2008

Minnesota's PCI Law: A Small Step on the Path to a Statutory Duty of Data Security Due Care

James T. Graves

Follow this and additional works at: http://open.mitchellhamline.edu/wmlr

Recommended Citation
Available at: http://open.mitchellhamline.edu/wmlr/vol34/iss3/2

This Note is brought to you for free and open access by the Law Reviews and Journals at Mitchell Hamline Open Access. It has been accepted for inclusion in William Mitchell Law Review by an authorized administrator of Mitchell Hamline Open Access. For more information, please contact sean.felhofer@mitchellhamline.edu.
© Mitchell Hamline School of Law
NOTE: MINNESOTA’S PCI LAW: A SMALL STEP ON THE PATH TO A STATUTORY DUTY OF DATA SECURITY DUE CARE

James T. Graves†

I. INTRODUCTION ................................................................. 1115

II. THE FIRST STEP: DATA BREACH NOTIFICATION LAWS .......... 1118
    A. History and Features .................................................. 1118
    B. Data Breach Laws’ Inadequacies .................................. 1120
        1. Notification ......................................................... 1121
        2. Behavior Modification ........................................... 1122
        3. Cost Shifting ...................................................... 1125

III. THE NEXT STEP: PCI-BASED LAWS .................................. 1129
    A. Background: Payment Cards and PCI DSS ....................... 1129
    B. Minnesota’s Plastic Card Security Act .......................... 1131
        1. Summary and History ............................................. 1131
        2. General Features ................................................ 1133
        3. Improvement on Data Breach Notification Laws .......... 1135

IV. THE FINISH LINE: A STATUTORY STANDARD OF DATA SECURITY DUE CARE ............................................................ 1138
    A. Duty of Due Care ..................................................... 1138
    B. Implementation Details ............................................. 1142
        1. Statute of Limitations .......................................... 1142
        2. Proving Cause-in-Fact ......................................... 1144

V. CONCLUSION ..................................................................... 1145

I. INTRODUCTION

Since 2000, security breaches have exposed over two hundred million sensitive personal data records.† In 2006 alone, data

† J.D. Candidate 2010, William Mitchell College of Law; M.S., Information Networking, Carnegie Mellon University, 2004; B.S., Mathematics/Computer Science, Carnegie Mellon University, 1994. The author gratefully acknowledges advice from Professor J. David Prince, the efforts of William Mitchell Law Review staff and editors who worked on this note, and the patience and support of his wife.
handlers lost eighty-three million records.\textsuperscript{2} Lost data has become so common that a breach must now affect millions of records even to be newsworthy.\textsuperscript{3} One of the first widely publicized breaches, ChoicePoint’s 2005 disclosure of 163,000 consumer records,\textsuperscript{4} seems almost harmless compared to the breaches at TJX,\textsuperscript{5} Certegy,\textsuperscript{6} Circuit City,\textsuperscript{7} and the Department of Veterans Affairs,\textsuperscript{8} each of which lost millions of records.

Many states passed data breach notification laws in response to this problem.\textsuperscript{9} These laws require anyone handling personal data to notify people when their data might have been compromised.\textsuperscript{10} As of 2008, thirty-nine states and the District of Columbia have enacted data breach notification laws.\textsuperscript{11} These laws have increased the visibility of data breaches, but have not solved the underlying problem of poor data security.\textsuperscript{12}

Minnesota recently attempted to fill part of this gap with a law forbidding companies from storing sensitive credit card

\textsuperscript{2} U.S. GOV’T ACCOUNTABILITY OFFICE, GAO-07-737, PERSONAL INFORMATION: DATA BREACHES ARE FREQUENT, BUT EVIDENCE OF RESULTING IDENTITY THEFT IS LIMITED; HOWEVER, THE FULL EXTENT IS UNKNOWN 12 n.18 (2007) [hereinafter 2007 GAO REPORT].  This is a conservative estimate.  It does not include the breach of CardSystems’ database, for example, which may have compromised up to forty million records although a CardSystems official claimed that only 263,000 of those records included “sensitive personal information.”  See infra note 23.
\textsuperscript{3} Data handlers announced 346 data breach events in 2006—an average of almost one per day, with no more than six days between announcements.  See Attrition.org, Data Loss Database, http://attrition.org/dataloss/dldos.html (last visited Mar. 3, 2007).  At that rate, a newspaper would need a regular data breach column to report them all.
\textsuperscript{7} See Will Wade, Security Watch, AM. BANKER, Sept. 8, 2006, at 5.
\textsuperscript{8} See David Stout, Veterans Agency to Atone with Free Credit Monitoring, N.Y. TIMES, June 22, 2006, at A22.
\textsuperscript{10} Id.
\textsuperscript{11} See infra note 23.
\textsuperscript{12} See discussion infra Part II.
authorization data.\footnote{13} It adopted this requirement from a credit card industry standard called the Payment Card Industry Data Security Standard (PCI DSS).\footnote{14} PCI DSS sets specific technical and business process requirements for securing credit card data.\footnote{15} Anyone who “store[s], process[es], or handl[es]” credit card data must comply with PCI DSS.\footnote{16}

Minnesota’s law, however, raises some troubling issues. PCI DSS only addresses credit card data, and Minnesota adopted only one part of the standard.\footnote{17} Minnesota’s law provides remedies only to financial institutions, not consumers.\footnote{18} Some have argued that the law is unnecessary because PCI DSS is already a requirement for anyone who handles, processes, or stores credit card data.\footnote{19} This note examines these issues, argues that Minnesota’s law does not do enough to help consumers, and that Minnesota should fill this gap by adopting a statutory duty of due care for data security.

Part II of this note describes state data breach notification laws and explains why they do not adequately improve data security. Part III describes PCI DSS and then discusses Minnesota’s law and some of its features and problems. Finally, Part IV argues for a statutory duty of due care and addresses some features such a law should have.


\footnotetext[15]{See PCI DSS, supra note 14, at 1.}

\footnotetext[16]{Id. at 2.}

\footnotetext[17]{See discussion infra Part II.B.}

\footnotetext[18]{See id.}

\footnotetext[19]{See Nadia Oehlsen, Data Security is Fast Becoming a Matter of Law, Cards & Payments, Oct. 1, 2007, at 32, available at 2007 WLNR 20225381.}
II. THE FIRST STEP: DATA BREACH NOTIFICATION LAWS

A. History and Features

Some of the first broad legislative efforts to improve data security came in the form of security breach notification laws.\(^\text{20}\) California led the charge in 2002 by becoming the first state to pass a law requiring public disclosure of security incidents.\(^\text{21}\) Most states followed with similar laws of their own.\(^\text{22}\) As of January 2008, thirty-nine states and the District of Columbia had enacted data breach notification laws.\(^\text{23}\)

\(^\text{20}\) Other laws affecting data security at the time only apply to certain industries. For example, the Health Information Portability and Accountability Act (HIPAA) covers health care, and the Gramm-Leach-Bliley Act (GLBA) applies to financial institutions. See 45 C.F.R. § 160.102 (2007) (HIPAA applicability); 15 U.S.C. § 6802(a) (2000) (GLBA).


Data breach notification laws require organizations to notify data subjects whose personal data the organization reasonably believes has been obtained by a third party. Notification must generally be given in writing reasonably quickly after the breach is discovered, and many data breach notification laws establish penalties for non-compliance.

State data breach notification laws vary in their details, including the standards for notification, the types of personal data...
that trigger the laws, and the causes of action they allow. Critics cite this “patchwork” of state requirements as a major problem with data breach notification laws. Despite some arguments calling for a uniform national data breach notification standard, Congress has yet to pass such a law.

B. Data Breach Laws’ Inadequacies

Although data breach notification laws warn consumers that their data may be at risk from a breach, these laws do not solve the root problem of poor data security. A solution requires more than mere notice of a breach; it requires laws that encourage careful handling of data and compensate victims. Data breach laws fall short of these goals.

29. Personal data usually includes, at a minimum: names, account numbers, driver’s license numbers, and social security numbers. See, e.g., CAL. CIV. CODE. § 1798.82(c) (West Supp. 2007); MINN. STAT. § 325E.61, subdiv. 1(e) (2006).

30. Most states allow enforcement through state regulatory agencies or attorneys general. See, e.g., IND. CODE ANN. § 24-4.9-4-1(a) (West Supp. 2007); KAN. STAT. ANN. § 50-7a02(g) (Supp. 2006); MINN. STAT. § 325E.61, subdiv. 6 (2006); N.D. CENT. CODE § 51-30-07 (2007); OHIO REV. CODE ANN. § 1349.19(I) (West Supp. 2007). A few states allow private causes of action. See, e.g., LA. REV. STAT. ANN. § 51:3075 (Supp. 2007); WASH. REV. CODE ANN. § 19.255.010(10)(a) (West 2007).

31. See, e.g., Eric Friedberg & Michael McGowan, Lost Backup Tapes, Stolen Laptops, and Other Tales of Data-Breach Woe, 79 N.Y. ST. B.J. 42, 42 (Feb. 2007) (referring to the “patchwork of state data breach notification statutes”); Sean C. Honeywill, Data Security and Data Breach Notification for Financial Institutions, 10 N.C. BANKING INST. 269, 271 (2006) (calling the twenty-one state data breach notification laws in 2005 a “patchwork regulatory environment”). Because these laws typically apply to any person or organization that holds data about a person in that state, an interstate business must either monitor its compliance with a hodgepodge of state data breach laws or choose to comply with the broadest provisions of all of them. See, e.g., Ian C. Ballon, E-COMMERCE AND INTERNET LAW: TREATISE WITH FORMS § 4.09[1][A] (Supp. 2006) (noting that nationwide businesses need to consider which state laws apply to a particular breach and may choose to follow the broadest definition of “personal information” and use the most restrictive method of notification).


34. See RESTATEMENT (SECOND) OF TORTS § 901 (1979).
1. Notification

Data breach laws aim to notify consumers when their data might be at risk. The constant stream of breach announcements shows that, if nothing else, the laws do that much. Data breach notification laws force breached entities to warn people whose data may have been compromised, giving consumers the chance to protect themselves. Yet these announcements happen so frequently, they may have lost effectiveness. In one survey, almost forty percent of respondents said they mistook breach notification letters for junk mail.

Data breach notification laws are warnings that only require disclosure after something bad has happened. But warnings of any sort are ill-suited to fixing the data security problem because consumers have little or no control over how their data is handled.

Several years before his appointment to the Supreme Court, Justice Breyer offered a three-pronged test for determining when disclosure is an effective means of regulation. Disclosure works well only when the public (1) understands the information disclosed; (2) has a choice in the market; and (3) believes the information provided is relevant to that choice. The main problem with data breach notification is the second prong. Consumers inevitably have Social Security numbers, credit histories, bank accounts, and all the other bits of economic data flotsam. Breached data brokers, like ChoicePoint, never asked consumers if it could gather their data and consumers could do little to prevent it. Breach notification also fails the third prong of Justice Breyer’s test. After-the-fact notification of a breach does

35. See Schwartz & Janger, supra note 9, at 915–16.
36. See Attrition.org, supra note 3.
38. Id. at 916 (discussing criticisms that data breach notification laws create too many warning letters).
39. Id. at 952 (citing PONEMON INST., NATIONAL SURVEY ON DATA SECURITY BREACH NOTIFICATION 2–4 (2005)).
41. STEVEN G. BREYER, REGULATION AND ITS REFORM 164 (1982).
42. Id.
43. See Solove, supra note 40, at 1251–55.
nothing to help consumers choose to work with businesses who will be careful with their data.\textsuperscript{45}

2. *Behavior Modification*

A loftier goal for a data security law would be to make proper handling of data the financially prudent choice. Laws change behavior when the expected cost of non-compliance exceeds the cost of the desired behavior.\textsuperscript{46} Most organizations choose to invest in security measures when doing so is, predictably and measurably, less expensive than not doing so.\textsuperscript{47} A law seeking to encourage organizations to invest in security should therefore make the expected cost of a breach sufficiently large and predictable.

This model assumes rational actors with enough information to choose actions based on well-defined costs and benefits.\textsuperscript{48} Poor or incomplete information can lead to irrational choices. Put more succinctly: “Garbage in, garbage out.”\textsuperscript{49}

Most current information on the likelihood of security breaches is statistically indistinguishable from garbage.\textsuperscript{50} Current


\textsuperscript{46} See David Bender, *Privacy Developments—2005*, 842 PLI/PAT 9, 19 (2005) (applying Adam Smith’s “invisible hand” effect to say that companies implement the level of security they deem necessary to avoid making a breach announcement).


\textsuperscript{49} “Garbage in, garbage out” (or GIGO) is a phrase often used in computer science to capture the idea that a program cannot generate valid output from invalid data. See 2 *Oxford English Dictionary Additions Series* 114 (1993). Charles Babbage articulated the fundamental idea in the nineteenth century: “On two occasions I have been asked, ‘Pray, Mr. Babbage, if you put into the machine wrong figures, will the right answers come out?’ . . . I am not able rightly to apprehend the kind of confusion of ideas that could provoke such a question.” Charles Babbage, *Passages from the Life of a Philosopher* 67 (1864).

data security studies have serious methodological problems, oversimplify, or do not claim to provide predictive data. Without this data, the probability of a security event and its financial impact are unknown. An organization’s practices regarding uncertainty, therefore, dominate its approach to data security. Organizations that are risk-averse will over-spend on security, those that seek risk will under-spend on security, and the risk-neutral will fall in a random distribution somewhere in the middle.

Organizational decisions also depend on the relative value of hard and soft dollars. Hard dollars count directly and measurably against an organization’s budget, while soft dollars involve

---


51. An oft-quoted survey in the computer security industry is the annual Computer Security Institute (CSI) Security Survey. See COMPUTER SECURITY INST., 2007 CSI COMPUTER CRIME AND SECURITY SURVEY (2007), available at http://gosci.com/forms/csi_survey.jhtml (registration required). The CSI survey’s ten percent response rate and sample bias (self-selecting CSI members and conference attendees) cast doubt on its results. See id. at 3. The latest survey’s introduction acknowledges these limitations, calling the survey “informal.” Id. at 2. However, the survey notes that “almost all financial information about [computer] crime losses are estimates.” Id. at 3. The survey is nonetheless popular with security vendors, who tend to use the survey’s bullet-point findings in their marketing materials while conveniently ignoring its self-confessed limitations. See, e.g., Ira Winkler, Time to End the FBI/CSI Study?, COMPUTERWORLD, Sept. 26, 2006 (discussing the CSI study’s misuses and statistical problems).

52. One survey, for example, found that the average cost to organizations of a data breach was $197 per record. See PGP CORP. & VONTU, INC., 2007 ANNUAL STUDY: U.S. COST OF A DATA BREACH 2 (2006), available at http://www.pgp.com/downloads/research_reports/ponemon_reg_direct.html (registration required). If it were that simple, TJX’s breach of over forty-five million records would cost them $9 billion. See Byron Acohido & Jon Swartz, TJX Discloses Largest Data Theft: 45.7M Customers, USA TODAY, Mar. 30, 2007, at 3B.

53. For example, Carnegie Mellon’s CERT publishes numbers of reported security incidents, but makes no claim that these incidents reflect the number of actual incidents. See CERT, CERT Historical Statistics, http://www.cert.org/stats/historical.html (last visited Jan. 29, 2008).

54. See SOO HOO, supra note 50, at 9.

55. Confirmation biases would lead organizations to make guesses or select data based on existing beliefs. See Hoffman & O’Shea, supra note 48, at 361.

56. Being risk averse, these organizations may overspend on security—a problem that may not worry consumers but hampers economic efficiency.

57. See Hoffman & O’Shea, supra note 48, at 361 (discussing confirmation biases); Schwartz & Janger, supra note 9, at 928 (noting that organizations can inaccurately calculate data security investment costs and benefits).
distributed, indirect, or immeasurable costs.\textsuperscript{58} Equipment purchases and labor expenses, for example, are both hard-dollar costs.\textsuperscript{59} Productivity savings are soft-dollar gains.\textsuperscript{60} Security investments almost always combine hard-dollar costs with soft-dollar savings.\textsuperscript{61} Many organizations favor hard-dollar savings over soft dollars, creating an internal exchange rate in which multiple soft dollars must be saved to justify spending a hard dollar.\textsuperscript{62} Data breach notification laws may increase potential (i.e., soft-dollar) losses, but they do not make those dollars any more concrete at the time security investment decisions are made.

Notification laws have secondary effects that improve security somewhat. Publicity resulting from a large data breach can affect public perception, profits, stock prices, and jobs.\textsuperscript{63} These secondary effects encourage careful data handling only to the extent that they are significant and predictable. Unpredictable, poorly estimated, or trivial costs fail to improve security because organizations cannot use them to create realistic cost-benefit comparisons.

Data breach laws also increase costs to breaching organizations through the laws’ requirements for notifying the Federal Trade Commission (FTC) in the event of a breach. The FTC can then file suit without meeting the same burden of harm and cause-in-fact that an individual would require,\textsuperscript{64} and through civil actions and

\textsuperscript{59} Id.
\textsuperscript{60} Id.
\textsuperscript{61} For example, security improvements require devoting resources to hardware, software, or process development—hard dollar costs—in return for an unknown decrease in the risk of a possible future security vulnerability with unknown impact.
\textsuperscript{62} To many, soft dollars do not count as real dollars. See Mark Ousnamer, Hide-and-Seek Cost Justification, IIE SOLUTIONS, Jan. 2002, at 22.
\textsuperscript{63} For example, after it suffered a security breach in 2005 affecting forty million credit and debit cardholders, CardSystems lost its contract with Visa to process credit cards and then declared bankruptcy in 2006. Shanon D. Murray, CardSystems Files Liquidation Plan, DAILY DEAL, May 17, 2006, available at 2006 WLNR 8444298. The repercussions for executives and managers at AOL and Ohio University were more personal; they lost their jobs after data breach events. See Ann Bednarz & Denise Dubie, IT Execs Feel the Heat As Security Woes Multiply, NETWORK WORLD, Aug. 28, 2006, at 1.
\textsuperscript{64} Consumer suits require showing that the consumer was individually harmed as a result of the breach, but the FTC has a cause of action on behalf of all consumers over unfair acts or trade practices under the Federal Trade Commission Act of 1914. See Schwartz & Janger, supra note 9, at 921–22.
consent decrees, it can levy fines and require improvements in security procedures.\textsuperscript{65} The FTC has exercised this right in a number of cases.\textsuperscript{66} Although FTC notification requirements raise the probable costs of a security incident, they do not improve those costs’ predictability.

3. \textit{Cost Shifting}

For most owners of large databases, the risk of poor data security is a negative externality.\textsuperscript{67} The data subject bears the primary risk of data loss but has no ability to protect her own data.\textsuperscript{68} The database owner can protect the data but may not have economic incentives to do so.\textsuperscript{69} By shifting costs of a breach from consumers to database owners, laws can internalize those externalities.\textsuperscript{70} Current data breach laws do little or nothing to shift these costs.\textsuperscript{71} Their textual provisions rarely provide direct compensation to data subjects,\textsuperscript{72} and consumer efforts to recover in court have usually failed.

Lawsuits following major data breaches show that courts are not willing to entertain causes of action for harm from a breach. The main problem is the difficulty of showing actual harm and cause-in-fact.\textsuperscript{73} Common law negligence and constitutional standing require plaintiffs to suffer genuine harm from the


\textsuperscript{68} See Solove & Hoofnagle, \textit{supra} note 44, at 362–66.

\textsuperscript{69} See discussion \textit{supra} Part II.B.2.

\textsuperscript{70} See Goldberg, \textit{supra} note 47, at 545.

\textsuperscript{71} It has, however, become “standard industry practice” for companies to offer free credit monitoring after a breach, even when applicable data breach notification laws do not require it. 2007 GAO REPORT, \textit{supra} note 2, at 35.


defendant’s alleged conduct. A plaintiff in a data-breach case must prove that (1) her data was among that stolen in a data breach, (2) she experienced an actual identity theft or other hardship, and (3) the theft was a result of the data breach and not some other cause. Because of the difficulties in proving these elements, courts hearing post-breach lawsuits rarely reach questions of due care.

Cause-in-fact is difficult to prove in data breach cases. People who steal mass amounts of data usually do not use the data themselves but sell it to others. Police often cannot find the perpetrators of individual-level fraud. These factors can prevent identity fraud victims from tracing the misused data back to a data breach. The law in this area, however, is still developing. For

74. See Lujan v. Defenders of Wildlife, 504 U.S. 555, 560–61 (1992) (listing three elements for constitutional standing: injury-in-fact; a causal connection between the injury and the conduct complained of; and an injury that is likely to be redressed by a favorable decision); Restatement (Second) of Torts § 281 (1965) (listing the elements for a negligence cause of action).


76. See Steve Lohr, Surging Losses, But Few Victims, N.Y. TIMES, Sept. 27, 2006, at G1 (discussing recent breaches involving mass amounts of stolen data).

77. See Erin Dowe, Frustration Station: Attempting to Control Your Credit, 16 Geo. Mason U. Civ. RTS. L.J. 359, 362–63 (2006) (noting that identity fraud offenders remain uncaught “more often than not” and that the remoteness of fraud makes perpetrators hard to catch).

78. One successful investigation shows how far stolen data can travel before it is used. In June, 2007, authorities arrested four people in Florida in connection with the TJX and Polo Ralph Lauren breaches. See Larry Greenemeier, Arrests in TJX Case—Data Theft’s Long Tentacles, INFO.Wk., July 16, 2007, at 20. The data used by the Florida men to create counterfeit credit cards came from Cuban nationals in a fraud ring, who bought the numbers from criminals in Eastern Europe. Id.
example, in Stollenwerk v. Tri-West Healthcare Alliance, a plaintiff suffered $7,000 in actual damages from “unknown individuals” who opened accounts in his name.\textsuperscript{79} Because the plaintiff had shared his address and Social Security number with others, the district court held that he could not prove cause-in-fact.\textsuperscript{80} A Ninth Circuit Court of Appeals panel reversed, holding that the possible causal relationship between the breach and the identity theft allowed the case to survive summary judgment.\textsuperscript{81}

The need to show actual damages has generated some novel theories of harm. Plaintiffs have tried to claim damages for the costs of credit monitoring and other preventive measures.\textsuperscript{82} Courts have rejected these claims, finding that the costs have been incurred in mere anticipation of possible future harm.\textsuperscript{83} Given the lack of other direct, measurable harms from data breaches,\textsuperscript{84} plaintiffs continue to test the boundaries of damage theories.\textsuperscript{85}

\textsuperscript{80} Id. at *7.
\textsuperscript{81} Stollenwerk v. Tri-West Health Care Alliance, No. 05-16990, 2007 WL 4116068, at *3–4 (9th Cir. Nov. 20, 2007).
\textsuperscript{83} See e.g., Kahle, 486 F. Supp. 2d at 709–13 (holding the cost of credit monitoring after a breach unrecoverable because it was incurred in anticipation of future injury); Hendricks, 444 F. Supp. 2d at 780 (rejecting cost of credit monitoring after a data breach as a theory for recovery); Guin v. Brazos Higher Educ. Serv. Corp., No. Civ. 05-668 RHK/JSM, 2006 WL 288483, at *6 (D. Minn. Feb. 7, 2006) (holding that the threat of future harm does not meet the damage requirement necessary to bring an action for negligence).
\textsuperscript{84} The biggest problem with a data breach is the risk that the compromised data will be misused. Until misuse has happened, however, breach victims’ direct costs consist of time, effort, and money spent responding to the breach, purchasing credit monitoring services, freezing their credit records, or consulting experts on other options for protecting themselves. See Ponemon Inst., National Survey on Data Security Breach Notification 17 (2006). http://www.whitecase.com/news/detail.aspx?news=670 (follow “click here” hyperlink near the end of the page).
\textsuperscript{85} These claims bear a remarkable similarity to the enhanced-risk and medical monitoring claims sometimes seen in toxic tort cases. Enhanced risk is controversial even in that context, where the risk is of death or serious disease. See Bill Charles Wells, The Grin Without the Cat: Claims for Damages from Toxic Exposure Without Present Injury, 18 WM. & MARY J. ENVTL. L. 285, 328–29 (1994). Courts seem unlikely to soon allow enhanced risk theories of harm for the relatively trivial
Banks have fared no better than consumers in their attempts to recover data breach costs. Some of the most notable litigation in this area resulted from a data breach incident at BJ's Wholesale Club in Pennsylvania.⁸⁶ The facts of the case tell a typical story: poor security practices at BJ's allowed third parties to access full magnetic stripe data for members' credit cards.⁸⁷ After some of these card numbers were used to rack up millions of dollars in fraudulent charges,⁸⁸ Pennsylvania State Employees Credit Union (PSECU) reissued over twenty thousand credit cards.⁸⁹ It then sued BJ's and BJ's acquiring bank⁹⁰ for the cost of reissuing the cards, claiming negligence and breach of contract as a third party beneficiary.

The federal district court rejected all of PSECU’s claims.⁹² It held that the economic loss doctrine barred PSECU’s tort claims.⁹³ It also dismissed PSECU’s claims for breach of contract, equitable indemnification, and unjust enrichment.⁹⁴ In a later decision, the court also rejected the remaining third party beneficiary claim.⁹⁵

The failure of post-breach lawsuits illustrates how little the data breach notification laws do to compensate victims of data breach. Courts are reluctant to classify immediate post-breach costs as harms. Even with more serious later harms that exploit breached data, the difficulty of showing cause-in-fact makes it nearly impossible for those harmed to recover from the organization whose mishandling of data predicated the problem.

financial harms that result from data breaches. See also Pisciotta, 499 F.3d at 638–39 (comparing claims for credit monitoring to requirements for recovery in toxic tort risk cases).

⁸⁷. Id. See also discussion supra note 13.
⁹⁰. Id. An “acquiring bank” processes credit card transactions for a merchant. See discussion infra Part III.A.
⁹². Id. at 327–31. The economic loss doctrine prevents recovery in tort for economic damages unless there is damage to the plaintiff's person or property. See Restatement (Third) of Torts: Prod. Liab. § 21 (1998).
III. THE NEXT STEP: PCI-BASED LAWS

In light of cases such as BJ’s Warehouse, and given continuing data breach announcements, existing data breach notification laws clearly were not enough to stop mishandling of personal data. Minnesota’s legislature saw a possible solution in the Payment Card Industry Data Security Standard. To explain why PCI DSS was perceived as a possible solution, this section first describes the payment card industry and the role of PCI DSS within it. Such information provides the necessary background for the ensuing discussion of Minnesota’s law.

A. Background: Payment Cards and PCI DSS

The Visa and MasterCard payment brands are incorporated as associations of financial institutions.96 These institutions consist of “issuers” and “acquirers.”97 “Issuers” issue credit cards to consumers while “acquirers” process credit card transactions for merchants.98 When a customer makes a credit card purchase, the merchant’s acquirer clears the transaction with the customer’s issuer, who charges the purchase against the customer’s account.99

The relationships between banks, merchants, and the card associations rely on a web of contracts. Contracts exist between merchants and their acquirers and between cardholders and their issuers.100 The issuer and acquirer each hold contracts with the payment brand association through their membership

98. See id. at *2 (discussing Visa’s relationship with the plaintiff and defendant financial institutions).
100. See Pa. State Employees Credit Union, 2006 WL 1724574, at *2–3. This description simplifies the relationships. For example, payment processors may act as intermediaries between merchants and acquiring banks, but they are not relevant to the discussions in this note. See Corporate.Visa.com, supra note 99.
agreements. The issuer in a transaction usually has no direct contractual relationship with the acquirer (except as a co-member of the card association) or with the merchant.

Card association membership contracts require banks to comply with the association Operating Regulations and the PCI DSS. PCI DSS is a set of technical and business process requirements for anyone who processes, handles, or stores credit card information. Visa, Mastercard, Discover, JCB, and American Express jointly developed PCI DSS and created the PCI Security Standards Council to manage the standard. The individual card brands enforce compliance. The credit card companies include PCI DSS in their contracts with acquiring banks; if a bank is found to violate the standard, the card company can levy fines against the offending acquirer.

Unlike many industry and government security standards that speak in generalities and leave room for interpretation, PCI DSS sets specific requirements. It requires particular methods of encryption, prescribes network security technologies and configurations, and demands or forbids certain practices.

101. See Pa. State Employees Credit Union, 2006 WL 1724574, at *3 (describing Visa’s “Operating Regulations”).
102. For example, in the BJ’s Wholesale case, PSECU tried to argue that it was a third party beneficiary of the contract between BJ’s Wholesale and its acquirer, Fifth Third Bank because PSECU had no contract with either Fifth Third or BJ’s Wholesale. See id. at *1 (explaining PSECU’s third-party beneficiary claim).
103. Id. at *9.
106. Id.
108. Petitti, supra note 107, at 32.
109. For example, the FTC’s rules under the Gramm-Leach-Bliley Act (GLBA) call for “appropriate” safeguards against “reasonably foreseeable” risks. 16 C.F.R. § 314.4 (2007). Federal Health Insurance Portability and Accountability Act (HIPAA) regulations allow covered entities to use any security measures that allow such entities “reasonably and appropriately” to implement the standards necessary for compliance. 45 C.F.R. § 164.306(b) (2007).
110. PCI DSS, supra note 14, at 5.
111. See id. at 3–4 (requiring network firewalls and specifying some ways in which these firewalls must be configured).
such requirement prohibits storing sensitive authentication data.\textsuperscript{113}
Under PCI DSS, anyone handling credit card data must never store—even if encrypted—a card’s full track data, card verification code, or PIN verification code after authorization has cleared.\textsuperscript{114}

Despite low early compliance with PCI DSS, merchants appear to be making progress in satisfying its security requirements.\textsuperscript{115} In July 2007, Visa announced that ninety-six percent of large merchants that accept Visa as payment no longer stored full track card data.\textsuperscript{116} That statistic only addresses one PCI DSS requirement; large merchants continue to struggle to comply with the rest of PCI DSS’s requirements.\textsuperscript{117}

B. Minnesota’s Plastic Card Security Act

1. Summary and History

In May 2007, Minnesota enacted a data security law based on PCI DSS.\textsuperscript{118} The law implements, in a modified form, the

\textsuperscript{112} See id. at 12 (requiring annual network and application penetration tests); id. at 8 (prohibiting developer access to production databases).

\textsuperscript{113} Id. at 5. See also supra note 13 and accompanying text.

\textsuperscript{114} PCI DSS, supra note 14, at 5.


\textsuperscript{117} See RSA, THE PAYMENT CARD INDUSTRY DATA SECURITY STANDARD IN 2007, at 1 (2007), available at https://rsa-email.rsa.com/servlet/campaignrespondent. Small merchants are doing even worse, with only a nineteen percent compliance rate as of March 2007. Id.

\textsuperscript{118} Act of May 21, 2007, No. 1758, ch. 108, § 1, 2007 Minn. Sess. Law Serv. 500–01 (West), 85th Leg., Reg. Sess. (Minn. 2007) (codified at MINN. STAT. § 325E.64 (Supp. 2008)). Minnesota was not the first state to contemplate such a law. A Texas bill would have adopted PCI DSS as law by reference so that any change to PCI DSS would be required under Texas law. See H.B. 3222, sec. 1, § 48.102(c), 80th Leg., Reg. Sess. (Tex. 2007), available at http://www.legis.state.tx.us/lodocs/80r/billtext/html/HB03222E.htm. That approach would have given private organizations the power to create public law, raising due process concerns. See id. It also would have influenced contract negotiations involving the card brands because the PCI Standards Council could impose any condition it wanted as a matter of law by making it part of PCI DSS. Fortunately, the Texas bill died in the Senate committee. See Texas Legislature Online, 80(R) History for H.B. 3222, http://www.legis.state.tx.us/BillLookup/History.aspx?LegSess=80R&Bill=HB3222 (last visited Feb. 5, 2008); Vijayan, supra note 14.
standard’s prohibition against storing full track data. Specifically, it mandates that no one conducting business in Minnesota may store a PIN verification code, card security code, or full track data after transaction authorization.

The law creates a private cause of action for financial institutions to recover from entities that fail to meet the statute’s requirements. It requires a breached entity to reimburse certain costs that a financial institution incurs related to the breach, offset by any reimbursement the financial institution receives from a credit card company.

Other states have proposed similar bills, but none had become law as of October 2007. Time will tell whether Minnesota’s law spurs a flurry of other state laws the way California’s breach notification law did. If it does, those states could learn from what Minnesota did right and wrong in its law.

119. See Minn. Stat. § 325E.64, subdiv. 2 (Supp. 2007).
120. Id. The law allows storage for forty-eight hours after authorization for PIN debit transactions. Id. Entities violate the statute even if service providers store the data for them. Id.
121. Id. § 325E.64, subdiv. 3 (Supp. 2008). The cause of action covers breaches of security that occur on or after August 1, 2008. Id.
122. Id. Financial institutions can recover costs involved in canceling or reissuing cards, closing accounts and stopping payments, reopening accounts, refunding unauthorized transactions to cardholders, and notifying cardholders of the breach. Id. The law also allows financial institutions to recover costs of damages paid to cardholders. Id.
123. Id.
124. See, e.g., S.B. 1675, 95th Gen. Assem., Reg. Sess. (Ill. 2007) (as amended Mar. 3, 2007), available at http://www.ilga.gov/legislation/fulltext.asp?DocName=&SessionId=51&GA=95&DocTypeId=SB&DocNum=1675&GAID=9&LegID=29808&SpecSess=&Session=; Tex. H.B. 3222. A similar California bill was vetoed. See A.B. 779, 2007–08 Leg., Reg. Sess. (Cal. 2007), available at http://info.sen.ca.gov/pub/07-08/bill/asm/ab_0751-0800/ab_779_bill_20070914_enrolled.pdf; Evan Schumann, Governor Kills California Data Protection Law, EWeek, Oct. 15, 2007, available at http://www.eeweek.com/article2/0,1895,2197107,00.asp. California’s bill would have been broader than Minnesota’s. In addition to prohibiting storage of sensitive authentication data, it would have restricted the handling of “payment-related data,” defined as an “[a]ccount number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account.” A.B. 779 at § 6, sec. 1798.82(e)(3). Entities would not have been allowed to store payment-related data unless they had data retention and disposal policies. Id. § 1, sec. 1724.4(b)(1). California’s bill would also have forbidden sending unencrypted payment-related data over open public networks, and would have required entities to limit access to payment-related data to people whose job functions require access. Id. § 1, sec. 1724.4(b)(6)–(7).
2. General Features

Legislating technology is hard. A statute must tread a fine line between generality and specificity. Make it too broad, and it risks interpretations contrary to the intent of the law. If it is too specific, tying itself to the technology of the time, it can become outdated or require legislative reconsideration when technology changes. By adopting part of a detailed technical standard and trying to generalize it, Minnesota gave its law both of these problems. In most ways, it is far too narrow and specific, but it also has surprising areas of generality.

Minnesota's law covers a narrow set of circumstances; it allows recovery only by financial institutions, not consumers. It applies to payment cards, but not other sensitive personal data such as bank account numbers or Social Security numbers. It prohibits

129. MINN. STAT. § 325E.64, subdiv. 3 (Supp. 2007). The legislative records show that the legislature explicitly considered, but then rejected, a cause of action for consumers. The version reported out of the House Commerce and Labor Committee would have created a private right of action for “any person injured by a violation” of the bill’s requirements. H.F. 1758, 85th Leg., Reg. Sess. (Minn. 2007) (as reported by H. Commerce & Labor Comm., Mar. 20, 2007). The Public Safety and Civil Justice committee removed the general cause of action and replaced it with language allowing recovery by financial institutions. Minn. H.F. 1758 (as reported by H. Public Safety & Civil Justice Comm., Mar. 27, 2007). That language substantially survived to final passage. See 2007 Minn. Sess. Law Serv. 500–01 (West).
130. § 325E.64.
storage of full track credit card data, but sets no standards for data in transit. This narrowness is the law’s chief weakness.

The statute also shows signs of a struggle to adopt a private contractual security standard as public law. It attempts flexibility by using “access device” as a general term for payment cards, but loses some of that flexibility when it limits those access devices to cards and describes security codes as three or four-digit values. But the statute also shows signs of unintentional breadth. For example, its definition of a PIN and PIN verification code could include cardholder names and passwords.

The law differs from PCI DSS in a number of ways. The largest difference is that it only adopts a small subset of the

131. *Id.* at subdiv. 2.
132. *Id.* at subdiv. 1(b). The statute defines an access device as having a magnetic stripe, microchip, or “other means for storage of information” and says that access devices include “but [are] not limited to” credit and debit cards. *Id.*
133. *Id.* The word “card” may tie the law to a particular physical form of payment device. See, e.g., THE OXFORD ENGLISH DICTIONARY 888 (2d ed. 1989) (defining a card as “[a] rectangular piece of stiffened plastic issued by banks and other institutions . . . .”). The definition could include smart cards, which have microprocessors and allow sophisticated authentication methods. See generally Katherine M. Sheller & J. Drew Proacco, *Smart Card Evolution*, COMM. ACM, Jul. 2002, at 83–88, but it would not include payment devices in forms other than cards. A key fob, for example, is not a card, and a payment device based on one may not, by the strict language of the statute, be subject to section 325E.64.
134. *Id.* at subdiv. 1(d). Florida’s definition of an access device in its criminal identity theft statute is much more precise:

“Access device” means any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds, other than a transfer originated solely by paper instrument. FLA. STAT. ANN. § 817.568(1)(a) (West Supp. 2003).
135. The statute defines a PIN as a code that identifies the cardholder, and a PIN verification code as any data used in combination with a PIN to verify the cardholder’s identity. M N N. STAT. § 325E.64, subdiv. 1(h)–(i) (Supp. 2007). Those definitions might include, for example, usernames and passwords used in online transactions. Nothing in the statute explicitly requires a PIN or PIN verification code to be a value stored on an access device. See *id.*
136. This difference is endemic to public laws based on private standards. When a legislative implementation differs from the standard that inspired it, organizations must comply with two similar but slightly different sets of requirements. If the difference is great enough, the public law could conflict with the private standard it meant to mimic. The problem can increase over time as the private standard is updated. Referring to the private standard directly (i.e., a law requiring all merchants to comply with the requirements of PCI DSS) would solve this problem, but at the same time, create a worse one by making a private
standard’s requirements. Minnesota Statutes section 325E.64 only adopts the element of the standard prohibiting storage of “sensitive authentication data.” PCI DSS is much broader than that one requirement, however, reflecting the wide range of business processes and controls necessary to ensure data security.

Fortunately for merchants, Minnesota’s law differs from PCI DSS by being more permissive. Unlike PCI DSS, it allows a forty-eight hour window for storing debit card information after a transaction. It may also allow entities to avoid liability by encrypting full track data, a practice PCI DSS prohibits. Since Minnesota’s law is more permissive than PCI DSS, merchants who comply with PCI DSS will also be in compliance with Minnesota’s law. The reverse is not true. Merchants who comply with the provisions of Minnesota’s law would not necessarily be in strict compliance with PCI DSS.

3. Improvement on Data Breach Notification Laws

Minnesota’s law fixes some of the problems that make data breach laws ineffective. It allows cost-shifting for financial institutions and further increases the potential cost of a data breach under contract law. See discussion supra note 118.

137. See § 325E.64, subdiv. 2.
138. Id. See also PCI DSS, supra note 14, at 5.
139. See PCI DSS, supra note 14, at 1 (listing PCI’s twelve requirement categories).
140. PCI DSS technically has room for permissiveness in that it allows compensating controls. See id. at 16; PCI DSS GLOSSARY, supra note 13. An organization storing full track credit card data might comply with PCI DSS through compensating controls, but it would still violate Minnesota’s law.
141. MINN. STAT. § 325E.64, subdiv. 2 (Supp. 2007); PCI DSS, supra note 14, at 5. The Minnesota law applies only to debit card transactions, not credit card payments. § 325E.64, subdiv. 2.
142. Section 325E.64 defines “breach of the security of the system” by reference to Minnesota’s security breach notification law, which defines it as the “unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information.” MINN. STAT. § 325E.61, subdiv. 1(d) (2006) (emphasis added). The breach notification law defines “personal information” as certain unencrypted data. Id. at subdiv. 1(e) (emphasis added). If a security breach requires unauthorized access to unencrypted data, encrypted data cannot be “breached” as that term is defined in Minnesota law. Because liability depends on a breach of security, encrypting data might allow data handlers to avoid liability even though the retention requirement itself does not exempt encrypted data.
143. See PCI DSS, supra note 14, at 5.
144. See generally § 325E.64; PCI DSS, supra note 14.
145. See § 325E.64; PCI DSS, supra note 14, at 5.
breach. However, the law does nothing to directly help consumers, and leaves an organization’s expected data-breach cost unpredictable.

Minnesota’s law allows financial institutions to recover the cost of reissuing credit cards when someone else suffers a breach of stored sensitive authentication data. As such, the statute is a direct salvo at the BJ’s Wholesale result, and a look forward to the pending TJX litigation. Recall that in the BJ’s Wholesale case, Pennsylvania State Employees Credit Union (PSECU) sued BJ’s credit card processor, Fifth Third Bank, after a security breach compromised full track credit card data stored in violation of Visa’s operating regulations. The court denied all of PSECU’s claims for relief. Had that case been litigated under Minnesota law after January 1, 2008, Minnesota Statutes section 325E.64 would have provided PSECU a viable cause of action.

Some have argued that the law is unnecessary. Card Association Operating Agreements already require anyone handling credit card data to meet PCI DSS requirements. Everyone involved in a payment card transaction has a contract with someone else and could establish rules for liability and reimbursement by contract. PSECU, for example, could have negotiated a contract with Visa that would have required Visa to

146. See supra Parts II.B.2 & II.B.3.
147. See § 325E.64, subdiv. 3.
150. Id. at 338 (dismissing all claims other than the third party contract claim. Subsequently, the third party claim was also dismissed in 2006 WL 1724574, at *13).
151. See § 325E.64.
152. See Oehlsen, supra note 19.
154. See supra Part II.A for a description of the contractual relationships between consumers, issuers, merchants, and acquirers.
reimburse PSECU any costs PSECU incurred replacing cards.\textsuperscript{155} In fact, the Operating Regulations contain just this sort of provision.\textsuperscript{156} In the BJ’s Wholesale case, Visa had “exercised its right under the Operating Regulations” to reallocate losses, forcing Fifth Third Bank to pay over $870,000 to issuing banks.\textsuperscript{157}

Minnesota’s card security law is not completely unnecessary, as it does not merely duplicate rights issuers have under the Operating Regulations. Visa has forbidden the storage of full track data since 1993,\textsuperscript{158} yet fourteen years later full track storage is still a problem.\textsuperscript{159} Moreover, the Operating Regulations do not cover all the forms of loss that the Minnesota law does.\textsuperscript{160} For example, the Operating Regulations allow reallocation of losses for fraud, but not for “operational costs” such as replacing lost credit cards.\textsuperscript{161} Visa also retains sole control over all disputes between member financial institutions under the Operating Regulations.\textsuperscript{162}

Arguments that Minnesota’s law meddles with freely-made contracts have some merit, however. Each issuer enters into the association membership voluntarily, with knowledge of the Operating Regulations and their dispute resolution procedures. The financial institutions that issue credit cards can ostensibly protect themselves through contracts; consumers cannot. Yet the Minnesota law protects financial institutions, not consumers.

\begin{itemize}
\item \textsuperscript{155} As unlikely as this seems given the relative power of the card associations compared with individual financial institutions, there may be some room for negotiation in the agreements.
\item \textsuperscript{156} \textit{Pa. State Employees Credit Union}, 2006 WL 1724574, at *5.
\item \textsuperscript{157} \textit{Id.} Visa also levied $555,000 in fines against Fifth Third Bank for violations of the Operating Regulations. \textit{Id.} Those fines were not redistributed to issuers. \textit{Id.}
\item \textsuperscript{158} \textit{Id.} at *7.
\item \textsuperscript{159} The BJ’s Wholesale and TJX breaches are just two examples of data breaches involving stored sensitive authentication data. Visa reports that of merchants who handle more than one million transactions per year, ninety-six percent now claim not to store sensitive authentication data, but compliance among smaller organizations is lagging. \textit{See Press Release, Visa Inc., Visa Marks Progress in Securing Merchant Systems} (July 30, 2007), available at http://corporate.visa.com/md/nt/press719.jsp.
\item \textsuperscript{160} \textit{See MINN. STAT. § 325E.64} (Supp. 2007); \textit{Pa. State Employees Credit Union}, 2006 WL 1724574, at *4–5 (describing Visa’s Operating Regulations).
\item \textsuperscript{161} \textit{Pa. State Employees Credit Union}, 2006 WL 1724574, at *4–5.
\item \textsuperscript{162} \textit{Id.} (describing dispute resolution procedures under Visa’s Operating Regulations). The dispute resolution procedures do not claim to be exclusive—members can still pursue legal options against other members outside the Visa system. \textit{Id.} at *6.
\end{itemize}
IV. THE FINISH LINE: A STATUTORY STANDARD OF DATA SECURITY DUE CARE

Data breach notification laws do not do enough to encourage secure handling of data, and do nothing to compensate victims. Minnesota’s card security law creates a narrow remedy to financial institutions that have to reissue credit cards, but offers no help to consumers. A better data security law is needed: one that would meet the behavior modification and compensation goals described in Part II.B.2.

Several principles should guide such a law. First, it should tilt the cost-benefit equation toward securing data. Second, it should compensate victims who suffer actual harm. Third, the law should be flexible enough to remain relevant as technology changes. Fourth, any related statutes of limitations or repose should allow recovery when breach-related fraud is discovered. Finally, the law should ameliorate the difficulty of proving cause-in-fact when a data breach has led to identity theft.

The most appropriate solution would: (1) adopt a statutory duty of due care in handling data; (2) use a notice standard for the statute of limitations on identity theft-related tort claims; and (3) presume cause-in-fact when a consumer has both suffered new account fraud and been the subject of a data breach. Each of these components is considered in turn.

A. Duty of Due Care

A due care standard would complement existing data notification laws and technology-focused laws such as Minnesota’s payment card law. It would create a multi-tiered approach in which the duty of due care establishes a general requirement to take proper care of data, a data breach law requires notification of consumers when a breach has happened, and a few technology laws specifically define examples of per se negligent behavior. At least

163. See RESTATEMENT (SECOND) OF TORTS § 901 (1979) (describing behavior modification as a goal of tort law).

164. Id.

165. See discussion supra Part III.B.2.

166. See discussion infra Part IV.B.1.

167. See discussion infra Part IV.B.2.

168. That would fit products liability’s general approach, where the common law has long recognized a duty of due care while statutes specify requirements for warning labels or product features. See, e.g., 21 C.F.R. § 101.2 (2007) (establishing
two states now have forms of statutory duty of due care for data protection. 169

Why due care? Although negligence or strict liability might satisfy the desired principles, recovery through negligence better fits the nature of data security. The reasons rely on theoretical interpretations of tort law.

Economic efficiency analysis suggests that strict liability might be appropriate. Negligence encourages due care by both the data handler and the victim. 170 Strict liability is efficient when the victim has no ability to prevent a harm (e.g., data loss) through due care, because it gives the victim no incentive to take care to avoid the harm. 171 Such is the case with data security. Data subjects cannot improve the handling of their data, nor can they choose to have their data handled by more careful organizations. 172 This comparison would seem to give an edge to strict liability, but other factors favor negligence.

One such factor is the way each theory of liability changes behavior. Negligence law encourages organizations to avoid accidents through carefulness, while strict liability creates incentives for organizations to avoid accidents by lowering their activity levels. 173 Negligence is appropriate when greater care, not reduced activity, is the more efficient means of avoiding accidents. 174 Strict liability has consequently been imposed on “abnormally dangerous” activities 175 such as explosive blasting.

---

169. See CAL. CIV. CODE § 1798.81.5 (West Supp. 2007); TEX. BUS. & COM. CODE § 48.102(a) (Vernon Supp. 2007). Although both statutes set duties of due care, neither establishes a private cause of action.


171. Id. at 282.

172. See Solove, supra note 40, at 1234–38.


174. Id. at 285.

175. RESTATEMENT (SECOND) OF TORTS § 519 (1979).

handling of hazardous wastes, and certain uses of poisons. Whether an activity is “abnormally dangerous” rests in part on whether reasonable care can eliminate the risk involved in the activity. The proper liability regime for data breaches therefore depends on whether they are the “inevitable byproduct” of data collection, or whether they can be reduced by the application of due care.

Products liability law offers a useful parallel. Design defects fall under negligence law because due care in design can avoid that particular kind of flaw. Manufacturing defects generate strict liability causes of action because those defects are seen as inherent and unavoidable when manufacturing products. Even careful manufacturers sometimes make defective products and society benefits by putting the cost of the harms caused by manufacturing defects on the manufacturer rather than the consumer.

The history of publicly disclosed breaches shows plenty of room for improving due care in handling data. Some of the more infamous data breaches happened to retailers who operated insecure wireless networks, stored unencrypted card data, failed to verify that certain customers actually were small businesses instead of data thieves, or did not use “simple, low-cost, and

183. See id. § 2 cmt. a.
184. See id.
187. See Tom Zeller, Jr., Release of Consumers’ Data Spurs ChoicePoint Inquiries,
readily available” methods of avoiding software application attacks. Other breaches involved un-patched software, weak user IDs and passwords, and postings of confidential data to the Internet. These data breaches were not inevitable side-effects of handling data; they were the direct results of preventable mishandling of data.

Of course, not all causes of data breach are so egregious. In many cases, data was lost because of insider misbehavior, lost or stolen laptops, disks lost in the mail, or lost backup tapes. In at least some of these cases, data was lost despite arguably careful handling, or through unforeseeable acts of third parties. Perhaps some data breaches are unavoidable, but it is too soon to know because so many breaches are clearly avoidable. Until due care is shown not to significantly reduce data disclosure, the law should err on the side of encouraging due care rather than


192. See, e.g., Shirley Duglin Kennedy, I’ve Been Violated, INFO. TODAY, June 1, 2006, at 17 (dishonest insider at the Georgia Department of Motor Vehicles); Paul Nowell, Banks Look At Insiders in Security Lapse, FORT WAYNE J.-GAZETTE, July 11, 2005, at 1C (reporting insider theft at Wachovia and Bank of America).

193. See, e.g., Melissa Allison, Missing Starbucks Laptops Had Data on 60,000 People, SEATTLE TIMES, Nov. 4, 2006, at A1 (containing a brief chronology of lost laptops with personal information, including those at Starbucks, Fidelity Investments, and Ameriprise); David Stout, Veterans Agency to Atone with Free Credit Monitoring, N.Y. TIMES, June 22, 2006, at A22 (describing Veterans Affairs breach caused by lost laptop).


195. See, e.g., Will Wade, Security Watch, AM. BANKER, Sept. 8, 2006, at 5 (reporting 2.6 million Circuit City customer records inadvertently thrown into trash); Assoc. Press, 4 Providence Workers out over Data Theft, COLUMBIAN, Feb. 25, 2006, at C5 (reporting theft of backup tapes from a van).

196. See, e.g., Guin v. Brazos Higher Educ. Serv. Corp., No. Civ. 05-668 RHK/JSM, 2006 WL 288483, at *4 (D. Minn. Feb. 7, 2006) (holding that an employee whose company laptop was stolen from his home “lived in a relatively ‘safe’ neighborhood and took” reasonable precautions against break-in, so theft of the laptop was not foreseeable).
imposing strict liability.

Finally, a negligence cause of action encourages data collectors to consider the effects its care of data has on others. Instead of merely estimating the cost to themselves should a breach occur, data collectors would have to use the same formula a jury would use—Judge Learned Hand’s formula comparing the burden of mitigation with the probability and degree of loss.\textsuperscript{197} The loss portion of that calculation encompasses the loss to data subjects, not merely the data handler, and represents a vast improvement over data handlers’ current self-centered cost-benefit calculations when security is concerned. Even if data handlers use different values than a jury would, or estimate different non-optimal values,\textsuperscript{198} at least they would be trying to estimate the right values.

B. Implementation Details

Even with a statutory duty of security due care, a victim could not recover if the statute of limitations and repose had expired, or if they could not prove cause-in-fact harm. Ensuring appropriate statutes of limitation and cause-in-fact standards could solve these issues.

1. Statute of Limitations

Some forms of post-breach harm can be hard to discover before the statute of limitations has expired. A discovery standard would allow enough time to file suit without subjecting breached organizations to near-endless liability.\textsuperscript{199} Specifically, a statute establishing a duty of due care should allow actions within two years of when someone discovers, or reasonably should have discovered, that harm has occurred.\textsuperscript{200}

\textsuperscript{197} U.S. v. Carroll Towing Co., 159 F.2d 169, 173 (2d Cir. 1947).
\textsuperscript{198} See Citron, supra note 180, at 263–64 (discussing the “uncertainty dilemma” of economic theories of negligence law).
\textsuperscript{199} The statute of limitations under a discovery standard begins to run when the plaintiff knows or should reasonably know of the existence of the cause of action. Herrmann v. McMenomy & Severson, 590 N.W.2d 641, 643 n.16 (Minn. 1999) (citation omitted).
\textsuperscript{200} Even without a discovery standard, the statute should not begin to run until some post-breach harm has happened. See Dalton v. Dow Chem. Co., 280 Minn. 147, 153, 158 N.W.2d 580, 584 (1968) (“An action for negligence cannot be maintained, nor does the statute of limitations begin to run, until damage has resulted from the alleged negligence.”).
A discovery standard is needed because victims may not notice post-breach harms until several years after the breach. Some breached data never expires, and misuse often creates no noticeable signs. Many victims of identity theft find out about it only when they are denied credit or even arrested. Recent statistics show that nearly one-quarter of identity theft victims do not discover the fraud within two years, and almost one in ten does not find out until five years have passed. These factors suggest that Minnesota’s default six-year statute of limitations for tort claims may not be long enough unless a discovery standard is used. A two-year post-discovery statute of limitations would recognize the need for a discovery standard, but reduce a data handler’s exposure to suit once that harm has been discovered.

A due care statute implementing a discovery standard must say so explicitly. The Minnesota Supreme Court generally has not recognized a discovery standard where a statute did not expressly include it. Furthermore, the United States Supreme Court’s

201. See Solove, supra note 40, at 1251–55 (detailing the undiscovered harm often caused by Social Security number identity theft).

202. Id.

203. See, e.g., Identity Theft: Restoring Your Good Name: Hearing before the S. Subcomm. on Technology, Terrorism, and Government Information, 107th Cong. 12 (2002) [hereinafter 2002 Hearings], (statement of Howard Beales, Director, FTC Bureau of Consumer Protection) (testifying that five percent of identity theft victims were unaware of the theft five years after it happened, and that the average time to detect an identity theft was twelve months), available at http://judiciary.senate.gov/testimony.cfm?id=171&wit_id=348.

204. See, e.g., Acton v. Equifax Credit Info. Serv., Inc., 293 F. Supp. 2d 1092, 1096 (D. Ariz. 2003) (involving a plaintiff who discovered inaccurate credit information after a mortgage loan was denied).

205. Criminal record identity theft happens when a criminal uses stolen identity information to “evade legal sanctions and criminal records.” See 2002 Hearings, supra note 203, at 13. This form of fraud is especially pernicious because consumers have no easy way to discover that they have criminal records. See U.S. GENERAL ACCOUNTING OFFICE, GAO-02-363, IDENTITY THEFT: PREVALENCE AND COST APPEAR TO BE GROWING 61 (March 2002), available at http://www.gao.gov/new.items/d02363.pdf.


207. MINN. STAT. § 541.05, subdiv. 1(5) (2006).

208. See, e.g., Herrmann v. McMenomy & Severson, 590 N.W.2d 641, 643 (Minn. 1999) (rejecting the discovery rule for professional malpractice); Johnson v. Winthrop Labs., 291 Minn. 145, 150–51, 190 N.W.2d 77, 81 (1971) (rejecting the discovery rule in medical malpractice cases). But see Schmucking v. Mayo, 183 Minn. 37, 40–41, 235 N.W. 633, 634 (Minn. 1931) (applying the discovery rule in
decision in *TRW Inc. v. Andrews* casts doubt on whether the notification standard would apply in identity theft cases.\(^{209}\)

Including the discovery standard in statutory language would avoid creating interpretive questions.

2. **Proving Cause-in-Fact**

The remaining problem is the difficulty of proving cause-in-fact.\(^{210}\) Common-law negligence requires the plaintiff to show by a preponderance of the evidence that the defendant caused the plaintiff’s harm.\(^{211}\) The problem with data-related harms is that it is often difficult or impossible for a plaintiff to trace the original source of misused data.\(^{212}\)

The law has dealt with similar problems by allowing rebuttable presumptions of cause-in-fact.\(^{213}\) Presumed cause-in-fact reverses the burden of proof by requiring the defendant to disprove causation.\(^{214}\) Courts have used this standard when causation would

\(^{209}\) See *TRW Inc. v. Andrews*, 534 U.S. 19, 27–28 (2001) (rejecting the discovery standard in an identity theft claim under the Fair Credit Reporting Act). A broad interpretation of *TRW* might suggest that the statute of limitations in all identity theft cases begins to run at the time of the harm, not discovery. See *id*. Presumably, that standard would extend to third-party liability for harm.

\(^{210}\) This section assumes a plaintiff has suffered actual post-breach harm. Therefore, the problem at issue is not whether the plaintiff has actually been harmed, but whether she can prove cause-in-fact.

\(^{211}\) Schulz v. Feigal, 273 Minn. 470, 476, 142 N.W.2d 84, 89 (1966). Although the standard does not require eliminating “every other possible hypothesis as to the cause of the injuries,” it demands more than “speculation or conjecture.” *Id*.

\(^{212}\) See *supra* notes 76–78 and accompanying text.

\(^{213}\) See, e.g., 42 U.S.C. § 300aa-14(a), construed in *Flores v. Sec. of Health and Human Servs.*, 52 Fed. Cl. 294, 299 (2002) (discussing presumed causation under Vaccine Act); Zuchowicz v. U.S., 140 F.3d 381, 390–91 (2d Cir. 1998) (summarizing the opinions of Chief Judge Cardozo and Chief Justice Traynor as allowing a presumption of cause when an act increases the chances of a particular type of accident, and an accident of that sort actually happens); Erdmann v. Frazin, 158 N.W.2d 281, 283 (Wis. 1968) (noting a rebuttable presumption of causation when “one owing a duty to make a place or an employment safe fails to do it and that accident occurs which performance of the duty was designed to prevent”); Gerald W. Boston, *Toxic Apportionment: A Causation And Risk Contribution Model*, 25 ENVTL. L. 549, 591–92 (1995) (noting that federal Superfund statutes do not require tracing cause to a particular defendant, in part because “the passage of years between the time of disposal and cleanup often results in unavailable relevant documents and knowledgeable witnesses.”).

otherwise be difficult to prove, and statutes have adopted it for similar purposes.

A data security due care statute should allow presumptive causation if the plaintiff proves two elements: (1) that the plaintiff’s information was compromised in a breach of data under the defendant’s care; and (2) that the information was both necessary and sufficient to enable the actual harm done. The defendant could rebut the presumption by showing another likely source of the misused data. It could also avoid the presumption by showing that the data was not actually compromised or that the data was not necessary or sufficient for the post-breach fraud.

Such a presumption would mitigate the problems of showing cause-in-fact. It recognizes cause when the plaintiff is prevented from connecting each of several dots needed to satisfy the common-law rule. When a customer has suffered actual fraud or other harm following a data breach and the information lost in the breach was enough to perpetrate that fraud, this rule improves the plaintiff’s ability to show cause-in-fact, but allows the defendant a reasonable chance to demonstrate that something other than the data breach caused the harm.

V. CONCLUSION

Legislatures and courts are still struggling to find the right approach to data security law. Ultimately, data security will not be improved through mere notification or through piecemeal legislation of individual technical requirements. A statutory standard of due care for data security could do what these other laws cannot: take externalities into account, compensate victims for actual harm, and adapt to new technologies without frequent legislative revisits. Most importantly, it could help prevent the next announcement of millions of lost personal data records.

215. See Zuchowicz, 140 F.3d at 390–91; Erdmann, 158 N.W.2d at 283.
216. See Flores, 52 Fed. Cl. at 299; Boston, supra note 213, at 591–92.
218. See Zuchowicz, 140 F.3d at 390–91.
219. See Wright, supra note 217, at 1788–89.