block.[59]

A recent case in the Seventh Circuit, *Pisciotta v. Old National Bancorp*,[60] demonstrates the difficulty of proving damages in a data breach suit.[61] Old

damages and let these cause of action go forward unless there is actual harm' from a data breach. Even in those cases, actually proving that the harm resulted from a specific data breach can be incredibly hard, especially given the high number of data breaches being disclosed these days, Pierson said. 'It's going to be difficult for an individual to prove that it was actually company A's breach as opposed to company B's breach that caused them harm.'").

[52] The TJX incident quickly lead to consumer and bank class action suits. *See Lawsuits Filed Against TJX*, *supra* note 7.

[53] Denis Rice, *Civil Actions for Privacy Violations 2007: Where Are We?*, June 2007, http://www.howardrice.com/uploads/content/Civil%20Actions%20For%20Privacy%20Violations%202007%20-%20Where%20Are%20We.pdf (detailing unsuccessful suits brought by consumers); *See Banknorth*, 442 F. Supp. 2d at 211-14 (leading case dismissing suit for credit card reissuing fees and fraudulent purchases based on economic loss rule).

[54] Rice, *supra* note 53, at 2-4, 14-17.

[55] Vijayan, *supra* note 51; Rice, *supra* note 53, at 2-4.

[56] *Id.*

[57] *See* KENNETH S. ABRAHAM, THE FORMS AND FUNCTIONS OF TORT LAW 47-48 (3d ed. 2007).

[58] Professor Johnson provides the best support for imposing a legal duty on businesses to their customers to protect personal information. *See* Johnson, *supra* note 25, at 263-80.

[59] Rice, *supra* note 53, at 14-17.

[60] *Pisciotta*, 499 F.3d 629.

[61] Brendon Tavelli, *No Harm, No Lawsuit: Seventh Circuit Refuses Data Breach Lawsuit Where Credit Monitoring Costs Are the Only "Damages" Sought*, PRIVACY LAW BLOG, Sept. 10, 2007, http://privacylaw.proskauer.com/2007/09/articles/identity-theft/no-harm-no-

National Bancorp suffered a data breach that compromised a variety of customer personal information.[62] While details of the breach are filed under seal,[63] "the scope and manner of access suggests that the intrusion was sophisticated, intentional and malicious."[64] Old National Bancorp's database stored the gamut of personal information: ". . . name, address, social security number, driver's license number, date of birth, mother's maiden name and credit card or other financial account numbers."[65] In the complaint, the plaintiffs alleged negligence on the part of Old National Bancorp for "failing to adequately protect [their] personal confidential information."[66] At trial, the plaintiffs argued that damages included expenses related to credit monitoring and emotional damages.[67] The plaintiffs, however, did not enumerate any direct economic losses resulting from the breach.[68] As a result, the district court granted the defendant's motion to dismiss.[69]

On appeal, Judge Ripple, writing for the Seventh Circuit, affirmed the district court's dismissal.[70] In doing so, the court rejected an argument that a recent Indiana state law requiring institutions to publicly report data breaches signaled state recognition that personal information loss, alone, could be considered a type of damage.[71] Judge Ripple also preemptively rejected an argument that tried to analogize personal information exposure to toxic tort cases, where exposure to chemicals may lead to medical problems in the future.[72] Whereas the plaintiffs in this case sought credit monitoring as a preventative measure, those exposed to chemicals in the toxic tort context often seek medical monitoring costs.[73] Finally, Judge Ripple cited several other jurisdictions which have concluded that "[w]ithout more than allegations of increased risk of future identity theft, the plaintiffs have not suffered a harm that the law is prepared to remedy."[74]

When an individual's personal information is stolen, there is no guarantee

lawsuit-seventh-circuit-refuses-data-breach-lawsuit-where-credit-monitoring-costs-are-the-only-damages-sought.

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

[63] *Id.*

[64] *Id.*

[65] *Id.* at 631.

[66] *Id.* at 632.

[67] *Id.*

[68] *Id.*

[69] *Id.* at 632-33.

[70] *Id.* at 640.

[71] *Id.* at 636-37 (referencing IND. CODE. § 24-4.9-3-1 (2006)).

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

[73] *Id.* at 639 (citing Badillo v. American Brands, Inc., 16 P.3d 435, 438-39 & nn. 1-2 (Nev. 2001)).

[74] *Id.*

that it will be used fraudulently.[75] In fact, only 2% of stolen credit card information from data breaches is subject to misuse.[76] Of all identity theft reports, only 1.5 to 4% are the result of stolen credit card information.[77] This probability goes down even further when the volume of personal information is large – since identity thieves can only make use of a small number of accounts.[78] Large class actions are more likely to develop from large-scale data breaches, so they are particularly unlikely to show real damage to all of their individual class constituents.

The consumer suits fail because of the inability to show real damages resulting from the exposure of personal information.[79] Increased likelihood that one's personal information will be used for illicit activity, standing alone, is not sufficient to warrant relief at law.[80] Attempts to argue that legislative intent supports awarding relief have also failed.[81] Finally, creative grafting of toxic tort theories to the increased likelihood of credit fraud has also failed.[82] Thus, plaintiffs face an uphill battle in court against institutions that have compromised their personal data.[83] This is not to say consumers never obtain any relief.[84] Retailers like TJX are quick to settle with consumers, likely to avoid negative publicity.[85] These efforts, however, will likely award consumers much less than a successful suit.

2. Failure of the Bank Suits

When a hacker obtains personal information from a retailer's database,

[75] Lohr, *supra* note 10.

[76] *Id.*

[77] *Id.*

[78] *Id.*

[79] *See Pisciotta*, 499 F.3d at 632; Bell v. Acxiom Corp., No. 4:06CV00485-WRW, 2006 WL 2850042 (E.D. Ark Oct. 3, 2006); Guin v. Brazos Higher Educ. Serv. Corp., Inc., No. Civ. 05-668 RHK/JSM, 2006 WL 288483 (D. Minn. Feb. 7, 2006); Walters v. DHL Express, No. 05-1255, 2006 WL 1314132, *5 (C.D. Ill. May 12, 2006).

[80] *See Pisciotta*, 499 F.3d at 632; *Guin*, 2006 WL 288483; *Walters*, 2006 WL 1314132 at *5.

[81] *Pisciotta*, 499 F.3d at 636-37.

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

[83] Vijayan, *supra* note 51.

[84] Consumers in class actions may still recover a settlement from defendants seeking to avoid a lengthy, expensive, and public civil trial. Consumer plaintiffs in the TXJ litigation have settled their claims. *See* TJX Settlement Website, http://www.tjxsettlement.com/ (last visited Feb. 19, 2009). Consumers affected by the TJX data breach may receive identity theft insurance, restitution for losses incurred from data theft, a $30 gift card to TJX, or some combination thereof. Furthermore, TJX agreed to hold a 15%-off sale event to benefit all TJX customers. Amended Settlement Agreement, In re TJX Companies Retail Security Breach, No. 07-10162 (D. Mass filed Nov. 14, 2007), *available at* http://www.tjxsettlement.com/Documents.aspx.

[85] *Id.*

notified banks and credit institutions must take immediate action.[86] They will lock or monitor the consumer accounts and reissue credit cards with new numbers.[87] The cost of reissuing the cards alone may be ten to twelve dollars per card,[88] making preventative measures costly when there are multiple compromised accounts.[89] As a result, financial institutions may file a negligence suit against the retailer for reimbursement of these costs,[90] but these suits have also met resistance.[91]

A recent case from the Middle District of Pennsylvania, *Banknorth, N.A. v. BJ's Wholesale Club, Inc.*, demonstrates judicial reluctance in these situations to award damages under tort law.[92] Hackers attacked BJ's Wholesale Club, Inc. ("BJ's") and stole credit information from about eight million of its customers.[93] Banknorth sued BJ's for negligent handling of its cardholders' data.[94] The bank sought $186,000 in card reissuing fees as well as $583,000 to recoup for fraudulent purchases.[95]

The court applied the economic loss rule,[96] which "bars recovery in a

---

[86] Bob Sullivan, *Credit card leaks continue at a furious pace*, MSNBC.COM, Sept. 24, 2004, http://www.msnbc.msn.com/id/6030057 ("Banks and credit card associations work fast after a batch of credit cards are leaked; Often, accounts are canceled long before fraud occurs.").

[87] Matt Hines, *Bank Card Reissues May Be Linked to Wal-Mart Breach*, eWEEK.COM, Feb. 10, 2006, http://www.eweek.com/c/a/Security/Bank-Card-Reissues-May-Be-Linked-to-WalMart-Breach.

[88] *See* Mechell Cooper, *Bank hears of data breach*, KENNEBEC JOURNAL, Jan. 17, 2009, http://kennebecjournal.mainetoday.com/news/local/5828410.html ("One bank executive at the time said the cost to issue about 14,000 new cards to customers—including administrative time, mailings to customers and the cards themselves—was about $10 to $12 per card in the Hannaford case.").

[89] Sullivan, *supra* note 86 ("Philadelphia-based Sovereign Bank, for example, told The Associated Press that it had to reissue 81,000 cards twice after the BJ's break-in, at a cost of about $1 million.").

[90] Nahra, *supra* note 12. *See Banknorth*, 442 F. Supp. 2d at 211-14 (dismissing the case on summary judgment under the economic loss rule); *Sovereign Bank*, 395 F. Supp. 2d 183 ("Sovereign should not be allowed to upset the expectations of the parties to the VISA system by injecting the uncertainty of tort law into the system.").

[91] Nahra, *supra* note 12. *See Banknorth*, 442 F. Supp. 2d at 211-14; *Sovereign Bank*, 395 F. Supp. 2d at 183.

[92] *See Banknorth*, 442 F. Supp. 2d at 213 (stating the "economic loss rule" and barring a negligence claim under the rule).

[93] Mark Jewell, *Credit Card Theft Brings Fresh Attention to Growing Problem*, USATODAY.COM, Jul. 6, 2004, http://www.usatoday.com/tech/news/computersecurity/2004-07-06-idtheft_x.htm.

[94] *Banknorth*, 442 F. Supp. 2d at 207.

[95] *Id.*

[96] *Id.* at 211-14.

negligence claim of economic damages alone."[97] Put succinctly, this rule rejects tort liability and leaves the issue to contract law, where terms are negotiated by both parties before conducting business.[98] In the products liability context, if damage is done only to the product itself, tort law gives way to the manufacturer's packaged contractual warranty to determine liability and the amount of damages.[99]

In applying the economic loss rule to the *Banknorth* case, Judge Caldwell stated that "[t]he insight behind the doctrine is that commercial disputes ought to be resolved according to the principles of commercial law rather than according to tort principles designed for accidents that cause personal injury or property damage. . . . Banknorth could have bargained for allocating the risk of fraudulent transactions with Visa before signing its Visa contract."[100] This case sends a clear message: banks and credit institutions should anticipate data breaches and resulting costs during negotiations with retailers and each other.

The statutory notification laws serve important goals: they inform the public of a risk of fraud and compel consumers and credit card issuers to take preventative measures to avoid the threat.[101] These laws, however, treat the symptoms of data breach incidents instead of the root cause: negligent handling of consumer data. Without more than notification, businesses can feel confident that mismanagement of data will lead to only legal nuisances, as opposed to serious liability, since civil actions have yet to impose substantial damage on defendants.[102] Defendants can feel confident that their adversaries will have difficulty proving damages, and efforts to find a way around this hurdle have failed. Part III will discuss two statutory actions aimed at deterring negligent handling of personal information. It will also explore several approaches to calculating damages and the requisite standard of care to impose upon institutions that warehouse personal information.

III. CALL FOR NEW CIVIL ACTIONS TO PROMOTE SECURE PROTECTION OF PERSONAL DATA

Since both consumer and credit institution suits fail,[103] neither can be relied upon to compel retailers to adopt cutting-edge, sophisticated means of protecting consumer data. The damage to reputation brought by public

[97] *Id.* at 211.

[98] Casa Clara Condominium Association, Inc. v. Charley Toppino & Sons, Inc., 620 So. 2d 1244, 1246 (Fla. 1993) ("In other words, economic losses are 'disappointed economic expectations,' which are protected by contract law, rather than tort law." (quoting Comment, *Manufacturers' Liability to Remote Purchasers for "Economic Loss" Damages – Tort or Contract?*, 114 U. PA. L. REV. 539, 541 (1966))).

[99] *Id.* at 1245-48.

[100] *Banknorth*, 442 F. Supp. 2d at 213.

[101] Schwartz, *supra* note 42, at 917.

[102] *See supra* Parts II.B.1-2.

[103] *See id.*

notification of data breaches has not prevented consumers from patronizing these businesses.[104] As a result, businesses have little incentive to strengthen data security and breaches continue to occur.[105] It is clear that stronger medicine is needed to strengthen the incentive to protect customer information. This Part will discuss the necessary elements of two new statutory civil actions against businesses, both focused on deterring future negligent handling of customer data. The first is created solely to establish damages in consumer negligence suits. The second is a state regulatory solution.

A. Rethinking the Damages Problem: Paving the Way to a Successful Consumer Suit

The state can easily remove the damages problem, which has plagued the consumer suits,[106] by recognizing a new type of injury. This injury is one of "personal data exposure," which doesn't rely on whether the exposure leads to injuries to reputation or credit. The courts have been reluctant to recognize this type of injury,[107] but statutory establishment of this legal fiction will yield beneficial results. Consumers will finally clear the damages hurdle in their negligence actions.

One may object to the injury of personal data exposure since it will allow plaintiffs to recover for no real losses, but the idea of potential damages, though rare, is not completely foreign to tort law.[108] Inchoate and future losses are notable examples.[109] Professor Vincent Johnson analogizes personal data exposure and cases of emotional distress stemming from exposure to toxic substances.[110] This distress, such as fear of developing illness from the incident, is an uncertain area of law.[111] Some courts, however, have allowed recovery if, "the fear stems from a knowledge, corroborated by reliable medical and scientific opinion, that is more likely than not that the feared [illness] will develop in the future due to the toxic exposure."[112] Since the logical remedy is payment of the plaintiff's medical monitoring costs, Professor Johnson concludes that security monitoring costs would be

---

[104] Reidy, *supra* note 40.

[105] Privacy Rights Clearinghouse, A Chronology of Data Breaches, http://www.privacyrights.org/ar/ChronDataBreaches.htm (last visited Mar. 28, 2008) (providing an up-to-date listing of major data breaches).

[106] *See* discussion *supra* Part II.B.1. *See also Pisciotta*, 499 F.3d at 637 (finding that "Indiana law would not recognize the costs of credit monitoring . . . as compensable damages").

[107] *See* discussion *supra* Part II.B.1.

[108] ABRAHAM, *supra* note 57, at 218-19.

[109] *Id.*

[110] Johnson, *supra* note 25, at 303-11.

[111] Jurisdictions widely differ over whether these actions can prevail. *Id.* at 303-04.

[112] *Id.* at 305 n.325 (quoting Potter v. Firestone, Tire & Rubber Co., 863 P.2d 795, 800 (Cal. 1993)).

appropriate in security breach cases.[113] Some courts have sided with Professor Johnson,[114] many others have not.[115]

The suit would proceed just as any other negligence action,[116] but the problem of showing actual damages would be removed. Plaintiffs who can demonstrate that a business housed their personal information in an unreasonably insecure manner, which lead to the information's exposure to hackers, would be able to recover some measure of damages. Part III.C will explore ways of calculating a damage award and Part III.D will examine the appropriate measure of reasonable security precautions.

B. State Regulatory Action

Another solution is to allow the state to bring suit against a retailer.[117] A local authority, most-likely the state's attorney general, would file suit against the retailer for negligent handling of customer information.[118] This suit would proceed much like the consumer action above, carrying all the indicia of a common law negligence suit.[119] If liable, the retailer would pay the state, not consumers, some measure of damages.

This money could be used to compensate victims of identity theft stemming from the incident.[120] Some plaintiffs would only suffer real injury after the suit is complete. Because the state can distribute funds well after the trial, it has the ability to wait and see if real injury does occur. As a matter of public policy, the state may decide to add proceeds from successful suits to a larger fund used to prevent future identity theft. The state may also use the funds to compensate all resident identity theft victims, regardless of whether the breach immediately at issue exposed their personal information. In essence, this state action could shift the costs of identity theft from the victims to a pool of negligent personal

---

[113] *Id.* at 305-11.

[114] *Id.* at 308 n. 345.

[115] *See supra* Part II.B.1; *Pisciotta*, 499 F.3d at 636-37 (requiring plaintiffs in emotional distress from toxic substance exposure to show at least some initial injury that may lead to greater illness, like cancer).

[116] *See* ABRAHAM, *supra* note 57, at 47-48.

[117] Arizona's statutory notification law allows the attorney general to bring suit against a retailer for $10,000 per breach incident. ARIZ. REV. STAT. § 44-7501(H)(2009).

[118] *Id.*

[119] *See* ABRAHAM, *supra* note 57, at 47-48.

[120] Before his epic fall-from-grace, Eliot Spitzer, former New York State Attorney General, came to a similar agreement with an online retailer that benefits consumers. "Under the terms of the agreement, Barnesandnoble.com will pay $60,000 in costs and penalties and establish an information security program to protect personal information; establish management oversight and employee training programs; and hire an external auditor to monitor compliance with the security program." Linda Rosencrance, *Barnesandnoble.com Hit with Fine for Online Security Breach*, COMPUTERWORLD.COM, Apr. 30, 2004, http://www.computerworld.com/securitytopics/security/holes/story/0,10801,92804,00.html.

information collectors.

C. Calculating Damages

Both the consumer and state-sponsored actions outlined above would have to determine the proper measure of liability to impose upon negligent companies. There are several possible solutions to this problem, and this portion of the Note will explore a few options. Whatever the solution, it is important to strike the proper balance between deterring negligent maintenance of online databases and encouraging a healthy online marketplace. When damages are set too high, businesses will be less likely to enter the market. When set too low, consumers are put at risk. It is also important to recognize that some smaller online retailers who collect personal data will be unable to pay even modest damages.

1. Expected Losses

One approach is to set liability at the level of expected monetary losses an individual, in the consumer action, or residents, in the state action, might suffer. The following simple formula expresses expected losses,

$$E = P \times L$$

where expected losses (E) are a function of probability of loss (P) multiplied by the monetary loss to an individual that would occur (L). As stated above, only two percent of stolen credit card accounts are subject to fraudulent purchases.[121] If the criminal, on average, fraudulently charges $1000 to each affected individual, this results in only (0.02 x $1000), or $20 in expected losses per individual.

No individual plaintiff would pursue costly litigation to recover such a small amount. This small amount of potential liability, however, would be enough for the class action market to take notice.[122] A data breach that compromises a mere two million accounts would yield $40 million in potential damages if all the plaintiffs could be joined – certainly enough liability exposure to attract a few class litigators. The possibility of a class action increases the likelihood of litigation and the resulting deterrent effect on the retailer.

Determining the extent of the violation, or how many accounts were compromised, may take time, but companies can arrive at reasonable

---

[121] Lohr, *supra* note 10.

[122] RICHARD A. EPSTEIN, MANHATTAN INSTITUTE FOR POLICY RESEARCH CLASS ACTIONS: THE NEED FOR A HARD SECOND LOOK¸ MANHATTAN INSTITUTE FOR POLICY RESEARCH 1 (2002), *available at* http://www.manhattan-institute.org/pdf/cjr_04.pdf ("Nor is it hard to see why class actions have surged to prominence in recent years. As litigation becomes ever more complex, the willingness and ability of individual plaintiffs to bear its costs is correspondingly diminished. The opportunities for gains, however, remain substantial, so the void is quickly filled by entrepreneurial lawyers who hope to profit by organizing a class of potential plaintiffs and bringing their joint claim to a successful conclusion.").

estimates.[123] Database administrators from the affected retailer, having implemented some measure of database logging, might be able to shed some light on how many accounts had been compromised.[124] These experts could pour over computer logs to determine the extent of the security violation. In the absence of direct evidence, a court could presume that all accounts were affected, or even just a small percentage.[125]

It would be much more difficult to determine the probability of loss. Though we know that, on average, only two percent of compromised accounts are used illicitly,[126] each individual case will vary. Some hackers may not intend to use the information illicitly at all, some may sell the account information to dozens of buyers, and still more will lie somewhere in the middle.[127] Most of the information will be useless and incapable of fraudulent use, especially because banks will have already closed many of the compromised accounts.[128] While experts could estimate probabilities of loss based on national trends, sophistication of attack, or intent (in cases where the perpetrator is identified), these values would remain highly speculative. Estimating monetary loss presents similar difficulties.[129] An even greater problem is posed by the unsettled nature of the crime. While litigation is ongoing, the variables change as more accounts are accessed and fraudulently charged.[130] Expected damages

---

[123] TJX originally estimated the number of compromised accounts at 45.7 million, only to increase this figure to 94 million seven months later. Mark Jewell, *Extent of TJX Credit Breach Grows Larger*, WASHINGTON POST, Oct. 25, 2007, at D02, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2007/10/24/AR2007102402434.html.

[124] This was not the case in the TJX incident. One "TJX consultant said that 'he had never seen such a void of monitoring and capturing via logs activity at a Level One merchant as he saw at TJX.'" Evan Schuman, *TJX Intruder Moved 80GB of Data Without Detection*, EWEEK.COM, Oct. 25, 2007, http://www.eweek.com/c/a/Security/TJX-Intruder-Moved-80GB-of-Data-Without-Detection.

[125] According to a Ponemon Institute study, an average of 26,300 user account are compromised per breach. Shamus McGillicuddy, *Data breach costs rise, drive security spending*, SEARCHDATAMANAGEMENT.COM, Nov. 15, 2006, http://searchdatamanagement.techtarget.com/news/article/0,289142,sid91_gci1230326,00.html.

[126] Lohr, *supra* note 10.

[127] *See Meet the Hackers*, BUSINESSWEEK.COM, Mar 29, 2006, http://www.businessweek.com/magazine/content/06_22/b3986093.htm.

[128] Evan Schuman, *The Forensic Felons: The Next Generation of Cyber Thieves*, EWEEK.COM, Apr. 13, 2007, http://www.eweek.com/c/a/Security/The-Forensic-Felons-The-Next-Generation-of-Cyber-Thieves ("Javelin Strategy & Research, for example, estimates that in any large-scale attack, 99.2 percent of the numbers accessed will *not* be usable to the thieves.").

[129] A Ponemon Institute research study estimated that monetary loss per lost customer record is around $182. McGillicuddy, *supra* note 125.

[130] *See* Jewell, *supra* note 123.

become even more difficult to estimate when the injuries are ongoing. Given the small awards to individual plaintiffs and difficulties estimating expected losses, this method of calculating damages seems untenable.

2. Credit Monitoring Costs

Credit monitoring is a service that alerts consumers to changes in their credit rating.[131] Consumers can buy these services for as low as ten dollars per month.[132] At first blush, this solution seems like a good fit since it could prevent future account misuse. Unfortunately, like expected losses, this approach makes damages difficult to calculate.

The most prominent problem is determining how long credit monitoring should continue.[133] Long after banks reissue credit cards, other compromised personal information may be used to cause damage to a consumer's credit.[134] Retailers cannot be expected to pay for credit monitoring indefinitely. Since credit damaging incidents may occur years after the information has been exposed, short-term credit monitoring may not be enough, and hence, this solution also falls short.

3. Statutory Schedule of Damages

These actions could also include a schedule of fines to impose upon negligent retailers. The fines would be set to impose a suitable punishment based upon the retailer's size and the number of accounts compromised by the breach.[135]

The size of the company is an important factor to weigh when drafting the different levels of fines. Because deterrence is the primary motive for such reform, larger companies should suffer greater losses than smaller companies. Since states have an interest in cultivating small business,[136] in most cases, the damages awarded against a smaller business should not be so large as to shut them down. The damages award should be enough to sting, thereby

[131] Professor Johnson analogizes security monitoring costs to medical monitoring costs in toxic exposure cases. Johnson, *supra* note 25, at 305-09.

[132] Equifax.com charges $9.95/month for their most basic plan. Equifax, Equifax Credit Watch Gold, http://www.equifax.com/credit-watch-gold/ (last visited Feb. 18, 2008).

[133] A recent TJX settlement proposal offered three years of credit monitoring to affected customers. Robert Vamosi, *TJX agrees to settlement in class action suits*, CNET NEWS, Sept. 25, 2007, http://news.cnet.com /8301-10784_3-9784465-7.html.

[134] Andrew K. Burger, *The Cost of ID Theft, Part 1: Beyond Dollars and Cents*, TECHNEWSWORLD, Feb. 5, 2008, http://www.technewsworld.com/story/61515.html ("Eighteen percent of respondents in 2004 said that it took them four years or more to discover that their identities had been misused, a 100 percent increase from 2003.").

[135] ARIZ. REV. STAT. § 44-7501(H)(2009) (setting fine at $10,000 per breach incident).

[136] Massachusetts is but one state with agencies directed to support small businesses within its borders. *See* Massachusetts Small Business Development Center Network, http://www.msbdc.org (last visited Feb. 20, 2009).

encouraging proper security measures. It may make some sense to award damages roughly equal to the probable cost of such security enhancements.[137] A company faced with paying an equal amount in either damages or security measures would almost always prefer spending on security.

The number of compromised accounts should also be taken into consideration. The more accounts a company collects, the greater the potential injury to customers in general. As the risk of greater injury grows, so does the need for stronger security measures to avoid the risk. Though most small businesses will suffer lower damages due to their size, those involved in maintaining large collections of consumer accounts should be exposed to greater liability. This approach should limit the number of compromised accounts overall.

D. Determining the Standard of Care

Both statutory solutions outlined above will have to set a reasonable level of security the retailer must take in maintaining its collections of personal information. Retailers who lose information and fall below this threshold will be subject to liability. The level of care imposed on retailers is pivotal because it will determine how many data breach incidents are subject to the statutory civil action. There are several common ways to establish this level of care. This portion will explore strict liability and negligence. Subsections within the discussion of negligence will consider application of the Hand Formula as well as industry custom.

1. Strict Liability

Strict liability imposes tort liability even when there is no fault.[138] Where strict liability is appropriate, plaintiffs only need show that the defendant had acted in a certain manner that caused the plaintiff's harm.[139] This level of absolute liability is typically applied to torts where evidence of negligence is particularly difficult to recover, the activity is not beneficial to the surrounding community at-large, the activity will likely cause great harm, the activity is inappropriate to the place where it is being carried out, and an inability on the part of the defendant to eliminate risk of injury by any amount of care.[140] Since all resultant injury will be costly to a defendant, strict liability imposes a heavy tax on the activity, and most parties engaged in the activity will seek other means to accomplish the task (or will avoid the activity altogether).[141]

The classic example of strict liability's application in tort law is explosive

---

[137] Such an approach is consistent with optimal deterrence in tort law, where the monetary cost of risking losses is roughly equal to the monetary cost of risk of outright prevention. ABRAHAM, *supra* note 57, at 16.

[138] *See id.* at 166.

[139] *See id.*

[140] RESTATEMENT (SECOND) TORTS § 520 (1977); ABRAHAM, *supra* note 57, at 178.

[141] ABRAHAM, *supra* note 57, at 171-72.

blasting.[142] When injury occurs, there is rarely evidence of negligent behavior, since whatever evidence had existed is likely blown to pieces.[143] It is nearly impossible to conduct blasting in a safe manner.[144] The activity is inherently dangerous and almost always results in serious harm.[145] Finally, blasting is hardly ever a common activity in a community.[146] As a result of these factors, those responsible for blasting are subject to strict liability in tort.[147]

For several reasons, strict liability is not appropriate for improper handling of personal information. Primarily, evidence of how the company handled information may be readily available in computer logs.[148] Investigation of the retailer's security procedures prior to the invasion could also yield important evidence of careless behavior.[149] There is also no guarantee that security breaches will cause great harm.[150] Indeed, as we are so often told by courts, very little harm occurs in most cases.[151] Finally, and most importantly, proper security measures can avoid or at least seriously lower the risk of theft by hackers.[152]

Strict liability is not the best way to compel retailers to adopt proper security measures. Because strict liability's tax on activity is so great, it may force these businesses to avoid engaging in electronic commerce altogether. This is not the best result for consumers or the economy in general.

---

[142] *See* Spano v. Perini Corp., 250 N.E.2d 31 (N.Y. 1969).

[143] Some courts will consider whether the activity tends to destroy evidence of negligent conduct. If so, forcing a plaintiff to produce such evidence may be too great a burden and strict liability will relieve them of this standard requirement for negligence. *See* Ind. Harbor Belt R.R. Co. v. Am. Cyanamid Co., 916 F.2d 1174, 1178 (7th Cir. 1990) (citing Siegler v. Kuhlman, 502 P.2d 1181, 1185 (Wash. 1972)).

[144] *See* RESTATEMENT (SECOND) TORTS § 520(c) (1977).

[145] *See id.* at § 520(a).

[146] *See id.* at § 520(d).

[147] *See Spano*, 250 N.E.2d 31.

[148] This may not always be the case. Smarter cyber criminals are adept at hiding their tracks by erasing logs of their activity. Schuman, *supra* note 128 ("Bryan Sartin, a vice president of investigative response for Cybertrust, said the new breed of cyber thief will delete their tracks and often purposely soil the crime scene, by perhaps using their own encryption to make transaction logs unreadable.").

[149] Some PCI auditors look back for practical lessons from the TJX security breach. Bill Brenner, *PCI DSS auditors see lessons in TJX data breach*, SEARCHSECURITY.COM, Mar. 1, 2007, http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1245727,00.html. The PCI-DSS security guidelines are discussed *infra* Part III.D.2.b.

[150] Lohr, *supra* note 10.

[151] *See Pisciotta*, 499 F.3d at 639.

[152] One such set of security standards are the PCI-DSS guidelines, discussed *infra* Part III.D.2.b.

2. Negligence

Negligence imposes liability when the defendant has a duty to the plaintiff, breaches that duty, and causes harm to a plaintiff resulting in damages.[153] There are many different ways to calculate the duty, or reasonable level of care, a defendant owes to a plaintiff, including the Hand Formula and industry custom.[154]

i. The Hand Formula

Judge Learned Hand presented the now-famous Hand Formula in *U.S. v. Carroll Towing Co.*[155] Evaluating liability when a ship breaks-away from her lines, Judge Hand claimed that there were three variables at play when determining whether her owner was at fault: "(1) The probability that she [the boat] will break free; (2) the gravity of the resulting injury if she does; (3) the burden of adequate precautions."[156] According to Judge Hand, if the expected injury outweighs the burden of taking precautionary measures, then the defendant has a duty to take that precautionary measure.[157] His legal algebra comes together in the following inequality,

$$B < PL$$

where (B) is burden of taking adequate precautions, (P) is the probability the injury will occur, and (L) is the amount injury if it does.[158] (P) and (L) together represent the expected cost of injury caused by the activity. Over time, this formula has proven very popular and has been cited in a number of judicial opinions and law review articles.[159]

The usefulness of this formula in data breach cases depends on our ability to estimate its variables properly.[160] The burden of installing the proper security measures (B) should be easily quantified because a multitude of security consulting firms are in the business of producing these estimates.[161] The

[153] *See* ABRAHAM, *supra* note 57, at 47-48.

[154] *Id.* at 47-85.

[155] U.S. v. Carroll Towing Co., 159 F.2d 169 (2d Cir. 1947).

[156] *Id.* at 173.

[157] *Id.*

[158] *See id.*

[159] TORTS STORIES 11 (Robert L. Rabin & Stephen D. Sugarman eds., Foundation Press 2003) ("Judge Learned Hand's opinion in *United States v. Carroll Towing Co.* has been cited in scores of judicial decisions and hundreds of law review articles . . . ."). This author is proud to continue this venerable tradition.

[160] ABRAHAM, *supra* note 57, at 66-67 ("[T]he factors that make up the negligence calculus are likely in most cases to be difficult to quantify, let alone to compare with each other. Statistics about the probability of particular kinds of injury in particular situations are generally not available, and when such statistics are available, their relevance is debatable and their implications are complex.").

[161] Accenture is one example of such a firm. Accenture Network Security, http://www.accenture.com/Global/Technology/Infrastructure_Solutions/Security_Solutions/

probability of personal information being exposed (P) may be quite high. Nearly one in four Americans will have their data exposed each calendar year.[162] A prominent security company has claimed that 77% of its clients are insecure when consultation begins[163] and as many as 75% of all online retailers are vulnerable.[164] The likelihood of a security breach is a difficult figure to estimate and depends upon the specific facts of each case. Stuart E. Schechter, one of many academics suggesting methods of estimation, has proposed a more economic approach to calculating this risk.[165] Schechter believes risk should be calculated by accounting for the number of potential hackers, the level of incentive to attack, the risk to a hacker of getting caught, and the expected costs a hacker would have to incur to launch a successful attack.[166] In the end, however, if the probability of personal data exposure is very high, almost any formulation of injury will tilt the formula towards finding liability.

Since this Note is proposing a new form of injury,[167] the total amount of resultant injury (L) is subject to the several damage calculations detailed above.[168] If damages are determined by expected losses,[169] which grow quickly when hackers steal numerous accounts, then a company with a large database of personal information would face a tremendous financial burden of installing satisfactory security measures. If damages are estimated based on security monitoring costs,[170] the key question would be just how long defendants should pay for the monitoring costs. If they are forced to continue payment for a substantial amount of time, then these costs may be even greater than the costs of implementing proper security. The last measure of damages asked the state to set statutory amounts.[171] In that case, the estimates on potential injury are most exact, because the state provides the figures. Everything would depend upon how the state prepares its schedule of damages.

If the expected cost of the breach is very high,[172] then, under the Hand

(last visited Mar. 28, 2008).

[162] Lohr, *supra* note 10.

[163] Jack M. Germain, *Hacker Safe: The Security of Online Commerce*, TECHNEWSWORD, Apr. 29, 2004, http://www.technewsworld.com/story/33567.html.

[164] Alan Rimm-Kaufman, *Hacker Safe's Ken Leonard: 75% Of Online Retail Sites Insecure*, THE RIMM-KAUFMAN GROUP, Oct. 3, 2007, http://www.rimmkaufman.com/rkgblog/2007/10/03/hacker-safer.

[165] Stuart E. Schechter, *Toward Econometric Models of the Security Risk from Remote Attack*, IEEE Security and Privacy, vol. 3, no. 1, 40-44 (Jan.-Feb. 2005), *available at* http://www.eecs.harvard.edu/~stuart/papers/eis04.pdf.

[166] *Id.* at 41.

[167] *See supra* Part II.A.

[168] *See supra* Part III.C.

[169] *See supra* Part III.C.1.

[170] *See supra* Part III.C.2.

[171] *See supra* Part III.C.3.

[172] *See* Germain, *supra* note 163; Rimm-Kaufman, *supra* note 164.

Formula, the level of care would be likewise extremely high. As a result, the law would force most retailers to adopt expensive network security measures. If so, the Hand Formula would yield the same result as imposing strict liability.[173] This Note rejected the imposition of strict liability, since it might deter businesses from engaging in electronic commerce altogether. If the risks of injury are very low, however, the Hand Formula may be useful in setting a more reasonable level of care.

ii. Industry Custom

Current industry standards could determine the standard of care. In other words, the current industry standards for network security could determine the reasonable precautions a defendant should take to protect personal data. Industry custom is still accepted in courts, but it does not carry the weight it had historically.[174]

The major credit card companies[175] have teamed-up to deliver a single set of security standards for online retailers, the Payment Card Industry Data Security Standard ("PCI DSS").[176] More than 400 organizations have already applied the PCI DSS to their sites[177] since its creation in January 2005.[178] The PCI DSS enumerates twelve security requirements,[179] which outline the proper measures that any business collecting personal information should employ.[180] A closer examination of these general requirements will give more detail to the standard of care this industry currently expects of itself.

---

[173] *See supra* Part III.D.1.

[174] *See* The T.J. Hooper, 60 F.2d 737, 740 (2d. Cir. 1932) (rejecting industry custom as a total defense, "there are precautions so imperative that even their universal disregard will not excuse their omission"); ABRAHAM, *supra* note 58, at 68 ("Evidence of non-compliance can be used as a sword [by plaintiffs], and evidence of compliance with custom may be used as a shield [by defendants]. This evidence is relevant and admissible, but it is not dispositive. That is, even in the face of uncontradicted evidence of party's compliance or non-compliance with custom, the jury may find that the party's action was or was not negligent.").

[175] The founding companies include American Express, Visa, MasterCard, Discover, and JCB. PCI Security Standards Council, https://www.pcisecuritystandards.org/ (last visited Feb. 20, 2009).

[176] The latest version of the standard, version 1.2, is available online. PCI Security Standards Council, The Payment Card Industry (PCI) Data Security Standard, Oct. 2008, *available at* https://www.pcisecuritystandards.org/security_standards/download.html?id=pci_dss_v1-2.pdf [hereinafter *PCI Data Security Standard*].

[177] PCI Security Standards Council, Participating Organizations, https://www.pcisecuritystandards.org/participation/member_list.html (last visited Feb. 20, 2009).

[178] *See* PCI Security Standards Council, *supra* note 175.

[179] *PCI Data Security Standard* at 3.

[180] *Id.* at 13-16.

The PCI DSS first requires that every personal data-collecting site build and maintain a secure network.[181] This requires building and maintaining a firewall between the site's internal computers and the external internet.[182] Network administrators should place all machines containing personal data behind this firewall,[183] and all computer addresses behind the firewall should be kept secret from the outside world.[184]

Though it may seem obvious, the PCI DSS warns network administrators to change all default passwords on security software and hardware, since hackers will be familiar with default installations.[185] Wireless access points, for example, often come out of the box unsecured.[186] Further, hackers can exploit a multitude of network protocols that are enabled by default, but are not necessary for all applications.[187] Network administrators should disable any unnecessary protocols before putting network hardware to use.[188]

The PCI DSS requires special protection for sensitive customer information.[189] The standards suggest that retailers should never store ancillary credit card authentication information, such as the card-validation code[190] or personal identification (PIN) numbers for ATM cards.[191] When a customer returns to the site to order again, the site should only display the last four digits of the user's credit card number.[192] To ensure even more security, network architects should encrypt all credit card numbers, even at the database level, to

[181] *Id.* at 13.

[182] *Id.* ("Firewalls are computer devices that control computer traffic allowed between a company's network (internal) and untrusted networks (external), as well as traffic into and out of more sensitive areas within a company's internal trusted network. The cardholder data environment is an example of a more sensitive area within the trusted network of a company.").

[183] *Id.*

[184] *Id.* at 16.

[185] *Id.* at 17 ("Malicious individuals (external and internal to a company) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known by hacker communities and are easily etermined via public information.").

[186] Jack M. Germaine, *The Woes of WiFi, Part 1: Insecure by Default*, LINUXINSIDER, Aug. 11, 2007, http://www.linuxinsider.com/story/58757.html?welcome=1203187989 ("According to a recent study by Adjunct Professor Rajiv Shah from the University of Illinois at Chicago, an alarming 96 to 99 percent of wireless users accept the default network settings created by manufacturers without attempting network encryption. The 'default' setting exposes users' networks to freeloaders in their proximity.").

[187] *PCI Data Security Standard* at 18.

[188] *Id.*

[189] *Id.* at 20.

[190] The 3-digit code on the back of most credit cards.

[191] *PCI Data Security Standard* at 22.

[192] *Id.*

protect them from employees or hackers with access to the database.[193] Retailers should also keep the accompanying encryption keys safe by restricting them to only a few employees.[194] Network administrators should employ procedures that periodically create new keys and destroy old ones in an appropriate manner.[195] In addition to personal information stored in the database, all personal information traveling across the network should be encrypted while in transit.[196]

Some computer and network viruses transmit personal information to the public.[197] As a result, system administrators should regularly update the anti-virus software on their machines.[198] Computer viruses, or hackers themselves, may exploit bugs in network hardware or software to steal private information.[199] Because of this threat, system administrators should also keep abreast of the latest patches for their network software and hardware.[200]

Businesses should restrict employee access to cardholder information.[201] Suggested restrictions include limiting the number of employees that can view the data,[202] assigning unique access passwords for each employee that accesses the data,[203] and logging all employee access to the data.[204] Finally, the PCI DSS advocates continued testing and inspection of security measures, as well as creating formal business policies to prevent employees from deviating from these accepted security practices.[205]

---

[193] *Id.* at 23.

[194] *Id.* at 24.

[195] *Id.* at 25.

[196] *Id.* at 26 ("Sensitive information must be encrypted during transmission over networks that are easily accessed by malicious individuals. Misconfigured wireless networks and vulnerabilities in legacy encryption and authentication protocols can be continued targets of malicious individuals who exploit these vulnerabilities to gain privileged access to cardholder data environments.").

[197] *Id.* at 28.

[198] *Id.*

[199] *Id.*

[200] *Id.* at 29 ("Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor-provided security patches, which must be installed by the entities that manage the systems. All critical systems must have the most recently released, appropriate software patches to protect against exploitation and compromise of cardholder data by malicious individuals and malicious software.").

[201] *Id.* at 35.

[202] *Id.*

[203] *Id.* at 37 ("Assigning a unique identification (ID) to each person with access ensures that each individual is uniquely accountable for his or her actions. When such accountability is in place, actions taken on critical data and systems are performed by, and can be traced to, known and authorized users.").

[204] *Id.* at 46.

[205] *Id.* at 46-58.

Unlike the other means of calculating the appropriate standard of care outlined above, guidelines like the PCI DSS present businesses and their network specialists with security concepts they can understand. Additionally, when in litigation, a jury will have an easier time evaluating whether a business took these practical precautions rather than a more abstract ideal. The risks associated with allowing businesses to determine their own levels of care are mitigated in this case because a commonly injured group, the credit card companies, is developing the standards to protect itself and, indirectly, their consumer customers. As technologies change and hackers adapt, standards like the PCI DSS will adjust to new threats. As a result of these positive considerations, industry standards like the PCI DSS are the most effective measurements of the appropriate level of care online businesses should employ to protect consumer information.

IV. CONCLUSION

As it stands today, two primary deterrents aim to prevent businesses from housing customer information in a negligent fashion: civil litigation and state statutory notification laws. Unfortunately, neither one effectively compels businesses to adopt adequate security measures capable of repelling sophisticated identity thieves. Litigation and notification laws do more to repair resulting damage to consumers and banks, while offering little in effective deterrence. New state legislation that recognizes a civil injury resulting from data breach incidents (the injury of personal data exposure) would produce better disincentives to businesses. In drafting this new civil action, state legislators have a wide array of options at their disposal. Smart legislators will favor setting the standard of care relative to current industry standards. They should also establish a statutory schedule of damages to apply when a defendant enterprise is found negligent. Forcing businesses to take customer information security more seriously would lower the likelihood of future data breaches and better protect consumers.