

**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. <i>History and Features</i>	1118
B. <i>Data Breach Laws' Inadequacies</i>	1120
1. <i>Notification</i>	1121
2. <i>Behavior Modification</i>	1122
3. <i>Cost Shifting</i>	1125
III. THE NEXT STEP: PCI-BASED LAWS	1129
A. <i>Background: Payment Cards and PCI DSS</i>	1129
B. <i>Minnesota's Plastic Card Security Act</i>	1131
1. <i>Summary and History</i>	1131
2. <i>General Features</i>	1133
3. <i>Improvement on Data Breach Notification Laws</i>	1135
IV. THE FINISH LINE: A STATUTORY STANDARD OF DATA SECURITY DUE CARE	1138
A. <i>Duty of Due Care</i>	1138
B. <i>Implementation Details</i>	1142
1. <i>Statute of Limitations</i>	1142
2. <i>Proving Cause-in-Fact</i>	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.² Lost data has become so common that a breach must now affect millions of records even to be newsworthy.³ One of the first widely publicized breaches, ChoicePoint's 2005 disclosure of 163,000 consumer records,⁴ seems almost harmless compared to the breaches at TJX,⁵ Certegy,⁶ Circuit City,⁷ and the Department of Veterans Affairs,⁸ each of which lost millions of records.

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

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

1. Privacy Rights Clearinghouse, A Chronology of Data Breaches, <http://www.privacyrights.org/ar/ChronDataBreaches.htm> (last visited Feb. 4, 2008).

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." *Id.*

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.

4. See Harry R. Weber, *ChoicePoint Agrees to Settlement in Data Scandal*, SEATTLE TIMES, Jan. 27, 2006, at D2.

5. Larry Greenemeier, *TJX Stored Customer Data, Violated Visa Payment Rules*, INFO. WK., Jan. 29, 2007, available at <http://www.informationweek.com/showArticle.jhtml?articleID=197001447>.

6. See *Latest Data Breach Hits Certegy, Info Allegedly Used Only For Marketing*, CREDIT UNION J., July 9, 2007, at 4.

7. See Will Wade, *Security Watch*, AM. BANKER, Sept. 8, 2006, at 5.

8. See David Stout, *Veterans Agency to Atone with Free Credit Monitoring*, N.Y. TIMES, June 22, 2006, at A22.

9. See Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913, 915–16 (2007).

10. *Id.*

11. See *infra* note 23.

12. See discussion *infra* Part II.

authorization data.¹³ It adopted this requirement from a credit card industry standard called the Payment Card Industry Data Security Standard (PCI DSS).¹⁴ PCI DSS sets specific technical and business process requirements for securing credit card data.¹⁵ Anyone who “store[s], process[es], or handl[es]” credit card data must comply with PCI DSS.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.¹⁷ Minnesota’s law provides remedies only to financial institutions, not consumers.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.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.

13. See MINN. STAT. § 325E.64 (Supp. 2007). Sensitive authorization data includes the data from a credit card’s magnetic stripe, the PIN verification code, and the credit card verification code (known as the CID, CVV2, or CVC2 code, depending upon the card brand). See PCI SEC. STANDARD COUNCIL, PAYMENT CARD INDUSTRY (PCI) DATA SECURITY STANDARD GLOSSARY, ABBREVIATIONS AND ACRONYMS (2007), http://www.pcisecuritystandards.org/pdfs/pci_dss_glossary_v1-1.pdf [hereinafter PCI DSS GLOSSARY]. Anyone armed with this data can duplicate a card. See VISA USA, CISP BULLETIN: TOP FIVE DATA SECURITY VULNERABILITIES IDENTIFIED TO PROMOTE MERCHANT AWARENESS 1 (2006), http://usa.visa.com/merchants/risk_management/cisp_alerts.html (follow “CISP Bulletins” hyperlink in middle of page; then follow “Top Five Data Security Vulnerabilities Identified to Promote Merchant Awareness—August 29, 2006”).

14. See PCI SEC. STANDARDS COUNCIL, PAYMENT CARD INDUSTRY (PCI) DATA SECURITY STANDARD 1 (2006), <https://www.pcisecuritystandards.org/tech/index.htm> (follow the link at “Click here to download the Specification”) [hereinafter PCI DSS]; Jaikumar Vijayan, *Minnesota Gives PCI Rules a Legal Standing*, COMPUTERWORLD, May 28, 2007, at 40.

15. See PCI DSS, *supra* note 14, at 1.

16. *Id.* at 2.

17. See discussion *infra* Part II.B.

18. See *id.*

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.²⁰ California led the charge in 2002 by becoming the first state to pass a law requiring public disclosure of security incidents.²¹ Most states followed with similar laws of their own.²² As of January 2008, thirty-nine states and the District of Columbia had enacted data breach notification laws.²³

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).

21. 2002 Cal. Legis. Serv. 4501–04 (West) (codified at CAL. CIV. §§ 1798.29, 1798.82 (2007)).

22. 2005 was a banner year for breach notification laws, with at least thirty-five states considering such laws and twenty-two states enacting them. National Conference of State Legislatures, 2005 Breach of Information Legislation, <http://www.ncsl.org/programs/lis/cip/priv/breach05.htm> (last visited Feb. 4, 2008).

23. See ARIZ. REV. STAT. ANN. § 44-7501 (Supp. 2007); ARK. CODE ANN. §§ 4-110-101 to -108 (Supp. 2007); CAL. CIV. CODE. §§ 1798.29, 1798.82 (West Supp. 2008); COLO. REV. STAT. ANN. § 6-1-716 (West Supp. 2007); CONN. GEN. STAT. ANN. § 36a-701b (West Supp. 2007); DEL. CODE ANN. tit. 6, §§ 12B-101 to -104 (2005); 2007-3 D.C. Code Adv. Leg. Serv. 29–32 (LexisNexis); FLA. STAT. ANN. § 817.5681 (West 2006); GA. CODE ANN. §§ 10-1-910 to -912 (Supp. 2007); HAW. REV. STAT. ANN. §§ 487N-1 to -4 (LexisNexis Supp. 2007); IDAHO CODE ANN. §§ 28-51-104 to -107 (Supp. 2007); 815 ILL. COMP. STAT. ANN. 530/1–30 (West Supp. 2007); IND. CODE ANN. §§ 24-4.9-1-1 to -5-1 (West Supp. 2007); KAN. STAT. ANN. §§ 50-7a01 to -7a04 (Supp. 2006); LA. REV. STAT. ANN. §§ 51:3071–3077 (Supp. 2008); ME. REV. STAT. ANN. tit. 10 §§ 1346 to 1350-A (Supp. 2007); MD. CODE ANN., COM. LAW § 14-3504 (LexisNexis Supp. 2007); 2007 Mass. Legis. Serv. 540–48 (West); MICH. COMP. LAWS ANN. § 445.72 (West Supp. 2007); MINN. STAT. § 325E.61 (2006); MONT. CODE ANN. §§ 30-14-1701 to -1705 (2007); NEB. REV. STAT. ANN. §§ 87-801 to -807 (LexisNexis 2007); NEV. REV. STAT. ANN. §§ 603A.010–.920 (LexisNexis Supp. 2005); N.H. REV. STAT. ANN. §§ 359-C:19 to :21 (LexisNexis Supp. 2007); N.J. STAT. ANN. § 56:8-163 (West Supp. 2007); N.Y. GEN. BUS. LAW § 899-aa (McKinney Supp. 2008) (applying to private organizations); N.Y. STATE TECH. LAW § 208 (McKinney Supp. 2008) (covering state agencies); N.C. GEN. STAT. § 75-65 (2007); N.D. CENT. CODE §§ 51-30-01 to -07 (2007); OHIO REV. CODE ANN. §§ 1347.12, 1349.19-192 (West Supp. 2007); OKLA. STAT. ANN. tit. 74, § 3113.1 (West Supp. 2008); 73 PA. STAT. ANN. §§ 2301–2329 (West Supp. 2007); R.I. GEN. LAWS. §§ 11-49.2-1 to -7 (Supp. 2007); TENN. CODE ANN. § 47-18-2107 (Supp. 2007); TEX. BUS. & COM. CODE ANN. §§ 48.101-.203 (Vernon Supp. 2006); UTAH CODE ANN. §§ 13-44-101 to -301 (Supp. 2007); VT. STAT. ANN. tit. 9, § 2435 (2006); WASH. REV. CODE ANN. §

Data breach notification laws require organizations to notify data subjects whose personal data the organization reasonably believes has been obtained by a third party.²⁴ Notification must generally be given in writing²⁵ reasonably quickly after the breach is discovered,²⁶ and many data breach notification laws establish penalties for non-compliance.²⁷

State data breach notification laws vary in their details, including the standards for notification,²⁸ the types of personal data

19.255.010 (West 2007); WIS. STAT. § 895.507 (West 2006); WYO. STAT. ANN. § 40-12-502 (2007); S.B. 583, 74th Leg. Assem., Reg. Sess. (Or. 2007).

24. See, e.g., CAL. CIV. CODE § 1798.29(a) (West Supp. 2008).

25. See, e.g., *id.* § 1798.82(g)(1); MINN. STAT. § 325E.61, subd. 1(g)(1) (2006); N.Y. GEN. BUS. LAW § 899-aa(5)(a) (McKinney Supp. 2008). Some states allow substitute notice based on cost. See, e.g., CAL. CIV. CODE § 1798.82(g)(3) (West Supp. 2008); KAN. STAT. ANN. § 50-7a01(c)(3) (Supp. 2006); MINN. STAT. § 325E.61, subd. 1(g)(3) (2006); VT. STAT. ANN. tit. 9, § 2435(b)(5)(B) (2006). Utah allows notification through electronic means, telephone, and newspaper publication without a threshold for cost or number of people affected. See UTAH CODE ANN. § 13-44-202(5)(a) (Supp. 2007). Wisconsin's statute allows notice by a means "reasonably calculated to provide actual notice," but only if the breached entity cannot determine a data subject's mailing address. WIS. STAT. § 895.507(3)(b) (West 2006).

26. See, e.g., CAL. CIV. CODE § 1798.82(a) (West Supp. 2008) (calling for notification to be "made in the most expedient time possible and without unreasonable delay"); MINN. STAT. § 325E.61, subd. 1(a) (2006) (using the same language as the California statute). A few states set specific time limits for notification. See FLA. STAT. ANN. § 817.5681(1)(b) (West 2006); OHIO REV. CODE ANN. § 1349.19(B)(2) (West Supp. 2007); WIS. STAT. § 895.507(3)(a) (West 2006).

27. See, e.g., IDAHO CODE ANN. § 28-51-107 (Supp. 2007) (establishing a maximum \$25,000 penalty for intentional failure to comply with notification requirements); IND. CODE ANN. §§ 24-4.9-4-1 to -2 (West. Supp. 2007) (creating up to a \$150,000 civil penalty for "deceptive acts" under the statute); UTAH CODE ANN. § 13-44-301(3) (Supp. 2007) (allowing civil fine of \$2,500 per affected consumer, up to \$100,000).

28. California's law and others like it require notice to any person whose data "was, or is reasonably believed to have been, acquired by an unauthorized person" without regard to whether the breach is likely to cause harm to the data subject. CAL. CIV. CODE § 1798.82(a) (West Supp. 2008). See also MINN. STAT. § 325E.61, subd. 1(a) (2006); N.Y. GEN. BUS. LAW § 899-aa(2) (McKinney Supp. 2008). Some states allow data handlers to avoid disclosure if they believe the breach does not pose a risk of harm. See, e.g., DEL. CODE ANN. tit. 6, § 12B-102(a) (2005) (requiring disclosure only when, after a good-faith internal investigation, the data handler determines that misuse of the information is "reasonably likely"); FLA. STAT. ANN. § 817.5681(10)(a) (West 2006) (permitting nondisclosure if, after consultation with relevant law enforcement, the organization determines that the breach "will not likely result in harm"); N.J. STAT. ANN. § 56:8-163(a) (West Supp. 2007) (exempting notification if the breached entity "establishes that misuse of the information is not reasonably possible").

that trigger the laws,²⁹ and the causes of action they allow.³⁰ Critics cite this “patchwork” of state requirements as a major problem with data breach notification laws.³¹ Despite some arguments calling for a uniform national data breach notification standard,³² Congress has yet to pass such a law.³³

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.³⁴ 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(e) (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.*, 1 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).

32. *See, e.g.*, Kathryn E. Picanso, Note, *Protecting Information Security Under a Uniform Data Breach Notification Law*, 75 FORDHAM L. REV. 355, 389 (2006); Lilia Rode, Comment, *Database Security Breach Notification Statutes: Does Placing the Responsibility on the True Victim Increase Data Security?*, 43 HOUS. L. REV. 1597, 1631–33 (2007).

33. *See* Brendan St. Amant, *The Misplaced Role of Identity Theft in Triggering Public Notice of Database Breaches*, 44 HARV. J. ON LEGIS. 505, 510–14 (2007); John B. Kennedy & Anne E. Kennedy, *What Went Wrong? What Went Right? Corporate Responses to Privacy and Security Breaches*, 903 PLI/PAT 11, 26 (2007).

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

1. Notification

Data breach laws aim to notify consumers when their data might be at risk.³⁵ The constant stream of breach announcements shows that, if nothing else, the laws do that much.³⁶ Data breach notification laws force breached entities to warn people whose data may have been compromised, giving consumers the chance to protect themselves.³⁷ Yet these announcements happen so frequently, they may have lost effectiveness.³⁸ In one survey, almost forty percent of respondents said they mistook breach notification letters for junk mail.³⁹

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.⁴⁰

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.⁴¹ 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.⁴² 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.⁴³ Breached data brokers, like ChoicePoint, never asked consumers if it could gather their data and consumers could do little to prevent it.⁴⁴ 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.

37. Schwartz & Janger, *supra* note 9, at 936–37.

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)).

40. See Daniel J. Solove, *Identity Theft, Privacy, and the Architecture of Vulnerability*, 54 HASTINGS L.J. 1227, 1234–38 (2003).

41. STEVEN G. BREYER, REGULATION AND ITS REFORM 164 (1982).

42. *Id.*

43. See Solove, *supra* note 40, at 1251–55.

44. See Daniel J. Solove & Chris Jay Hoofnagle, *A Model Regime of Privacy Protection*, 2006 U. ILL. L. REV. 357, 362–66 (2006) (observing that data brokers do not allow data subjects to opt out of having their data collected and distributed).

nothing to help consumers choose to work with businesses who will be careful with their data.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.⁴⁶ Most organizations choose to invest in security measures when doing so is, predictably and measurably, less expensive than not doing so.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.⁴⁸ Poor or incomplete information can lead to irrational choices. Put more succinctly: “Garbage in, garbage out.”⁴⁹

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

45. See Schwartz & Janger, *supra* note 9, at 947–48.

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).

47. See John C. P. Goldberg, *Twentieth-Century Tort Theory*, 91 GEO. L.J. 513, 545 (2003). Businesses often follow this cost-benefit or return on investment approach when evaluating investments in security. See, e.g., Huseyin Cavusoglu, Birendra Mishra & Srinivasan Raghunathan, *A Model for Evaluating IT Security Investments*, COMM. ACM, July 2004, at 87, 87–88; Judy Greenwald, *Cost/Benefit Analysis, Access Crucial to Data Security*, BUS. INS., May 23, 2005, at 18; Doug Lewis, *Selling Security to the CFO*, COMPUTERWORLD, Oct. 13, 2003, at 46.

48. See, e.g., David A. Hoffman & Michael P. O’Shea, *Can Law and Economics Be Both Practical and Principled?*, 53 ALA. L. REV. 335, 360–61 (2002); Gregory Mitchell, *Taking Behavioralism Too Seriously? The Unwarranted Pessimism of the New Behavioral Analysis of Law*, 43 WM. & MARY L. REV. 1907, 1913–29 (2002) (discussing criticisms of the rationality theory).

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).

50. See, e.g., Greg Shipley, *Desperately Seeking the Security ROI*, NETWORK COMPUTING, May 27, 2002, at 35; KEVIN J. SOO HOO, *HOW MUCH IS ENOUGH? A RISK-MANAGEMENT APPROACH TO COMPUTER SECURITY* 29–46 (June 2000)

data security studies have serious methodological problems,⁵¹ oversimplify,⁵² or do not claim to provide predictive data.⁵³ Without this data, the probability of a security event and its financial impact are unknown.⁵⁴ An organization's practices regarding uncertainty, therefore, dominate its approach to data security.⁵⁵ Organizations that are risk-averse will over-spend on security,⁵⁶ those that seek risk will under-spend on security, and the risk-neutral will fall in a random distribution somewhere in the middle.⁵⁷

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

(Consortium for Research of Information Security and Policy Working Paper), available at <http://iis-db.stanford.edu/pubs/11900/soohoo.pdf> (discussing the lack of useful security data).

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://gocsi.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 Acohidio & 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.⁵⁸ Equipment purchases and labor expenses, for example, are both hard-dollar costs.⁵⁹ Productivity savings are soft-dollar gains.⁶⁰ Security investments almost always combine hard-dollar costs with soft-dollar savings.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.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.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,⁶⁴ and through civil actions and

58. See, e.g., April L. Dmytrenko, *Cost Benefit Analysis*, RECORDS MGMT. Q., Jan. 1997, at 16–17.

59. *Id.*

60. *Id.*

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.

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.

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.

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.⁶⁵ The FTC has exercised this right in a number of cases.⁶⁶ Although FTC notification requirements raise the probable costs of a security incident, they do not improve those costs' predictability.

3. Cost Shifting

For most owners of large databases, the risk of poor data security is a negative externality.⁶⁷ The data subject bears the primary risk of data loss but has no ability to protect her own data.⁶⁸ The database owner can protect the data but may not have economic incentives to do so.⁶⁹ By shifting costs of a breach from consumers to database owners, laws can internalize those externalities.⁷⁰ Current data breach laws do little or nothing to shift these costs.⁷¹ Their textual provisions rarely provide direct compensation to data subjects,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.⁷³ Common law negligence and constitutional standing require plaintiffs to suffer genuine harm from the

65. See 15 U.S.C. § 45(l)-(m) (2000).

66. See, e.g., *In re* CardSystems Solutions, Inc., No. 052-3148, 2006 WL 515749 (F.T.C. Feb. 23, 2006); *In re* DSW, Inc., No. 052-3096, 2005 WL 3366974 (F.T.C. Dec. 1, 2005); *In re* BJ's Wholesale Club, No. 042-3160, 2005 WL 2395788 (F.T.C. Sept. 20, 2005).

67. See Dennis D. Hirsch, *Protecting the Inner Environment: What Privacy Regulation Can Learn from Environmental Law*, 41 GA. L. REV. 1, 28-29 (2006).

68. See Solove & Hoofnagle, *supra* note 44, at 362-66.

69. See discussion *supra* Part II.B.2.

70. See Goldberg, *supra* note 47, at 545.

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, *supra* note 2, at 35.

72. See Ian C. Ballon, *A Legal Analysis of State Security Breach Statutes*, 903 PRAC. L. INST.: PATS., COPYRIGHTS, TRADEMARKS, & LITERARY PROP. COURSE HANDBOOK SERIES 135, 155-58 (June-July 2007) (discussing remedies for noncompliance in various state breach notification statutes).

73. See Denis T. Rice, *Increased Civil Litigation Over Privacy and Security Breaches*, 902 PRAC. L. INST.: PATS., COPYRIGHTS, TRADEMARKS, & LITERARY PROP. COURSE HANDBOOK SERIES 149, 173-77 (June-July 2007) (describing plaintiffs' difficulties showing cause-in-fact and harm in data mishandling lawsuits).

defendant's alleged conduct.⁷⁴ 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.⁷⁵

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.⁷⁶ Police often cannot find the perpetrators of individual-level fraud.⁷⁷ These factors can prevent identity fraud victims from tracing the misused data back to a data breach.⁷⁸ 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).

75. See *Kahle v. Litton Loan Servicing, LP*, 486 F. Supp. 2d 705, 709–13 (S.D. Ohio 2007) (stating that “courts have embraced the general rule that an alleged increase in risk of future injury is not an ‘actual or imminent’ injury,” therefore, plaintiffs do not have standing in such identity theft cases); *Hendricks v. DSW Shoe Warehouse, Inc.*, 444 F. Supp. 2d 775, 779 (W.D. Mich. 2006) (stating that the plaintiff did not claim any *cognizable* damages as a result of a data theft); *Forbes v. Wells Fargo Bank, N.A.*, 420 F. Supp. 2d 1018, 1020–21 (D. Minn. 2006) (citing the rule that the perceived risk of future harm—as opposed to a “reasonably certain future injury”—will not satisfy the damages requirement). *But see* *Guin v. Brazos Higher Educ. Serv. Corp.*, No. Civ. 05-668 RHK/JSM, 2006 WL 288483, at *3–5 (D. Minn. Feb. 7, 2006) (finding a duty of care under the Gramm-Leach Bliley Act, but one that did not extend to a duty to encrypt the contents of a laptop, which was later stolen); *Bell v. Mich. Council 25 of Am. Fed’n of State, County, & Mun. Employees, AFL-CIO, Local 1023*, No. 246684, 2005 WL 356306, at *1–6 (Mich. Ct. App. Feb. 15, 2005) (allowing negligence claims resulting from misuse of inadequately safeguarded personal information). Note that *Bell v. Michigan Council* involved clear cause-in-fact and harm (fraud by the defendant’s treasurer’s daughter). *Id.*

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.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.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.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.⁸² Courts have rejected these claims, finding that the costs have been incurred in mere anticipation of possible future harm.⁸³ Given the lack of other direct, measurable harms from data breaches,⁸⁴ plaintiffs continue to test the boundaries of damage theories.⁸⁵

79. *Stollenwerk v. Tri-West Healthcare Alliance*, No. Civ. 03-0185PHXSRB, 2005 WL 2465906, at *1 (D. Ariz. Sept. 6, 2005), *aff'd in part and rev'd in part*, No. 05-16990, 2007 WL 4116068 (9th Cir. Nov. 20, 2007).

80. *Id.* at *7.

81. *Stollenwerk v. Tri-West Health Care Alliance*, No. 05-16990, 2007 WL 4116068, at *3–4 (9th Cir. Nov. 20, 2007).

82. *See, e.g.,* *Pisciotta v. Old Nat'l Bancorp*, 499 F.3d 629 (7th Cir. 2007); *Kahle v. Litton Loan Servicing, LP*, 486 F. Supp. 2d 705, 709–13 (S.D. Ohio 2007); *Bell v. Acxiom, Corp.*, No. 4:06CV00485-WRW, 2006 WL 2850042 (E.D. Ark. Oct. 3, 2006); *Hendricks v. DSW Shoe Warehouse, Inc.*, 444 F. Supp. 2d 775, 779 (W.D. Mich. 2006); *Forbes v. Wells Fargo Bank, N.A.*, 420 F. Supp. 2d 1018, 1020–21 (D. Minn. 2006); *Stollenwerk*, 2005 WL 2465906, at *2–3.

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).

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).

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.⁹¹

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 Pisciotto*, 499 F.3d at 638–39 (comparing claims for credit monitoring to requirements for recovery in toxic tort risk cases).

86. *See Pa. State Employees Credit Union v. Fifth Third Bank*, 398 F. Supp. 2d 317, 322 (M.D. Pa. 2005).

87. *Id.* *See also* discussion *supra* note 13.

88. *See In re BJ's Wholesale Club, Inc.*, No. 042-3160, 2005 WL 2395788 (F.T.C. Sept. 20, 2005).

89. *Pa. State Employees Credit Union*, 398 F. Supp. 3d at 322.

90. *Id.* An "acquiring bank" processes credit card transactions for a merchant. *See* discussion *infra* Part III.A.

91. *Pa. State Employees Credit Union*, 398 F. Supp. 3d at 322.

92. *Id.* at 327–31.

93. *Id.* at 326–30. 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).

94. *Pa. State Employees Credit Union*, 398 F. Supp. 3d at 338.

95. *Pa. State Employees Credit Union v. Fifth Third Bank*, No. 1:CV-04-1554, 2006 WL 1724574, at *1, *13 (M.D. Pa. June 16, 2006) (granting summary judgment for Fifth Third Bank on the third party beneficiary claims that remained after the court had granted a motion to dismiss on all other claims).

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

96. See Douglas Akers et al., *Overview of Recent Developments in the Credit Card Industry*, 17 FDIC BANKING REV., No. 3, at 25 (2005), available at <http://www.fdic.gov/bank/analytical/banking/2005nov/article2.pdf> (describing the corporate composition of the major credit card brands).

97. See, e.g., *Pa. State Employees Credit Union*, 2006 WL 1724574 at *2 (discussing Visa's relationship with the plaintiff and defendant financial institutions). American Express, Discover, and JCB use a different model: they issue credit cards and process merchant transactions themselves without the participation of other financial institutions. See Steven Semeraro, *Credit Card Interchange Fees: Three Decades of Antitrust Uncertainty*, 14 GEO. MASON L. REV. 941, 946-47 (2007).

98. See *id.* at *2 (discussing Visa's relationship with the plaintiff and defendant financial institutions).

99. See Corporate.Visa.com, *Understanding Payment Transactions*, <http://www.corporate.visa.com/md/fs/corporate/transactions.jsp> (last visited Feb. 3, 2008).

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.¹⁰¹ 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.¹⁰²

Card association membership contracts require banks to comply with the association Operating Regulations and the PCI DSS.¹⁰³ PCI DSS is a set of technical and business process requirements for anyone who processes, handles, or stores credit card information.¹⁰⁴ Visa, Mastercard, Discover, JCB, and American Express jointly developed PCI DSS and created the PCI Security Standards Council to manage the standard.¹⁰⁵ The individual card brands enforce compliance.¹⁰⁶ 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.¹⁰⁷ The acquiring bank usually passes this fine to the merchant whose poor security caused the violation.¹⁰⁸

Unlike many industry and government security standards that speak in generalities and leave room for interpretation,¹⁰⁹ PCI DSS sets specific requirements. It requires particular methods of encryption,¹¹⁰ prescribes network security technologies and configurations,¹¹¹ and demands or forbids certain practices.¹¹² One

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.

104. See PCI Security Standards Council, About the PCI DSS, available at <https://www.pcisecuritystandards.org/tech/index.htm> (last visited Feb. 4, 2008).

105. PCI Security Standards Council, Frequently Asked Questions, available at <https://www.pcisecuritystandards.org/about/faqs.htm> (last visited Feb. 4, 2008).

106. *Id.*

107. Mike Petitti, *Community Banks Benefit from Awareness of Payment Card Security*, CMTY BANKER, Apr. 2007, at 32. See, e.g., Press Release, Visa Inc., Visa USA Pledges \$20 Million in Incentives to Protect Cardholder Data (Dec. 12, 2006), available at <http://corporate.visa.com/md/nr/press667.jsp>.

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.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.¹¹⁴

Despite low early compliance with PCI DSS, merchants appear to be making progress in satisfying its security requirements.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.¹¹⁶ That statistic only addresses one PCI DSS requirement; large merchants continue to struggle to comply with the rest of PCI DSS's requirements.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.¹¹⁸ The law implements, in a modified form, the

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

113. *Id.* at 5. *See also supra* note 13 and accompanying text.

114. PCI DSS, *supra* note 14, at 5.

115. *See* Evan Schuman, *Have Retailers Given Up on PCI Compliance?*, EWEEK, May 10, 2007, *available at* <http://www.eweek.com/c/a/Retail/Have-Retailers-Given-Up-on-PCI-Compliance/>.

116. Press Release, Visa Inc., *Visa Marks Progress in Securing Merchant Systems* (July 30, 2007), *available at* <http://corporate.visa.com/md/nr/press719.jsp>. Large merchants are those that process over one million transactions per year. *Id.*

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.*

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/tlodocs/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.¹¹⁹ 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.¹²⁰

The law creates a private cause of action for financial institutions to recover from entities that fail to meet the statute's requirements.¹²¹ It requires a breached entity to reimburse certain costs that a financial institution incurs related to the breach,¹²² offset by any reimbursement the financial institution receives from a credit card company.¹²³

Other states have proposed similar bills, but none had become law as of October 2007.¹²⁴ 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.eweek.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.¹²⁵ A statute must tread a fine line between generality and specificity.¹²⁶ Make it too broad, and it risks interpretations contrary to the intent of the law.¹²⁷ If it is too specific, tying itself to the technology of the time, it can become outdated or require legislative reconsideration when technology changes.¹²⁸ 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.¹²⁹ It applies to payment cards, but not other sensitive personal data such as bank account numbers or Social Security numbers.¹³⁰ It prohibits

125. See, e.g., Matt Hines, *Policy Experts Split on Spyware Laws*, INFOWORLD, June 28, 2007, available at http://www.infoworld.com/article/07/06/28/Policy-experts-split-on-spyware-laws_2.html (discussing the difficulties in drafting anti-spyware legislation).

126. See, e.g., Allison W. Freedman, Note, *The Electronic Signatures Act: Preempting State Law by Legislating Contradictory Technology Standards*, 2001 UTAH L. REV. 807, 813 (2001) (noting the contrasting technology-specific and technology-neutral approaches to digital signature laws).

127. See, e.g., ELEC. FRONTIER FOUND., UNINTENDED CONSEQUENCES: SEVEN YEARS UNDER THE DMCA 1-3 (2006), available at http://www.eff.org/files/DMCA_unintended_v4.pdf (discussing unintended consequences of the Digital Millennium Copyright Act); Hines, *supra* note 125 (noting pursuit of lawsuits lacking under the broad SafeWeb Act).

128. See, e.g., Health Insurance Reform: Security Standards, 68 Fed. Reg. 8334, 8357 (Feb. 20, 2003) (to be codified at 45 C.F.R. pts. 160, 162, & 164) (noting that "rapidly changing technology makes it impractical and inappropriate to name a specific [encryption] technology" in administrative regulations); Laura Hildner, Note, *Defusing the Threat Of RFID: Protecting Consumer Privacy Through Technology-Specific Legislation at the State Level*, 41 HARV. C.R.-C.L. L. REV. 133, 167 (2006) (discussing criticisms of technology specific legislation as too slow to keep up with changing technology).

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.¹³¹ 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,¹³² but loses some of that flexibility when it limits those access devices to cards¹³³ and describes security codes as three or four-digit values.¹³⁴ 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.¹³⁵

The law differs from PCI DSS in a number of ways.¹³⁶ 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. Shelfer & J. Drew Procaccino, *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. MINN. 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.¹³⁷ Minnesota Statutes section 325E.64 only adopts the element of the standard prohibiting storage of "sensitive authentication data."¹³⁸ PCI DSS is much broader than that one requirement, however, reflecting the wide range of business processes and controls necessary to ensure data security.¹³⁹

Fortunately for merchants, Minnesota's law differs from PCI DSS by being more permissive.¹⁴⁰ Unlike PCI DSS, it allows a forty-eight hour window for storing debit card information after a transaction.¹⁴¹ It may also allow entities to avoid liability by encrypting full track data,¹⁴² a practice PCI DSS prohibits.¹⁴³ 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.¹⁴⁴ 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.¹⁴⁵

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

contractual agreement public 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.¹⁴⁶ 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.¹⁴⁷ As such, the statute is a direct salvo at the BJ's Wholesale result, and a look forward to the pending TJX litigation.¹⁴⁸ 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.¹⁴⁹ The court denied all of PSECU's claims for relief.¹⁵⁰ 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.¹⁵¹

Some have argued that the law is unnecessary.¹⁵² Card Association Operating Agreements already require anyone handling credit card data to meet PCI DSS requirements.¹⁵³ Everyone involved in a payment card transaction has a contract with someone else and could establish rules for liability and reimbursement by contract.¹⁵⁴ 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.

148. See *In re TJX Cos. Retail Sec. Breach Litigation*, No. 07-10162-WGY, 2007 WL 2982994, at *1 (D. Mass. Oct. 12, 2007); *Pa. State Employees Credit Union v. Fifth Third Bank*, 398 F. Supp. 2d 317, 321 (M.D. Pa. 2005). Cf. *Pa. State Employees Credit Union v. Fifth Third Bank*, No. 1:CV-04-1554, 2006 WL 1724574, at *13 (M.D. Pa. June 16, 2006).

149. *Pa. State Employees Credit Union*, 398 F. Supp. 2d at 321.

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.

153. *Pa. State Employees Credit Union*, 2006 WL 1724574, at *3. The PSECU case discusses Visa's integration of its Cardholder Information Security Program (CISP) into its Operating Agreements. *Id.* CISP is a Visa-specific program that started in 2001 and was incorporated into PCI DSS when the latter industry-wide standard arose in 2004. See Visa USA, Cardholder Information Security Program, http://usa.visa.com/merchants/risk_management/cisp_overview.html (last visited Feb. 10, 2008).

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.¹⁵⁵ In fact, the Operating Regulations contain just this sort of provision.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.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 1993,¹⁵⁸ yet fourteen years later full track storage is still a problem.¹⁵⁹ Moreover, the Operating Regulations do not cover all the forms of loss that the Minnesota law does.¹⁶⁰ For example, the Operating Regulations allow reallocation of losses for fraud, but not for "operational costs" such as replacing lost credit cards.¹⁶¹ Visa also retains sole control over all disputes between member financial institutions under the Operating Regulations.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.

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.

156. *Pa. State Employees Credit Union*, 2006 WL 1724574, at *5.

157. *Id.* Visa also levied \$555,000 in fines against Fifth Third Bank for violations of the Operating Regulations. *Id.* Those fines were not redistributed to issuers. *Id.*

158. *Id.* at *7.

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. See Press Release, Visa Inc., Visa Marks Progress in Securing Merchant Systems (July 30, 2007), available at <http://corporate.visa.com/md/nr/press719.jsp>.

160. See MINN. STAT. § 325E.64 (Supp. 2007); *Pa. State Employees Credit Union*, 2006 WL 1724574, at *4-5 (describing Visa's Operating Regulations).

161. *Pa. State Employees Credit Union*, 2006 WL 1724574, at *4-5.

162. *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. *Id.* at *6.

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.¹⁶³ Second, it should compensate victims who suffer actual harm.¹⁶⁴ Third, the law should be flexible enough to remain relevant as technology changes.¹⁶⁵ Fourth, any related statutes of limitations or repose should allow recovery when breach-related fraud is discovered.¹⁶⁶ Finally, the law should ameliorate the difficulty of proving cause-in-fact when a data breach has led to identity theft.¹⁶⁷

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.¹⁶⁸ 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” activities¹⁷⁵ such as explosive blasting,¹⁷⁶

food labeling requirements); RESTATEMENT (THIRD) OF TORTS: PROD. LIAB. § 7 (1998) (discussing common-law food product liability); Henry H. Drummonds, *The Dance of Statutes and the Common Law: Employment, Alcohol, and Other Torts*, 36 WILLAMETTE L. REV. 939, 989–90 (2000).

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.

170. See William M. Landes & Richard A. Posner, *The Positive Economic Theory of Tort Law*, 15 GA. L. REV. 851, 873–74 (1981), reprinted in 2 LAW AND ECONOMICS 259, 281–82 (Richard A. Posner & Francesco Parisi eds., 1997). Much of this effect comes from the existence of contributory and comparative negligence, which each reduce the wrongdoer’s liability (either proportionally for comparative negligence or entirely for contributory negligence) according to the victim’s share of the fault for the accident. *Id.*

171. *Id.* at 282.

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

173. See Landes & Posner, *supra* note 170, at 283–324.

174. *Id.* at 285.

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

176. See, e.g., *Exner v. Sherman Power Const. Co.*, 54 F.2d 510, 513–14 (2d Cir. 1931) (applying strict liability to blasting).

handling of hazardous wastes,¹⁷⁷ and certain uses of poisons.¹⁷⁸ Whether an activity is “abnormally dangerous” rests in part on whether reasonable care can eliminate the risk involved in the activity.¹⁷⁹ The proper liability regime for data breaches therefore depends on whether they are the “inevitable byproduct” of data collection,¹⁸⁰ or whether they can be reduced by the application of due care.¹⁸¹

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.¹⁸² Manufacturing defects generate strict liability causes of action because those defects are seen as inherent and unavoidable when manufacturing products.¹⁸³ 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.¹⁸⁴

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,¹⁸⁵ stored unencrypted card data,¹⁸⁶ failed to verify that certain customers actually were small businesses instead of data thieves,¹⁸⁷ or did not use “simple, low-cost, and

177. See, e.g., *Sterling v. Velsicol Chem. Corp.*, 647 F. Supp. 303, 313 (W.D. Tenn. 1986) (applying strict liability to chemical maker that buried toxic waste near a water source), *rev'd on other grounds*, 855 F.2d 1188 (6th Cir. 1988).

178. See, e.g., *Langlois v. Allied Chem. Corp.*, 249 So. 2d 133, 139 (La. 1971) (applying strict liability to storage of poisonous gas), *superseded by statute*, LA. CIV. CODE ANN. art. 2323 (1980), *as recognized in* *Murray v. Ramada Inns, Inc.*, 521 So. 2d 1123 (La. 1988); *Luthringer v. Moore*, 190 P.2d 1, 5 (Cal. 1948) (holding fumigator to a strict liability standard).

179. RESTATEMENT (SECOND) OF TORTS § 520 (1979).

180. Danielle Keats Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 S. CAL. L. REV. 241, 264–65 (2007).

181. See, e.g., Vincent R. Johnson, *Cybersecurity, Identity Theft, and the Limits of Tort Liability*, 57 S.C. L. REV. 255, 276–78 (2005) (arguing in favor of a negligence-based theory of data security liability).

182. See RESTATEMENT (THIRD) OF TORTS: PRODUCTS LIABILITY § 2 cmt. o (1998).

183. See *id.* § 2 cmt. a.

184. See *id.*

185. See, e.g., *In re CardSystems Solutions, Inc.*, No. 052-3148, 2006 WL 515749 (F.T.C. Feb. 23, 2006); *In re DSW, Inc.*, No. 052-3096, 2005 WL 3366974 (F.T.C. Dec. 1, 2005); *In re BJ's Wholesale Club, Inc.*, No. 042-3160, 2005 WL 2395788 (F.T.C. Sept. 20, 2005).

186. See *In re DSW, Inc.*, No. 052-3096, 2005 WL 3366974 (F.T.C. Dec. 1, 2005); *In re BJ's Wholesale Club, Inc.*, No. 042-3160, 2005 WL 2395788 (F.T.C. Sept. 20, 2005).

187. See Tom Zeller, Jr., *Release of Consumers' Data Spurs ChoicePoint Inquiries*,

readily available” methods of avoiding software application attacks.¹⁸⁸ Other breaches involved un-patched software,¹⁸⁹ weak user IDs and passwords,¹⁹⁰ and postings of confidential data to the Internet.¹⁹¹ 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,¹⁹² lost or stolen laptops,¹⁹³ disks lost in the mail,¹⁹⁴ or lost backup tapes.¹⁹⁵ In at least some of these cases, data was lost despite arguably careful handling,¹⁹⁶ 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

N.Y. TIMES, Mar. 5, 2005, at C2.

188. *In re CardSystems Solutions, Inc.*, No. 052-3148, 2006 WL 515749 (F.T.C. Feb. 23, 2006).

189. See Press Release, Univ. of Colo., CU-Boulder Arts and Scis. Server Hacked on May 12 (May 22, 2007), available at <http://www.colorado.edu/news/releases/2007/224.html>.

190. See Heather Timmons, *Security Breach at LexisNexis Now Appears Larger*, N.Y. TIMES, Apr. 13, 2005, at C7.

191. See Stewart Verney, *Credit Union Paying for ID Theft Protection After Info Error*, JACKSONVILLE BUS. J., June 1, 2007, available at <http://jacksonville.bizjournals.com/jacksonville/stories/2007/05/28/daily24.html>.

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).

194. See, e.g., Andy Miller & Bill Hendrick, *Georgians' Personal Data Lost*, ATLANTA J.-CONST., Apr. 11, 2007, at A1.

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.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,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.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.²⁰⁰

197. U.S. v. Carroll Towing Co., 159 F.2d 169, 173 (2d Cir. 1947).

198. See Citron, *supra* note 180, at 263–64 (discussing the “uncertainty dilemma” of economic theories of negligence law).

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. McMenemy & Severson, 590 N.W.2d 641, 643 n.16 (Minn. 1999) (citation omitted).

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.²⁰¹ Some breached data never expires,²⁰² and misuse often creates no noticeable signs.²⁰³ Many victims of identity theft find out about it only when they are denied credit²⁰⁴ or even arrested.²⁰⁵ 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.²⁰⁶ These factors suggest that Minnesota's default six-year statute of limitations for tort claims²⁰⁷ 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.²⁰⁸ 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>.

206. See FED. TRADE COMM'N, *IDENTITY THEFT COMPLAINT DATA: JANUARY 1–DECEMBER 31, 2006* fig.8 (2007), available at http://www.ftc.gov/bcp/edu/microsites/idtheft/downloads/clearinghouse_2006.pdf (summarizing 2006 statistics from the FTC's Identity Theft Data Clearinghouse).

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

208. See, e.g., *Herrmann v. McMenemy & 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

cases of fraud).

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.”).

214. See Erik S. Knutsen, *Ambiguous Cause-in-Fact and Structured Causation: A Multi-Jurisdictional Approach*, 38 TEX. INT'L L.J. 249, 262–63 (2003) (discussing the so-called “reversal” cause-in-fact doctrine).

otherwise be difficult to prove,²¹⁵ and statutes have adopted it for similar purposes.²¹⁶

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.²¹⁷ The defendant could rebut the presumption by showing another likely source of the misused data.²¹⁸ 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.²¹⁹ 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.

217. See Richard W. Wright, *Causation in Tort Law*, 73 CAL. L. REV. 1735, 1788–91 (1985) (discussing the “necessary element of a sufficient set” test of causality).

218. See *Zuchowicz*, 140 F.3d at 390–91.

219. See Wright, *supra* note 217, at 1788–89.