# Data Breach: From Notification to Prevention Using PCI DSS

ABRAHAM SHAW*

*With over 350 million records containing sensitive personal information having been compromised since 2005, it is evident that data breaches are an epidemic problem. After demonstrating the security breach problem, the Note begins by discussing California's pioneering data breach notification law, which requires breached entities to notify those affected that their personal information has been compromised. Drawing on various provisions found in California's notification law, the Note evaluates current state and federal data breach laws. To further explore the relationship between federal and state enforcement, two recent data breaches, the ChoicePoint and TJX breaches, are discussed in-depth. The Note then examines proposed federal and state legislation to strengthen the argument that data breach laws, which currently focus on notification, must also advance to breach prevention. Finally, the Note proposes a solution for preventing data breaches by increasing liability for merchants who fail to meet heightened security standards based on those used in the credit card industry.*

## I. INTRODUCTION

In an age when internet transactions have become a part of everyday life, both individual users and corporations have become more sophisticated. Users who used to receive content only passively now actively engage in e-commerce. Companies that used to only keep paper files now maintain digital databases worldwide. Because private information is increasingly available over

* Farnsworth Notes Writing Competition Winner, 2009–2010. J.D. Candidate 2010, Columbia Law School. The author would like to thank his wife Monica for her love and support as well as Professors Julie Brill and James Tierney for their gracious help with this Note.

the internet, there is a rising demand for data breach laws that protect private information.

Approximately eighty to ninety percent of Fortune 500 companies and government agencies have experienced data breaches.[1] Since January 2005, over 350 million records containing sensitive personal information have been compromised in data breaches.[2] The leading cause of these security breaches is hacker intrusion, followed by stolen laptops and computers, and insider thefts of private information.[3] Terrorists have also increasingly utilized the internet not only to communicate and recruit, but also to perpetrate online crimes to obtain financial support for their agendas.[4] Furthermore, data breaches often result in fraud. The Internet Crime Complaint Center reported that fraud-related losses totaled $264.6 million in 2008, up from $239.1 million in 2007.[5] These figures only address *reported* losses; computer crime experts agree that most computer-related crimes go either undetected or unreported.[6] With personal information being compromised almost daily in data breaches,[7] the main question

---

1. Jones Day LLP, Security Breach Notification Requirements: Guidelines and Securities Law Considerations (Mar. 2006), http://www.jonesday.com/pubs/pubs_detail.aspx?pubID=S3225 (last visited May 11, 2010).

2. The U.S. Privacy Rights Clearinghouse reported that, to its knowledge, from January 2005 to May 4, 2010, 354,140,197 records containing sensitive personal information were involved in security breaches in the U.S. Privacy Rights Clearinghouse, Chronology of Data Breaches, http://www.privacyrights.org/ar/ChronDataBreaches.htm (last visited May 11, 2010).

3. Jay Cline, *Lessons Learned from Corporate Security Breaches*, COMPUTERWORLD, Aug. 9, 2005, http://www.computerworld.com/securitytopics/security/story/0,10801,103733,00.html.

4. *See, e.g.*, Todd M. Hinnen, *The Cyber-Front in the War on Terrorism: Curbing Terrorist Use of the Internet*, 5 COLUM. SCI. & TECH. L. REV. 5, 9 (2004) (noting that terrorists perpetrate online crimes to support their missions).

5. INTERNET CRIME COMPLAINT CTR., FED. BUREAU OF INVESTIGATION & NAT'L WHITE COLLAR CRIME CTR., 2008 INTERNET CRIME REPORT 1 (2008), http://www.ic3.gov/media/annualreport/2008_IC3Report.pdf. The Internet Crime Complaint Center, which the FBI and National White Collar Crime Center began operating jointly in May 2000, is a clearinghouse for various cyber-crime complaints and is designed to track the prevalence of internet fraud in the U.S. *Id.* at 2.

6. Scott Charney, *The Internet, Law Enforcement and Security*, *in* FIFTH ANNUAL INTERNET LAW INSTITUTE, at 937, 943–44 (PLI Patents, Copyrights, Trademarks, and Literary Prop., Course Handbook Series No. 662, 2001).

7. U.S. Privacy Rights Clearinghouse, *supra* note 2 (reporting 100 data breaches in the 127 day span from January 1, 2010 to May 7, 2010); *see also* Cline, *supra* note 3 (reporting that personal information was being compromised every three days in 2005).

is: what are state and federal governments doing about this problem?

Having demonstrated that a security breach problem exists, this Note will go on to describe the current state and federal laws addressing the problem, highlight certain enforcement actions that have been undertaken in response to the problem, and, finally, propose that lawmakers craft legislation that focuses not only on notification of injured parties and damage control but also on data breach prevention. Part II begins by discussing California's pioneering data breach law and then draws on that law to evaluate current state data breach laws. Part III examines the current federal laws addressing data breach issues, specifically the Gramm-Leach-Bliley Act and various Federal Trade Commission acts. Part IV illuminates the need for legislation that goes beyond requiring consumer notification after data breaches to prevent such breaches. This section also explores the relationship between federal and state data breach laws using the Choice Point and TJX breaches. Part V discusses pending state and federal legislation to demonstrate that data breach laws need to progress toward preventing data breaches. Finally, Part VI proposes a solution: data breaches can be prevented by increasing liability for merchants who fail to meet heightened security standards based on those used in the credit card industry.

## II. STATE DATA BREACH LAWS

In response to increasing data breaches, many states have enacted data breach notification laws. Some commentators argue that this has resulted in a medley of unrelated statutes and regulations that are difficult to comply with.[8] Yet, as this section explains, there is actually a common thread that runs through state notification laws: requiring entities that lose personal information to notify those affected. California led the charge by passing a notification law, the California Computer Security Act of 2002, which requires public disclosure of security incidents.[9] Forty-five states, the District of Columbia, Puerto Rico, and the Virgin Isl-

8. *See* Glen Fest, *Data Breach Notification: States Differ on When to Sound the Alarm*, BANK TECH. NEWS, Jan. 2006, http://www.americanbanker.com/btn_issues/19_1/-267017-1.html.

9. CAL. CIV. CODE §§ 1798.82–.84 (West 2010).

ands followed suit.[10] Only four states currently do not have a security breach law.[11] This section will first present the history and provisions of the California security breach law before evaluating other states' laws.

## A. CALIFORNIA COMPUTER SECURITY ACT

The California data breach notification law is significant because it was the first such state law. It has since served as a backdrop and model for many states that have emulated it. The policy impetus behind the California law was the realization that "the privacy and financial security of individuals is increasingly at risk due to the ever more widespread collection of personal information by both the private and public sector."[12] The California legislature unanimously passed the law in response to a security breach at the Stephen P. Teale Data Center, which exposed the personal information of 260,000 state employees, including 120 state legislators.[13] California lawmakers were concerned not only about the damage that the loss of credit card information would cause to contractual relations between cardholders and credit card companies, but also about empowering consumer victims whose personal data had been stolen.[14] Providing consumers with early notice that their personal information has been breached enables them to cancel credit cards and alert credit bureaus to prevent further fraud.[15]

The California notification statute has six major components: coverage, notification trigger, notification mechanism, timeliness, remedies, and enforcement.[16] Regarding coverage, the California law's scope is extremely broad, essentially covering anyone who

10. *See* National Conference of State Legislatures, State Security Breach Notification Laws (Apr. 12, 2010), http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm (last visited May 11, 2010).

11. Alabama, Kentucky, Mississippi, New Mexico, and South Dakota. *Id.*

12. S.B. 1386, 2001–2002 Leg., Reg. Sess. (Cal. 2002).

13. Deb Kollars, *U.S. Follows State's Lead on Data-Theft Notification*, SACRAMENTO BEE, June 22, 2005, at A1.

14. Timothy H. Skinner, *California's Database Breach Notification Security Act: The First State Breach Notification Law is Not Yet a Suitable Template for National Identity Theft Legislation*, 10 RICH. J.L. & TECH. 1 (2003).

15. *Id.* at 6.

16. CAL. CIV. CODE §§ 1798.80–.84 (West 2010).

does business in California[17] and any publicly available personal information.[18] A parallel statute also explicitly covers government entities.[19] Both statutes are limited, however, to "computerized" information.[20] A data breach triggers the notification statute. This breach is defined as "the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information" on the system.[21] The breach does not have to be reported unless the "unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person."[22]

Once a breach occurs, the breached entity has a duty to inform California residents[23] through written notice, electronic notice, or substitute notice.[24] In contrast to subsequently enacted laws,[25] there is no requirement in the triggering provision that the breach must be likely to cause harm to the consumers. Further, the disclosure must be made "in the most expedient time possible and without unreasonable delay"[26] According to the statute, it is reasonable to delay notification pending a company-initiated investigation, allowing the company time to evaluate the extent of the breach and restore system integrity.[27] Delaying notification is also proper if law enforcement determines it will impede a criminal investigation.[28]

---

17. § 1798.80(a) ("Business" is defined as "a sole proprietorship, partnership, corporation, association, or other group, however organized and whether or not organized to operate at a profit, including . . . an entity that disposes of records."); *see also* § 1798.82 (applying law to any person or business).

18. §§ 1798.82(e)–(f) (defined as a person's "first name (or first initial) and last name in combination with" the person's social security number; driver's license number or California Identification Card number; account number or credit or debit card number, in combination with any code that would permit access to a financial account, but not information lawfully made available to the general public from government records).

19. § 1798.29 (applying to any California state agency).

20. §§ 1798.29, 1798.82(a).

21. § 1798.82(d).

22. § 1798.82(a).

23. *Id.*

24. § 1798.82(g). "Substitute notice" allows breaching entities the option to email consumers, conspicuously post the notice on their Web site, or give notice through major statewide media, if it can demonstrate that the cost of regular notice would be more than $250,000, the affected class exceeds 500,000, or the entity has insufficient contact information. §1798.82(g)(3).

25. *See infra* Part II.B.

26. § 1798.82(a).

27. *Id.*

28. § 1798.82(c).

When noncompliance with the notification provision occurs, the California statute expressly provides injured consumers with a private right of action to recover damages,[29] along with possible injunctive relief against the statute-violating entity.[30] These rights and remedies are cumulative with respect to each other and to any other rights and remedies available under law.[31] Thus, the notification statute places no limits on other possible claims such as unfair business practices or misrepresentation (for example, privacy policies that guarantee safety of personal data)[32] and further allows the State Attorney General to prosecute the breaching entity under his general consumer protection powers.[33]

## B. STATE NOTIFICATION STATUTES ENACTED AFTER CALIFORNIA

While most states have emulated California's notification statute, others have created laws with different breach trigger levels, notification methods, specificity requirements, outside reporting requirements, and safe harbors.[34] Evaluating various state security breach laws leads to the conclusion that they are, on balance, rather harmonious.

---

29. § 1798.84(b).

30. § 1798.84(e).

31. § 1798.84(h).

32. Cheryl A. Falvey et al., *Disclosure of Security Breaches Required by New California Privacy Legislation*, METRO. CORP. COUNSEL, Aug. 1, 2003, at 5.

33. CAL. BUS. & PROF. CODE §§ 17200–17210 (West 2010). The statutes provide for public enforcement of the data breach laws by the California State Attorney General as part of his general consumer protection power over "unlawful, unfair or fraudulent business act[s] or practice[s]". § 17200. *See e.g.*, People v. CVS, Inc., Case No. 37-2000-0000-1517-CU-MC-CTL (Cal. Super. Ct. Jun. 10, 2009), *available at* http://ag.ca.gov/cms_attachments/press/pdfs/n1752_cvs_comp.pdf.

34. *See* CSO Disclosure Series, Data Breach Notification Laws, State by State (Feb. 12, 2008), http://www.csoonline.com/article/221322/CSO_Disclosure_Series_Data_Breach_Notification_Laws_State_By_State (last visited May 11, 2010) (containing a useful diagram of state notification laws with pertinent information regarding notification, private right of action, penalties, and exemptions). For a list of current state security breach statutes, see also the Web site of the National Conference of State Legislatures, *supra* note 10.

1. *Coverage*

Although every state breach notification law covers businesses, there are differences regarding coverage of other entities such as government agencies and third-party storage providers, as well as differences regarding the information each law defines as "personal." While some states do not apply their breach statute to government agencies, and others exempt only enforcement agencies, almost all states apply their breach statute to all governmental entities.[35] Additionally, although all states require notification if a person or business experiences a data breach, there are differences when third parties, such as data storage providers, lose the information. Third parties who have lost personal information are generally required only to notify and cooperate with the owner of the information (as opposed to directly notifying consumers), but a few states require notification even if the entity that experiences the breach does not own the information.[36] On the other hand, New York and New Jersey require no-

35. States that do not apply breach laws to government agencies include Colorado, COLO. REV. STAT. § 6-1-716 (2010); Connecticut, CONN. GEN. STAT. 36a-701b (2010); Delaware, DEL. CODE ANN. tit. 6, § 12B-102 (2010); Montana, MONT. CODE ANN. § 30-14-1704 (2010); and North Carolina, N.C. GEN. STAT. § 75-65 (2010). In Arizona, Georgia, and Vermont, the security breach laws apply to all governmental entities except enforcement agencies. ARIZ. REV. STAT. ANN. § 44-7501(L)(5) (2010); GA. CODE ANN. § 10-1-910 (2010); VT. STAT. ANN. tit. 9, § 2435 (2010) (exemption set to be replaced June 30, 2012).

36. The following state laws require notification if a person or business that does not own information experiences the breach: Alaska, ALASKA STAT. § 45.48.040 (2010); Iowa, IOWA CODE § 715C.2 (2010); Maine, ME. REV. STAT. ANN. tit. 10, § 1348 (2010); Massachusetts, MASS. GEN. LAWS ch. 93H, § 3(a) (2010); and Michigan, MICH. COMP. LAWS § 445.72 (2010). Notification only to the owner or licensee of the information is required in: Arizona, ARIZ. REV. STAT. ANN. § 44-7501 (2010); Arkansas, ARK. CODE ANN. § 4-110-105 (2010); California, CAL. CIV. CODE §1798.82 (West 2010); Colorado, COLO. REV. STAT. § 6-1-716 (2010); Connecticut, CONN. GEN. STAT. § 36a-701b(c) (2010); Delaware, DEL. CODE ANN. tit. 6, § 12B-102(b) (2010); District of Columbia, D.C. CODE § 28-3852(b) (2010); Florida, FLA. ST. ANN. § 817.5681(2) (West 2010); Georgia, GA. CODE ANN. § 10-1-912(b) (2010); Hawaii, HAW. REV. STAT. § 487N-2(b) (2010); Idaho, IDAHO CODE §§ 28-51-105(2) (2010); Illinois, 815 ILL. COMP. STAT. 530/10(b) (2010); Kansas, KAN. STAT. ANN. 50-7a02(b) (2010); Louisiana, LA. REV. STAT. ANN. § 51:3074(B) (2010); Maine, ME. REV. STAT. ANN. tit. 10, § 1348 (2010); Minnesota, MINN. STAT. § 325E.61(b) (2010); Montana, MONT. CODE ANN. § 30-14-1704(2) (2010); Nebraska, NEB. REV. STAT. § 87-803(2) (2010); Nevada, NEV. REV. STAT. § 603A.220(2) (2010); New Hampshire, N.H. REV. STAT. ANN. § 359-C:20(I)(c) (2010); New Jersey, N.J. STAT. ANN. § 56:8-163(b) (West 2010); New York, N.Y. GEN. BUS. LAW § 899-aa(3) (McKinney 2010); North Carolina, N.C. GEN. STAT § 75-65(b) (2010); North Dakota, N.D. CENT. CODE § 51-30-03 (2010); Ohio, OHIO REV. CODE ANN. § 1347.12(C) (West 2010); Oklahoma, OKLA. STAT. tit. 74, § 3113.1(B) (2010); Oregon, OR. REV. STAT. § 646A.600-628 (2010); Pennsylvania, 73 PA. STAT. ANN. § 2303(c) (West 2010);

tification to a designated state agency irrespective of who lost the information.[37] Regarding the data covered, most states follow California and cover only electronic data, but six states cover all media where personal information is stored, including paper records.[38] These state statutes may cover non-electronic data to protect against insider theft and dumpster-diving — that is, when paper documents containing personal information are improperly disposed of.

There are some variations among states concerning what qualifies as personal information, but most states have followed California's definition, which includes: a first name or initial and last name; one or more unencrypted elements, such as a social security number or an account number; and required passwords that would permit access to an individual's financial account.[39] North Dakota has expanded the definition of personal information to include mother's maiden name;[40] North Carolina has expanded it to include other identifying characteristics such as digital signa-

---

Rhode Island, R.I. GEN. LAWS § 11-49.2-3(b) (2010); South Carolina, S.C. CODE ANN. § 39-1-90(B) (2010); Tennessee, TENN. CODE § 47-18-2107(c) (2010); Texas, TEX. BUS. & COM. CODE ANN. § 521.053(c) (Vernon 2010); Utah, UTAH CODE ANN. §§ 13-44-202(3) (2010); Vermont, VT. STAT. ANN. tit. 9, § 2435(b)(2) (2010); Virginia, VA. CODE ANN. § 18.2-186.6(D) (2010); Washington, WASH. REV. CODE ANN. § 19.255.010 (LexisNexis 2010); West Virginia, W.VA. CODE ANN. § 46A-2A-102(c) (LexisNexis 2010); Wisconsin, WIS. STAT. ANN. § 134.98(2) (West 2010) and Wyoming, WYO. STAT. ANN. § 40-12-502(g) (2010).

37. N.J. STAT. ANN. § 56:8-163(c) (West 2010) (requiring reporting of breach to Division of State Police in the Department of Law and Public Safety for investigation or handling); N.Y. GEN. BUS. LAW § 899-aa(8) (McKinney 2010) (requiring notification to the State Office of Cyber Security and Critical Infrastructure Coordination as to the timing, content, and distribution of the notice and approximate number of affected persons). Other states, like Vermont, require this by regulation or guidance. Press Release, Vt. Dep't of Banking, Ins., Sec. & Health Care Admin., Attorney General Sorrell Issues Security Breach Notification Guidance (Apr. 24, 2007) (on file with author).

38. These states are Alaska, ALASKA STAT. § 45.48.010(a)(2010); Hawaii, HAW. REV. STAT. § 487N-2 (2010); Massachusetts, MASS. GEN. LAWS ch. 93H, § 3 (2010); North Carolina, N.C. GEN. STAT. § 75-65 (2010); South Carolina, S. 453, 117th Sess. (S.C. 2008); and Wisconsin, WIS. STAT. § 134.98 (2010).

39. CAL CIV. CODE § 1798.82(e) (West 2010); *see e.g.*, ALASKA STAT. § 45.48.090(7) (2010); ARIZ. REV. STAT. § 44-7501(L)(6) (2010); COLO. REV. STAT. § 6-1-716 (2010); FLA. STAT. § 817.5681(5); KAN. STAT. ANN. 50-7a01(g) (2010); LA. REV. STAT. ANN. § 51:3073(4) (2010); ME. REV. STAT. ANN. tit. 10, § 1347(6) (2010); N.H. REV. STAT. ANN. § 359-C:19(IV) (2010); N.J. STAT. ANN. § 56:8-161 (West 2010); OHIO REV. CODE ANN. § 1347.12(A)(6) (West 2010); R.I. GEN. LAWS § 11-49.2-5(c) (2010); TENN. CODE ANN. § 47-18-2107(a)(3) (2010); VT. STAT. ANN. tit. 9, § 2430(5) (2010); VA. CODE ANN. § 18.2-186.6(A) (2010); WASH. REV. CODE § 19.255.010(5) (2010); W. VA. CODE § 46A-2A-101(6) (2010); WIS. STAT. § 134.98(1)(b) (2010).

40. N.D. CENT. CODE § 51-30-01 (2010).

tures, biometric data, and fingerprints;[41] and Arkansas has expanded it to include medical information.[42] Oregon, on the other hand, has broadened the definition not by adding elements but by removing the requirement that the breached information include a name; notification is only required if the breached information is sufficient for identity theft.[43] Texas and Massachusetts have also broadened California's statute by leaving out the exception for encrypted data and requiring notification whenever information is stolen.[44] Despite variations by state, at a minimum, data breach laws cover businesses that lose information due to a security breach where that information, encrypted or not, may lead to identity theft.

### 2. *Breach Trigger*

Where a breach has occurred, states differ on whether the victim must be notified in all cases or only where there is a risk of actual harm.[45] California's trigger is acquisition-based,[46] meaning that the breach always requires notice to consumers regardless of whether there was harm or even risk of harm.[47] This trigger

41. N.C. GEN. STAT § 14-113.20(b) (2010).

42. ARK. CODE ANN. § 4-110-103(7)(D) (2010). California also expanded its data breach law, effective January 1, 2008, to include medical information. CAL. CIV. CODE § 1798.82(e)(4) (West 2010).

43. OR. REV. STAT. § 646A.602(11)(b) (2010).

44. *See* MASS. GEN. LAWS ch. 93H, § 1(a) (2010) (defining personal information as "a resident's first name and last name or first initial and last name in combination with any 1 or more of the following data elements that relate to such resident: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account . . . ."); TEX. BUS. & COM. CODE ANN. § 521.002(a)(1) (Vernon 2010) (defining personal identifying information as "information that alone or in conjunction with other information identifies an individual, including an individual's: (A) name, social security number, date of birth, or government-issued identification number; (B) mother's maiden name; (C) unique biometric data, including the individual's fingerprint, voice print, and retina or iris image; (D) unique electronic identification number, address, or routing code; and (E) telecommunication access device . . . .").

45. *See* State PIRG Summary of State Security Freeze and Security Breach Notification Laws [hereinafter State PIRG Summary], http://pirg.org/consumer/credit/statelaws.htm (last visited May 9, 2010).

46. CAL CIV. CODE § 1798.82(a) (West 2010). See Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913, 972–84 (2007) for a chart summary of triggers and other notification elements by state, indicating that 20 state statutes are acquisition based.

47. CAL. CIV. CODE § 1798.82(a) (West 2010).

makes California's data breach law one of the strictest state laws.[48] Although New York also has an acquisition-based statute, it goes one step further by specifically defining acquisition as the downloading, copying, or unauthorized usage of information, including opening fraudulent accounts and identity theft.[49] Other states, such as Arkansas, have a risk-based trigger where notification is presumptively required, but a company may forgo notification if a reasonable investigation determines that "there is no reasonable likelihood of harm to customers."[50] The Delaware statute has a twist on its risk-based trigger: instead of allowing entities to conduct voluntary investigations to rebut the need for notification, the statute imposes a mandatory duty to investigate when entities are aware of a breach.[51] Furthermore, among states that use risked-based triggers, the required levels of risk for data misuse vary, and the statutory texts are often vague.[52]

3. *Notification*

While state data breach statutes uniformly require notification when consumers' personal information has been compromised, the statutes differ concerning the notification process. Specifically, the statutes differ as to whether a third-party must be notified, whether notification is required when the breaching entity is an in-state business, what information must be disclosed in a consumer notification, and how many individuals must be affected to trigger the notification requirement. Twenty-two states require reporting of the security breach to a credit-reporting agency if a certain number of records are compromised.[53] Regarding different treatment for in-state versus out-of-

48. *See* Patti Waldmeir, *Federal Data Security Law Reaches Turning Point in Congress*, FT.COM, Apr. 12, 2006.

49. N.Y. GEN. BUS. LAW § 899-aa(1)(c) (McKinney 2010).

50. ARK. CODE ANN. § 4-110-105(d) (2010).

51. DEL. CODE ANN. tit. 6, § 12B-102(a) (2010). This distinction is important because a company that simply notifies consumers after a breach has still violated Delaware law if it has not conducted an investigation to determine the likelihood that the personal information has been or will be misused.

52. DOUG MARKIEWICZ, VIGILANTMINDS, STATE SECURITY BREACH LEGISLATION 9 (2006), http://www.contrib.andrew.cmu.edu/~dmarkiew/docs/breach_whitepaper_200602.pdf.

53. It must be reported to a credit agency if more than 1,000 residents will be notified in: Alaska, ALASKA STAT. § 45.48.040 (2010); Colorado, COLO. REV. STAT. § 6-1-716(d)

state businesses, Wyoming gives local businesses an advantage by lowering their threshold requirement for substitute notice.[54]

In contrast, New York has stricter requirements than most states regarding the content and process of notification. New York requires notifications to include the contact information of the person making the notification, the categories of personal information that the breach affected, and information that has or is reasonably believed to have been acquired.[55] When notification is required under New York law, the breaching entity must also inform state law enforcement agencies of the notice's timing, distribution, and content along with the approximate number of affected individuals.[56] If more than 5,000 New York residents are notified, New York law requires this information to be furnished to consumer reporting agencies as well.[57]

---

(2010); District of Columbia, D.C. CODE § 28-3852(c) (2010); Florida, FLA. STAT. § 817.5681(12) (2010); Georgia, GA. CODE ANN. § 10-1-910 (2010); Hawaii, HAW. REV. STAT. § 487N-2(f) (2010); Indiana, IND. CODE § 24-4.9-3-1(b) (2010); Kansas, KAN. STAT. ANN. § 50-7a02(f) (2010); Maine, ME. REV. STAT. ANN. tit. 10, § 1348 (2010); Michigan, MICH. COMP. LAWS § 445.72 (2010); Nevada, NEV. REV. STAT. § 603A.220(6) (2010); New Jersey, N.J. STAT. ANN. § 56:8-163(f) (West 2010) ; North Carolina, N.C. GEN. STAT. § 75-65(f) (2010); Ohio, OHIO REV. CODE ANN. § 1347.12(F) (West 2010); Pennsylvania, 73 PA. CONS. STAT. ANN. § 2305 (West 2010); South Carolina, S.C. CODE ANN. § 39-1-90 (2010); Tennessee, TENN. CODE ANN. § 47-18-2107(g) (2010); Texas, TEX. BUS. & COM. CODE § 521.053(h) (Vernon 2010); Vermont, VT. STAT. ANN. tit. 9, § 2435(c) (2010); Virginia, VA. CODE ANN. § 18.2-186.6(E) (2010); West Virginia, W. VA. CODE § 46A-2A-102(f) (2010); and Wisconsin, WIS. STAT. § 134.98(2) (2010). Minnesota requires a report to the credit agency if more than 500 residents must be notified, MINN. STAT. § 325E.61 (2010), and New York requires a report if more than 5000 residents must be notified. N.Y. GEN. BUS. LAW § 899-aa(8)(b) (McKinney 2010).

54. WYO. STAT. ANN. § 40-12-502(d)(iii) (2010) (stating that Wyoming businesses may provide substitute notice if more than 10,000 state residents must be notified of a security breach or if the cost of notice would exceed $10,000). Out-of-state businesses are permitted to use substitute notice only when more than 500,000 residents are affected or the cost of notice would exceed $250,000. *Id.* Both may use substitute notice if they have insufficient contact information. *Id.*

55. N.Y. GEN. BUS. LAW § 899-aa(7) (McKinney 2010).

*56*. § 899-aa(8)(a) (requiring notification to the State Attorney General, the consumer protection board, and the Office of Cyber Security and Critical Infrastructure Coordination).

57. § 899-aa(8)(b).

4. *Timeliness*

The timeliness of notification is vague in most states' data breach statutes,[58] which usually have a standard similar to California's requirement that there be no "unreasonable delay."[59] Some states, such as Florida and Ohio, have more definite standards that require notification within forty-five days.[60] New York specifies that state agencies must notify potential victims within 120 days.[61] Most states, however, have exceptions allowing delay of notification if law enforcement officials determine that it would impede a criminal investigation.[62]

5. *Remedies*

Noncompliance with state security breach law will generally result in a civil or criminal penalty, but remedies vary widely among states.[63] While many states allow personal recovery, Iowa provides that the Attorney General may litigate and receive damages on behalf of an injured person.[64] Some states also provide for injunctive relief.[65] Maryland does not specify remedies in its data breach statute; instead it indicates that breaches constitute a deceptive and unfair trade practice actionable by the State Attorney General.[66] This power is similarly given to State Attorneys General in Colorado and California by expressly allowing

58. However, in some states the State Attorney General's guidance has indicated when notifications must be issued. *See, e.g.*, Press Release, Vt. Dep't of Banking, Ins., Sec. & Health Care Admin., *supra* note 37 (mandating that Vermont consumers affected by a data breach be notified within ten days).

59. CAL. CIV. CODE § 1798.29(a) (West 2010).

60. *See* FLA. STAT. § 817.5681 (2010); OHIO REV. CODE ANN. § 1347.12 (West 2010).

61. *See* N.Y. STATE TECH. LAW § 208(8) (McKinney 2010).

62. MARKIEWICZ, *supra* note 52, at 7.

63. *Compare* CAL. CIV. CODE § 1798.82(c) (West 2010) (providing statutory civil damages for willful, intentional, or reckless violations), *with* FLA. STAT. § 817.5681(b) (2010) (providing for administrative fines).

64. IOWA CODE § 715C.2(8)(a) (2010).

65. *See* CAL. CIV. CODE § 1798.84(e) (West 2010); ME. REV. STAT. ANN. tit. 10, § 1349(2)(B) (2010); NEV. REV. STAT. § 603A.920 (2010).

66. MD. CODE ANN., COM. LAW § 14-3508 (West 2010). Penalties for violating Maryland's Unfair or Deceptive Trade Practice Laws may include a fine up to $1,000, injunction, actual damages, attorney's fees, and up to twelve months in jail. §§ 13-408 to -10; *see also* Deceptive Trade Practices laws: Information on the Law About Deceptive Trade Practices, http://law.jrank.org/pages/11799/Deceptive-Trade-Practices.html (last visited May 9, 2010) (providing a fifty-state survey of unfair and deceptive trade practice laws and available remedies).

simultaneous actions under the state unfair and deceptive practices statutes.[67] In contrast, Illinois and Pennsylvania specify that violating the data breach statute constitutes an unlawful practice under the Consumer Fraud and Deceptive Business Act, triggering penalties and remedies under those laws.[68]

Many states explicitly provide for direct payment of damages to consumers or penalties to the state. For example, Delaware's security breach statute allows consumers to collect treble damages for successful lawsuits.[69] In comparison, Hawaii provides up to $2,500 per violation in addition to the actual sum of damages that injured parties sustained from the breach.[70] Other state statutes do not provide damages for individual consumers but instead provide for penalties to the state.[71] The District of Columbia allows private actions for damages, and the Attorney General may recover up to $100 per violation, plus costs and reasonable attorneys' fees.[72]

Damages are practically difficult to prove because the monetary loss from receiving untimely notification must be shown. Additionally, courts have held that an increased risk of future injury from identity theft exposure is insufficient to support an injury claim or to establish damages.[73] Although proving damages is difficult, the ultimate purpose of the notification laws is not to punish the breaching entity, but rather to give consumers timely notice so they can take action to protect against future fraud.[74]

---

67. CAL. BUS. & PROF. CODE § 17204 (West 2010); COLO. REV. STAT. § 6-1-103 (2010).

68. 815 ILL. COMP. STAT. 530 § 20 (2010); 73 PA. STAT. ANN. § 2308 (West 2010).

69. DEL. CODE ANN. tit. 6, §§ 12B-104, 2533 (2010); *see* JOHN P. HUTCHINS, U.S. DATA BREACH NOTIFICATION LAW: STATE BY STATE 90–91 (2007).

70. HAW. REV. STAT. § 487N-3 (2010). Similarly, Arizona provides for civil penalties of up to $10,000 per breach. ARIZ. REV. STAT. ANN. § 44-7501(H) (2010). Idaho limits damages to not more than $25,000 per breach. IDAHO CODE ANN. § 28-51-107 (2010).

71. *See e.g.*, MONT. CODE ANN. § 30-14-1705 (2010) (making a violation of Montana's data breach law subject to MONT. CODE ANN. § 30-14-142, which provides for a civil fine of $10,000 among other penalties); OHIO REV. CODE ANN. § 1347.12 (West 2010) (providing for the State Attorney General to investigate and bring civil action against the violators of the Ohio data breach laws with any damages awarded being paid to the state).

72. D.C. CODE § 28-3853 (2010).

73. John B. Kennedy, *A Primer on Key Information Security Laws in the United States*, *in* Ninth Annual Institute on Privacy and Security Law, at 117, 201 (PLI, 2008).

74. *See* Schwartz & Janger, *supra* note 46, at 949. For an overview of current state freeze laws, *see* Kristan T. Cheng, *Identity Theft and the Case for a National Credit Report Freeze Law*, 12 N.C. BANKING INST. 239, 251–54 (2008) (providing an overview of current state freeze laws).

To further the goal of consumer protection, forty-seven states and the District of Columbia[75] have passed statutes to provide credit freezes.[76] By initiating a credit freeze, a consumer prevents lenders from seeing her credit report unless she specifically grants them access.[77] A credit freeze helps prevent identity thieves from taking out new lines of credit in the consumer's name, even when the thieves have her social security number and other personal information.[78] A freeze differs from a fraud alert, which only covers consumers for ninety days and requires lenders to take extra precautions before granting credit in that consumer's name.[79] State laws vary as to whether a freeze is available only for victims or can be prophylactic, and whether the freeze can be lifted for a specific party and how much that costs.[80]

Consumers can also address breached personal information by subscribing to a credit monitoring service, which will notify consumers if suspicious or unusual transactions appear on their consumer credit report.[81] Although no state law currently requires giving affected consumers a credit monitoring service, this practice has become widespread among breached businesses.[82]

---

75. *See* Consumers Union's Guide to Security Freeze Protection, http://www.consumersunion.org/campaigns/learn_more/003484indiv.html (last visited May 11, 2010). As of May 11, 2010, Alabama, Michigan, and Missouri do not have security freeze laws.

76. *See* State PIRG Summary, *supra* note 45.

77. Kimberly Lankford, *Fraud Alert vs. Credit Freeze*, KIPLINGER.COM., Mar. 6, 2008, http://www.kiplinger.com/columns/ask/archive/2008/q0306.htm.

78. *Id*.

79. *Id.* An extended fraud alert can last up to seven years and entitles the consumer to two free credit reports every twelve months and removal from marketing lists for prescreened credit offers for five years. Fed. Trade Comm'n, Defend: Recover from Identity Theft, http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/defend.html (last visited May 11, 2010).

80. *See* State PIRG Summary, *supra* note 45.

81. Consumers Union, Credit Reports, http://www.consumersunion.org/creditmatters/creditmattersfactsheets/001634.html (last visited May 11, 2010).

82. Philip Gordon, *What Does the Crazy Quilt of Security Breach Laws Mean for Employers as Massachusetts Becomes the 39th State to Enact One?*, WORKPLACE PRIVACY COUNS., Aug. 21, 2007, http://privacyblog.littler.com/2007/08/articles/data-security/what-does-the-crazy-quilt-of-security-breach-laws-mean-for-employers-as-massachusetts-becomes-the-39th-state-to-enact-one/ (stating that providing free access to a credit monitoring service is the most commonly offered assistance after breach-induced data loss).

### 6. *Enforcement*

State data breach notification laws vary concerning who has the power to enforce them. Twenty-four state statutes explicitly allow the State Attorney General to bring an action for violation of the state data breach law.[83] Arizona's data breach statute is unique in designating the State Attorney General the sole enforcer.[84] In most states, the Attorney General shares enforcement power. For example, the Kansas Attorney General may bring an action in law or in equity for violations of the data breach statute, but if the entity is an insurance company, the state insurance commissioner has exclusive enforcement authority.[85] Other states have completely different enforcement mechanisms. Florida relies on the State Department of Legal Affairs to enforce and collect fines[86] and affords consumers no private right of action.[87] Yet most states, like Tennessee, have provisions for both state and private rights of action.[88]

State Attorneys General may have a role even when the data breach statute does not explicitly mention them. For example, in California, the State Attorney General has enforcement authority over the data breach laws because they are part of the general consumer protection chapter.[89] Additionally, due to the high visibility of data breach cases where personal information is used,

---

83. ARIZ. REV. STAT. ANN. § 44-7501(H) (2010); ARK. CODE ANN. § 4-110-108 (2010); COLO. REV. STAT. § 6-1-716(4) (2010); CONN. GEN STAT. 36a-701(b)(g) (2010); DEL. CODE ANN. tit. 6, § 12B-104 (2010); D.C. CODE § 28-3853(b) (2010); IND. CODE § 24-4.9-4-2 (2010); IOWA CODE § 715C.2(8)(a) (2010); KAN. STAT. ANN. § 50-7a02(g) (2010); MASS. GEN. LAWS ch. 93H, § 6 (2010); MINN. STAT. § 325E.61 (2010); NEB. REV. STAT. § 87-806 (2010); NEV. REV. STAT. § 603A.920 (2010); N.Y. GEN. BUS. LAW § 899-aa(6)(a) (McKinney 2010); N.C. GEN. STAT. § 75-65 (2010); N.D. CENT. CODE § 51-30-07 (2010); OHIO REV. CODE ANN. § 1347.12(G) (West 2010); 73 PA. STAT. ANN. § 2308 (West 2010); TEX. BUS. & COM. CODE ANN. § 521.151(b) (Vernon 2010); UTAH CODE ANN. § 13-44-301(1) (2010); VT. STAT. ANN. tit. 9, § 2435(g) (2010); VA. CODE ANN. § 18.2-186.6(I) (2010); W. VA. CODE § 46A-2A-104(b) (2010); WYO. STAT. ANN. § 40-12-502(f) (2010).

84. ARIZ. REV. STAT. ANN. § 44-7501(H) (2010).

85. S.B. 196, 2006 Leg., §4(g)-(h) (Kan. 2006), *available at* http://www.kslegislature.org/bills/2006/196.pdf; *see also* VT. STAT. ANN. tit. 9, § 2435(g)(1) (2010) (indicating that the Vermont Attorney General has the sole authority to investigate and enforce the state data breach statute, except when the breaching entity is registered with the State Department of Banking, Insurance, Securities and Health Care Administration).

86. FLA. STAT. § 817.5681(11) (2010).

87. *Id.*

88. TENN. CODE ANN. §§ 47-18-2105, 47-18-2107(a) (2010).

89. CAL. BUS. & PROF. CODE § 17200 (West 2010).

many State Attorneys General have used their authority under state unfair or deceptive practice laws to investigate and prosecute entities that have failed to secure personal information, even though the notification law was not violated.[90]

New York was the first state to reach a settlement under its data breach law when Attorney General Cuomo exercised his power under the notification statute to settle with CS Stars LLC for a breaching 540,000 consumers' private information.[91] In CS Stars, the Attorney General accused the company of unreasonable delay for waiting more than seven weeks after the breach to notify consumers.[92] More recently, Connecticut Attorney General Blumenthal exercised his authority under that state's data breach law to investigate a subsidiary of Fidelity concerning an employee's security breach that affected 2.3 million consumers.[93] These two cases illustrate the broad powers that State Attorneys General have under various general consumer protection laws to bring actions against businesses for data breaches, even when state notification laws have not been violated. These broad powers have been extended across state lines, as State Attorneys General have joined together in multistate actions against businesses for wide-spread breaches arising from poor system security.[94]

In addition to state Attorneys General actions, many states allow for consumers to bring a private right of action.[95] However, consumer class action lawsuits have proven difficult to win due to the challenge of linking notification delay with actual damages.

---

90. Patricia Covington & Meghan Musselman, *Recent Developments Affecting Privacy in 2007*, 63 BUS. LAW. 639, 647 (2008).

91. John Herzfeld, *Data Breaches: First Settlement Reached Under State's Data Breach Law*, 6 PRIVACY & SECURITY L. REP. 701 (2007).

92. Press Release, Office of N.Y. Att'y Gen., Cuomo Obtains First Agreement for Violation of Security Breach Notification Law (Apr. 26, 2007), http://www.oag.state.ny.us/media_center/2007/apr/apr26a_07.html.

93. Press Release, Office of Conn. Att'y Gen., Attorney General's Statement on Fidelity Security Breach Involving 2.3 Million Consumers (July 3, 2007), http://www.ct.gov/ag/cwp/view.asp?A=2341&Q=385814.

94. *See, e.g.*, Press Release, Office of Mass. Att'y Gen., Massachusetts Attorney General Martha Coakley Leads Multi-State Investigation into TJX Security Practices (Feb. 7, 2007) (on file with author).

95. *See e.g.*, LA. REV. STAT. ANN. § 51:3075 (2010) ("A civil action may be instituted to recover actual damages resulting from the failure to disclose in a timely manner to a person that there has been a breach of the security system resulting in the disclosure of a person's personal information.").

One example is *Hendricks v. DSW Shoe Warehouse, Inc.*, where a class action lawsuit was brought against DSW for failing to prevent the theft of its customers' personal information, which it stored in its computer systems.[96] In that case, customers sought reimbursement of fees for the credit monitoring service they purchased to protect themselves from identity theft after learning about the security breach.[97] The *Hendricks* court dismissed the complaint, finding that the plaintiffs failed to allege cognizable damages.[98] In a similar class action lawsuit against DSW, *Richardson v. DSW, Inc.*, the court rejected all of the plaintiff's recovery theories except for an implied contract claim.[99] Despite the rather difficult challenges plaintiffs face in class actions against companies that fail to maintain their private information, there seems to be no reduction in consumer class action claims.[100]

Thus, even though data breach notification requirements vary by state, there is a common thread running through all of them: if an entity is breached and personal information is taken, the breached entity has a duty to notify those potentially affected. Notification is critical for providing consumers time to secure their data through fraud alerts, credit freezes, or simply by contacting their credit card companies. Furthermore, the paucity of recent enforcement action against businesses for failure to give notice seems to indicate that compliance with notification laws is not overly burdensome for businesses. The lack of enforcement action does not mean, however, that data breaches are solved through notification. Increasingly, both state Attorneys General and consumers are trying to target the underlying system security (or lack thereof) that led to the breach, rather than the violation of notification laws. The law needs to advance from mere notification to prevention of breaches; nonetheless, before discussing this idea, it will be useful to examine the relevant federal

96. 444 F. Supp. 2d 775, 776–77 (W.D. Mich. 2006).
97. *Id.*
98. *Id.* at 781.
99. No. 05 C 4599, 2005 WL 2978755, at *5 (N.D. Ill. Nov. 3, 2005).
100. *E.g.*, *Hannaford Bros. Face Class Action over Data Breach*, CONSUMERAFFAIRS.COM, Mar. 21, 2008, http://www.consumeraffairs.com/news04/2008/03/hannaford_data2.html; Robert McMillan, *Sears Sued over Privacy Breach,* INFOWORLD, Jan. 8, 2008, http://www.infoworld.com/article/08/01/08/Sears-sued-over-privacy-breach_1.html (discussing a class action lawsuit that was filed against Sears after it published consumer purchase histories on its Web site, Managemyhome.com).

laws, and the interplay between federal and state enforcement of data breach laws through two recent situations.

## III. FEDERAL DATA BREACH LAWS

Although there are statutes that impose criminal penalties on individuals who intentionally hack into network systems, the following sections focus on federal statutes that impose obligations on entities to secure data and networks and to disclose information to affected individuals following data breaches. Several federal statutes and regulations govern corporate computer security. Many focus on narrow issues. For example, the Fair Credit Reporting Act addresses the use of credit reports;[101] the Health Insurance Portability and Accountability Act governs the disclosure of medical information;[102] and the Privacy Act of 1974 controls individuals' information that federal government agencies hold and how that information may be disclosed.[103] As these statutes evidence, wide gaps exist where information is unprotected, and there is no single overriding consumer-targeted law that protects information that both companies and the government store from abuse.[104] This Section will discuss two main security breach notification laws: the notification law aimed at the financial services industry and the unfair or deceptive trade practice law that is used to prosecute substandard security measures when personal information is lost in a security breach.

---

101. *See* 15 U.S.C. § 1681 (2006).

102. *See* 45 C.F.R. § 164.502 (2010).

103. *See* 5 U.S.C. § 552a (2006); *see also* 18 U.S.C. § 1029, 1343 (2006); Computer Fraud and Abuse Act § 2, 18 U.S.C. § 1030 (2006).

104. In contrast, the European Union codified its response to personal data in 1995 in the European Union's Council Directive on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data. Council Directive 95/46, 1995 O.J. (L 281) 31-50 (EC). The Member States have, however, a relatively unharmonious implementation in their national data protection laws. *See* Benjamin J. Keele, Note, *Privacy by Deletion: The Need for a Global Data Deletion Principle*, 16 IND. J. GLOBAL LEGAL STUD. 363, 365 (2009). More recently, "[t]wo European data protection bodies (the Working Party 29 advisory body and the European Data Protection Supervisor (EDPS) supervisory authority) have now published their opinions regarding the proposed reform of the data breach notifications." Patrick Van Eecke & Maarten Truyens, *Recent Events in EU Internet Law*, 12 No. 2 J. INTERNET L. 25, 26 (Aug. 2008).

### A. GRAMM-LEACH-BLILEY ACT

Despite the absence of a universal consumer-targeted law, there is one federal statute that contains a security breach notification component. In 1999, Congress passed the Gramm-Leach-Bliley Act ("GLBA"), which targets the financial services industry.[105] The GLBA's main focus is not on regulating security breaches; rather, it was designed primarily to repeal regulations that prevented mergers of banking, insurance, and securities companies.[106] To accomplish its goal, the GLBA also imposes requirements on using specific information by regulating the type of nonpublic personal information financial institutions collect, with whom they share the information, and how they must protect that information.[107]

Although the GLBA is focused on financial institutions,[108] its enforcement was left to the various agencies that regulated these various institutions.[109] Thus, it was not until 2005, six years after the California data breach statute took effect, that the GLBA was used as a notification law under the "Interagency Guidances."[110] One guidance requires financial institutions to maintain reason-

105. *See* Pub. L. No. 106-102, 113 Stat. 1338 (codified as amended in scattered sections of 12 U.S.C. and 15 U.S.C).

106. U.S. Senate Committee on Banking, Housing, & Urban Affairs, Financial Services Modernization Act: Gramm-Leach-Bliley Summary of Provisions, http://banking.senate.gov/conf/grmleach.htm (last visited May 11, 2010).

107. Federal Trade Commission, In Brief: The Financial Privacy Requirements of the Gramm-Leach-Bliley Act, http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus53.pdf (last visited May 11, 2010).

108. Financial institutions are defined quite broadly as any businesses engaged in financial activities. 12 U.S.C. § 1843(k) (2006). This includes banks, brokers, dealers, insurance companies, credit unions, non-depository lenders, consumer reporting agencies, debt collectors, data processors, courier services, retailers that issue credit cards, personal property or real estate appraisers, check-cashing businesses, and mortgage brokers. *See* 16 C.F.R. § 313.3 (2009).

109. 15 U.S.C. § 6801(b) (2006).

110. The GLBA was apparently the only means congressional legislators had to deal with the problem of security breaches and identity theft. This is evidenced by the fact that the proposed Guidances were announced August 12, 2003 just after the FTC published a report in September of that year estimating that almost 10 million Americans were victims of identity theft. *See* Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 68 Fed. Reg. 47,954 (proposed Aug. 12, 2003); FED. TRADE COMM'N, IDENTITY THEFT SURVEY REPORT 4–9 (2003), http://www.ftc.gov/os/2003/09/synovatereport.pdf.

able data security,[111] and the other guidance requires financial institutions to develop a formal response program to deal with data security breaches.[112]

The GLBA is noteworthy because, through the Interagency Guidances, the federal government established a process-oriented approach to security regulation for the financial industry.[113] The guidelines increase consumers' security by placing an affirmative duty on financial institutions to protect customer data and notify customers of unauthorized access or use of their private information.[114] The GLBA has many similarities to the California data breach notification statute discussed earlier.[115]

In terms of notification, the institutions have a duty to investigate security breaches and determine whether there is a reasonable possibility that an individual's personal information will be misused; if there is, the institution must notify the individual "as soon as possible."[116] This trigger of reasonable possibility of misuse is rather high compared to most states, which presumptively require notification when private data has been breached or when personal information might be misused.[117] Despite this relatively high notification trigger, the close relationship between federal functional regulators and regulated industries is something states do not have. This close relationship has allowed reg-

111. Proper Disposal of Consumer Information Under the Fair and Accurate Credit Transactions Act of 2003, 69 Fed. Reg. 77,610 (Dec. 28, 2004) (to be codified at 12 C.F.R. pts. 30, 41, 208, 211, 222, 225, 334, 364); *see also* § 6805(b).

112. Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 Fed. Reg. 15,736, 15,743 (Mar. 29, 2005) (to be codified at 12 C.F.R. pts. 30, 208, 225, 364, 568, 570).

113. *See* §§ 6801–09; Interagency Guidelines Establishing Information Security Standards, 12 C.F.R. pt. 208 app. D-2 (2009) (Federal Reserve Board); 12 C.F.R. pt. 30 app. B (Comptroller of the Currency, Treasury); 12 C.F.R. pt. 364 app. B (2006) (Federal Deposit Insurance Corporation); and 12 C.F.R. pt. 570 app. B (Office of Thrift Supervision, Treasury).

114. Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 Fed. Reg. at 15,752.

115. *See supra* Part II.A. For example, there is a similar definition of personal information being an individual's name, address, or telephone number, in conjunction with the customer's driver license number, social security number, account number, credit or debit card number, or data that would permit access to a customer's account that is otherwise protected.

116. *Id*. Just as in many state statutes, notification may be delayed where a law enforcement agency determines disclosure would interfere with a criminal investigation. *Id.*

117. Schwartz & Janger, *supra* note 46, at 916–17; *see also supra* Part II.B.2.

ulators to review notification decisions and has made the Interagency Guidances effective.[118]

When notice is required, it must be in a medium that a customer would expect to receive, such as by telephone, mail, or email.[119] Furthermore, the notification must be clear and unambiguous, describing the institution's unauthorized access and remedial protective measures, and it must provide a telephone number that customers can call for assistance.[120]

In addition to the statutory text, the Federal Trade Commission ("FTC") has promulgated a safeguard rule under the GLBA that affects both financial[121] and non-financial organizations that handle customer information. This rule covers "any other financial institution or other person that is not subject to the jurisdiction of any agency or authority."[122] It affects not only institutions that collect nonpublic personal information from their own customers, but also those institutions that receive customer information from other financial institutions.[123] The general standard for compliance with the FTC safeguard rule requires the institutions to implement security programs to protect customer information.[124] The safeguard rule, although flexible to accommodate each corporation's particular circumstances, requires certain administrative safeguards such as regular testing of key controls, systems, and procedures as well as designation of a security coordinator to ensure accountability.[125]

---

118. *See* Schwartz & Janger, *supra* note 46, at 940.

119. Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 Fed. Reg. at 15,753. Email notification is allowed when the institution possesses a customer's valid email address and the customer has consented to receiving electronic communication. *Id*.

120. *Id.* at 15,752–53.

121. "Financial institutions under the FTC's jurisdiction include state-chartered credit unions and certain other entities that hold consumer transaction accounts." Federal Trade Commission, New 'Red Flag' Requirements for Financial Institutions and Creditors Will Help Fight Identity Theft, http://www.ftc.gov/bcp/edu/pubs/business/alerts/alt050.pdf (last visited May 10, 2010).

122. 15 U.S.C. § 6805(a)(7) (2006).

123. 16 C.F.R. § 314.1(b) (2009).

124. § 314.3(a) (requiring institutions to "develop, implement, and maintain a comprehensive information security program that is written . . . and contains administrative, technical, and physical safeguards that are appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue.").

125. § 314.4.

Because the safeguard rule was promulgated under the GLBA, however, its scope is limited to regulating data breaches between consumers and businesses in the financial sector (including those that receive private information from financial institutions).[126] Furthermore, the FTC safeguard rule covers only "nonpublic personal information" that comprises "personally identifiable financial information."[127] It does not cover other types of non-financial businesses or government entities, nor does it cover other types of personal, but non-financial information. Even when the GLBA notification system and FTC safeguard rule are successfully implemented, consumers who have suffered direct loss from a data breach still have no remedy under the statute.

## B. FEDERAL TRADE COMMISSION ACT

In contrast, when data breaches occur between retail businesses and consumers, the FTC must rely upon Section 5 of the Federal Trade Commission Act ("FTCA"), which prohibits "unfair and deceptive acts or practices."[128] Under the statute's general enforcement authority, the FTC can investigate and pursue actions against a business whose activity qualifies as a practice that "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[129] Despite the fact that the provision's language suggests that the FTC may act to *prevent* data breaches, the agency generally exercises its enforcement power under the statute only after a data breach has occurred.[130]

In 1999, the FTC began utilizing this enforcement power against companies that violated their own privacy policies that governed their treatment of consumer data within their possession.[131] The FTC advanced one step further in 2002 by alleging

126. *See* 15 U.S.C. § 6809(4).
127. *Id.*
128. § 45(a)(4)(B).
129. § 45(n).
130. *See Data Breaches and Identity Theft: Hearing Before the S. Comm. on Commerce, Sci., and Transp.*, 109th Cong. 6 (2005) (statement of Deborah Platt Majoras, Chairman, Federal Trade Commission), *available at* http://commerce.senate.gov/pdf/ftc.pdf.
131. *See* Complaint, *In re* Geocities, 127 F.T.C. 94 (1999) (No. C-3850).

that companies violated their own privacy policies because of their statements regarding the safety of consumer information.[132] This reasoning opened the door for investigation into businesses for failure to implement appropriate security measures.[133] Since 2002, the FTC has used this power nineteen times.[134] Through

---

132. *See* Complaint at 4, *In re* Petco Animal Supplies, Inc., 139 F.T.C. 102 (2005) (No. C-4133) (stating the violation of a privacy policy was alleged to be "unfair or deceptive acts or practices," but it was unspecified whether the practice was unfair or deceptive).

133. *Id*.

134. As of January 5, 2010, the breaches are:

(1) Eli Lilly & Co., *see* Press Release, Fed. Trade Comm'n, Eli Lilly Settles FTC Charges Concerning Security Breach (Jan. 18, 2002) [hereinafter Eli Lilly Press Release], http://www.ftc.gov/opa/2002/01/elililly.htm, alleging unfair or deceptive acts or practices generally without specifying whether they were unfair or deceptive;

(2) Microsoft Corp., *see* Press Release, Fed. Trade Comm'n, Microsoft Settles FTC Charges Alleging False Security and Privacy Promises (Aug. 8, 2002), http://www.ftc.gov/opa/2002/08/Microsoft.htm, alleging unfair or deceptive acts or practices generally without specifying whether they were unfair or deceptive;

(3) Guess, Inc., *see* Press Release, Fed. Trade Comm'n, Guess Settles FTC Security Charges; Third FTC Case Targets False Claims about Information Security (June 18, 2003), http://www.ftc.gov/opa/2003/06/guess.htm, alleging unfair or deceptive acts or practices generally without specifying whether they were unfair or deceptive;

(4) Tower Records, s*ee* Press Release, Fed. Trade Comm'n, Tower Records Settles FTC Charges (Apr. 21, 2004), http://www.ftc.gov/opa/2004/04/towerrecords.shtm, alleging unfair or deceptive acts or practices generally without specifying whether they were unfair or deceptive;

(5) Petco, s*ee* Press Release, Fed. Trade Comm'n, Petco Settles FTC Charges (Nov. 17, 2004), http://www.ftc.gov/opa/2004/11/petco.htm, alleging unfair or deceptive acts or practices generally without specifying whether they were unfair or deceptive;

(6) Vision I Properties, LLC, s*ee* Press Release, Fed. Trade Comm'n, Internet Service Provider Settles FTC Privacy Charges (Mar. 10, 2005), http://www.ftc.gov/opa/2005/03/cartmanager.shtm, alleging unfair acts or practices;

(7) Superior Mortgage Corp., *see* Press Release, Fed. Trade Comm'n, Mortgage Company Settles Information Security Charges (Sept. 28, 2005), http://www.ftc.gov/opa/2005/09/superior.htm, alleging unfair or deceptive acts or practices and the FTC Safeguard Rule under the GLBA;

(8) BJ's Wholesale Club, *see* Press Release, Fed. Trade Comm'n, BJ's Wholesale Club Settles FTC Charges (June 16, 2005), http://www.ftc.gov/opa/2005/06/bjswholesale.htm, alleging unfair acts or practices;

(9) DSW Shoe Warehouse, *see* Press Release, Fed. Trade Comm'n, DSW Inc. Settles FTC Charges (Dec. 1, 2005), http://www.ftc.gov/opa/2005/12/dsw.htm, alleging unfair acts or practices;

(10) ChoicePoint, *see* Press Release, Fed. Trade Comm'n, ChoicePoint Settles Data Security Breach Charges (Jan. 26, 2006) [hereinafter ChoicePoint Press Release], http://www.ftc.gov/opa/2006/01/choicepoint.htm, alleging unfair or deceptive acts or practices and an FRCA violation;

(11) CardSystems, *see* Agreement Containing Consent Order, *In re* CardSystems Solutions, Inc., 2005 F.T.C. Lexis 176 (Oct. 28, 2005) (No. 052 3148), alleging unfair acts or practices;

these actions, the FTC has set a normative baseline for security with which all companies subject to FTC jurisdiction must comply or else face an unfair and deceptive trade practice claim. Failure to implement reasonable security measures may violate a business's privacy statement and therefore be a deceptive trade practice.[135] An example of this is the FTC action against Petco, where the company's Web site promised that personal information was safe and "strictly shielded from unauthorized access."[136] The FTC complaint alleged that Petco failed to implement reasonable procedures to detect foreseeable application vulnerabilities and to prevent unauthorized access to sensitive consumer information, thereby constituting an unfair or deceptive trade practice.[137]

Despite initial success in prosecuting companies under the "deceptive practices" prong, many companies have stopped making any safety or privacy claims, thereby avoiding vulnerability to the charge of deceptive conduct.[138] Although the FTC could theo-

---

(12) Guidance Software, Inc., *see* Press Release, Fed. Trade Comm'n, Guidance Software Inc. Settles FTC Charges (Nov. 16, 2006), http://www.ftc.gov/opa/2006/11/guidance.shtm, alleging deceptive acts or practices;
(13) Life is Good, Inc., *see* Press Release, Fed. Trade Comm'n, Online Apparel Retailer Settles FTC Charges that It Failed to Safeguard Consumers' Sensitive Information, in Violation of Federal Law (Jan. 17, 2008), http://www.ftc.gov/opa/2008/01/lig.shtm, alleging deceptive acts or practices;
(14) Goal Financial, *see* Press Release, Fed. Trade Comm'n, Student Lender Settles FTC Charges that It Failed to Safeguard Sensitive Consumer Information and Misrepresented Its Security Practices (Mar. 4, 2008), http://www.ftc.gov/opa/2008/03/studlend.shtm, alleging unfair or deceptive acts or practices and a violation of the GLBA;
(15) REI and Seisint, Inc. *see* Press Release, Fed. Trade Comm'n, Agency Announces Settlement of Separate Actions Against Retailer TJX, and Data Brokers Reed Elsevier and Seisint for Failing to Provide Adequate Security for Consumers' Data (Mar. 27, 2008), http://www.ftc.gov/opa/2008/03/datasec.shtm, alleging unfair acts or practices;
(16) TJX Companies, Inc., s*ee id.*, alleging unfair acts or practices;
(17) Gregory Navone, s*ee* Press Release, Fed. Trade Comm'n, FTC Says Mortgage Broker Broke Data Security Laws: Dumpster Wrong Place for Consumers' Personal Information (Jan. 21, 2009), http://www.ftc.gov/opa/2009/01/navone.shtm, alleging deceptive acts or practices;
(18) Genica Corp., s*ee* Complaint, *In re* Genica Corp., 2009 F.T.C. Lexis 65 (Mar. 16, 2009) (No. C-4252), alleging deceptive acts or practices;
(19) CVS Caremark Corp., *see* Complaint, *In re* CVS Caremark Corp., 2009 F.T.C. Lexis 136 (June 18, 2009) (No. C-4259), alleging an unfair act or practice.

135. Complaint, *In re* Life is Good, Inc., 2008 F.T.C. Lexis 45 (Apr. 16, 2008) (No. C-4218); *see also* Complaint, *supra* note 132 (alleging a business has violated its privacy policy by failing to implement reasonable security measures).

136. Complaint, *supra* note 132, at 2.

137. *Id.* at 4.

138. *See supra* note 134 (although a new trend may be appearing with FTC actions against Genica Corp. and Gregory Navone).

retically argue that the companies made implied representations of safety or privacy, the FTC has generally prosecuted companies under the "unfair acts or practices" prong instead.[139] Thus, even though the privacy policy has not been violated, poor information security practices may be determined to be unfair trade practices. In three actions involving security breaches, the FTC has alleged that a business should be liable for failing to employ appropriate security measures regardless of whether the company ever had a customer privacy policy in place.[140]

In these instances, the breached company's business model influences the FTC's response and penalty. There is a difference between retail and data broker companies. The majority of the nineteen breaches since 2002[141] have involved retail companies that have gained customers' personal information through retail business transactions and failed to secure that data.[142] In such cases, the FTC relies on its "unfairness" or "deceptive acts" jurisdiction under Section 5 of the FTCA, which gives the government no right to collect monetary penalties.[143] Practically, however, settlements still "cost" the company in reputation, time, and money, especially if it needs to pay for and allow outside third-party auditors and the FTC to verify its security program.[144] In contrast, companies that sell personal information, data brokers,[145] are held to a higher duty to protect that information. In cases dealing with these types of companies, the FTC may use the Fair Credit Reporting Act ("FRCA")[146] to impose penalties in addition to monitoring solutions, thereby forcing these companies to

139. *Id.*

140. Complaint, *In re* DSW Inc., No. C-4157 (F.T.C. Mar. 7, 2006), *available at* http://www.ftc.gov/os/caselist/0523096/0523096c4157DSWComplaint.pdf; Complaint, *In re* BJ's Wholesale Club, Inc., 140 F.T.C. 465 (2005) (No. C-4148); Complaint, *In re* Cardsystems, Inc., 2005 F.T.C. Lexis 176 (Oct. 28, 2005) (No. 0523148) (attached as appendix to agreement containing consent order).

141. *See supra* note 134.

142. *See* Eli Lilly Press Release, *supra* note 134.

143. *See* 15 U.S.C. § 45 (2006).

144. *See* Christopher S. Rugaber, Guidance Software Settles FTC Charges, MSNBC, Nov. 17, 2006, http://www.msnbc.msn.com/id/15757047/ (discussing Guidance Software, Inc.'s settlement with the FTC, which called for a comprehensive information-security program with third-party auditing every other year for ten years).

145. *See infra* Part IV.A.

146. 15 U.S.C. §§ 1681–81w (2006). This statute regulates collecting, disseminating, and using consumer credit information. *Id.*

pay more than retail companies for data breaches.[147] These nineteen cases have distilled certain factors indicating an FTC trend toward considering failure to provide reasonable and appropriate security for personal information a violation of Section 5 of the FTCA, which prohibits unfair and deceptive acts or practices. These factors include: (1) inadequately assessing system vulnerability to commonly known or reasonably foreseeable attacks; (2) failing to apply low-cost, simple, and readily available defenses; (3) using default user ID or passwords to protect sensitive data rather than stronger passwords to prevent hackers; (4) storing information in unencrypted files and sending sensitive data via unencrypted transmission routes; and (5) failing to develop unauthorized access detection mechanisms.[148]

While the FTC has not made these factors an explicit policy, the agency has become more focused on preventing data breaches as opposed to mere consumer notification after a breach has taken place. The fact that the FTC is expanding Section 5 of the FTCA to include aspects of data security indicates the need for new legislation that progresses from notification to prevention of data breaches.

## IV. FEDERAL AND STATE ENFORCEMENT IN DATA BREACH SITUATIONS

To analyze the interplay between federal and state enforcement actions subsequent to a data breach where consumers' personal information is compromised, it is helpful to scrutinize two recent breach situations: ChoicePoint and TJX. ChoicePoint is significant because the breach involved a data broker, and it was the catalyst for many states to follow California by enacting data breach notification laws. TJX is significant because it has been characterized as the largest retail security breach in history.[149] For each of the incidents, this Note will address the actions taken by the FTC, State Attorneys General, and consumers. Addition-

147. ChoicePoint Press Release, *supra* note 134 (discussing the loss of 163,000 personal records, the $10 million in civil penalties, and $5 million in consumer redress).

148. Joel B. Hanson, Note, *Liability for Consumer Information Security Breaches: Deconstructing FTC Complaints and Settlements*, 4 SHIDLER J. L. COM. & TECH. 11 (2008).

149. Joseph Pereira, *Breaking the Code: How Credit-Card Data Went Out Wireless Door*, WALL ST. J., May 4, 2007, at A1.

ally, this Section will discuss the advantages of state versus federal enforcement of security breach laws, in relation to the incidents.

## A. CHOICEPOINT

ChoicePoint was in the business of gathering and selling personal data, and was regarded as the world's largest data broker with 119 billion records in its database.[150] ChoicePoint sold the personal information of consumers, including names, social security numbers, birth dates, employment information, and credit histories to over 50,000 businesses.[151] In 2004, ChoicePoint announced that fifty of its business clients were not who they claimed to be but were instead fraudulent entities set up entirely to collect data.[152] Additionally, experts determined that the data those fraudulent entities received had been used in identity theft.[153] This case has been likened to a "modern version of the classic dumpster diving schemes," where thieves would open up new lines of credit from personal information found in the garbage.[154] Approximately 5,000 cases of identity theft occurred, and the breach exposed the information of over 163,000 consumers.[155] Initially, the company notified the 35,000 California residents that were affected, as California was the only state at the time that required notification of customers after a security breach.[156] The Interagency Guidances discussed above were also not yet in

150. Tom Zeller, Jr., *Breach Points Up Flaws in Privacy Laws*, N.Y. TIMES, Feb. 24, 2005, at C1; *see also* Sarah D. Scalet, *ChoicePoint Data Breach: The Plot Thickens*, CSO, May 1, 2005, http://www.csoonline.com/article/220341/ChoicePoint_Data_Breach_The_Plot_Thickens (listing a timeline of key events surrounding the ChoicePoint data breach).

151. ChoicePoint Press Release, *supra* note 134.

152. David Bender, *Privacy Developments — 2005*, *in* Eleventh Annual Institute on Intellectual Property Law, at 11, 15 n. 15 (PLI Patents, Copyrights, Trademarks, and Literary Prop., Course Handbook Series No. 6036, 2005).

153. *Id.*

154. Flora J. Garcia, *Data Protection, Breach Notification, and the Interplay Between State and Federal Law: The Experiments Need More Time*, 17 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 693, 718 (2007).

155. Joshua Pantesco, *FTC Imposes Record Fine on ChoicePoint in Data-Loss Case*, JURIST, Jan. 26, 2006, http://jurist.law.pitt.edu/paperchase/2006/01/ftc-imposes-record-fine-on-choicepoint.php.

156. Verne Kopytoff, *35,000 in State to Receive Warning*, S. F. CHRON., Feb. 19, 2005, at A3; *see also* Thomas Claburn, *Law Prompts Company to Disclose Data Breach*, INFORMATIONWEEK, Feb. 21, 2005, http://www.informationweek.com/news/security/privacy/showArticle.jhtml?articleID=60402273.

place. Nevertheless, because of the strong public outcry and pressure from State Attorneys General combined with both FTC and SEC investigations, ChoicePoint agreed to notify the other 128,000 affected individuals.[157] Eventually, this incident became one of the main catalysts for many states to enact their notification laws.[158]

The FTC complaint alleged that ChoicePoint had failed to utilize readily available business verification products, examine applications, conduct site visits, and utilize other reasonable methods to detect discrepancies in applications.[159] Additionally, the complaint cited a lack of common sense, such as providing information to customers who did not even submit their last name and continuing to sell them information after both law enforcement authorities and ChoicePoint employees had identified the customers as suspicious.[160] The FTC utilized its authority under the FRCA and Section 5 of the FTCA to support its claims.[161] Ultimately, the FTC fined ChoicePoint $10 million in civil penalties and $5 million to compensate the victims; it also required Choice Point to better secure personal information with third-party professional security auditing until 2026.[162]

State Attorneys General from forty-three states also targeted ChoicePoint primarily under the various states' consumer protection and unfair or deceptive trade practices laws.[163] Although ChoicePoint agreed to pay the states $500,000, the settlement with the Attorneys General was not focused on monetary damages since ChoicePoint had already settled with the FTC and agreed to reimburse victims of identity theft.[164] Instead, the set-

157. *Id.*

158. Satish M. Kini & James T. Shreve, *Notice Requirements: Common Themes and Differences in the Regulatory and Legislative Responses to Data Security Breaches*, 10 N.C. BANKING INST. 87, 88 (2006).

159. Complaint, United States v. ChoicePoint Inc., No. 106-CV-0198 (N.D. Ga. Jan. 30, 2006), *available at* http://www.ftc.gov/os/caselist/choicepoint/0523069complaint.pdf.

160. *Id.*

161. *Id.*

162. ChoicePoint Press release, *supra* note 134.

163. Assurance of Voluntary Compliance & Discontinuance, *In re* Tex. & ChoicePoint, Inc., No. D-1-GV-07-001080 (Dist. Ct. Tex. County May 31, 2007), *available at* http://www.oag.state.tx.us/newspubs/releases/2007/053107choicepoint_avc.pdf.

164. *See* Press Release, Office of Conn. Att'y Gen., Attorney General Announces Nationwide Settlement with ChoicePoint for Security Breach (May 21, 2007), http://www.ct.gov/ag/cwp/view.asp?A=2341&Q=382400 (announcing the ChoicePoint multi-state settlement).

tlement obligated ChoicePoint to provide the highest level of security to safeguard its data.[165] Finally, in addition to the FTC and State Attorneys Generals, ChoicePoint paid out $10 million in 2008 to settle a class-action lawsuit based on the 2004 breach.[166]

This incident brought the mysterious world of data brokers and information selling into the public's awareness, and prompted new scrutiny and greater oversight of the data sales trade by spurring state security breach notification laws.[167] The fines and settlements were a record high for data breach settlements,[168] perhaps because the roles of data broker and information seller require a higher duty to protect private information from misuse. Additionally, the high fines may have resulted from the availability of the FRCA, which specifically allows such penalties as an enforcement mechanism.[169] In addition to the fines and the settlement money, ChoicePoint spent $2 million on notifications and $9.4 million for legal and other professional fees in 2005.[170] It was also estimated that compliance with the settlement by changing business practices to secure personal information would cost ChoicePoint between $15 million and $20 million in sales and reduce earnings per share by ten to twelve cents.[171]

## B. TJX COMPANIES, INC.

The TJX Companies, Inc., which includes T.J. Maxx and Marshalls, is the largest off-price department store chain in the

165. *Id.*

166. Martin H. Bosworth, *ChoicePoint Settles Data Breach Lawsuit*, CONSUMERAFFAIRS.COM, Jan. 27, 2008, http://www.consumeraffairs.com/news04/2008/01/choicepoint_settle.html.

167. *Id.*

168. Consumer Protection Bulletin, Record-High ChoicePoint Settlement Emphasizes Need to Reassess Corporate Data-Security Programs, http://www.bryancave.com/files/Publication/039c9df4-c52a-4bc9-84b8-2598006383da/Presentation/PublicationAttachment/00b09644-f5b7-4ebb-8aff-28676b782515/ConsumerProtectionBulletin1-28-06.pdf (last visited May 11, 2010).

169. *But see* Marcy E. Peek, *Information Privacy and Corporate Power: Towards a Re-Imagination of Information Privacy Law*, 37 SETON HALL L. REV. 127, 157 (2006) (stating that fines are merely the cost of business for ChoicePoint, which then had an annual revenue of $1.1 billion).

170. Joris Evers, *Break-in Costs ChoicePoint Millions*, ZDNET, July 21, 2005, http://news.zdnet.com/2100-1009_22-143833.html.

171. *Id.*

U.S.[172] The TJX breach occurred because TJX retained magnetic strip data from customers' credit cards in unencrypted form for too long.[173] TJX announced the breach on January 17, 2007.[174] The breach began in July 2005 when thieves took stored data from 36,200,000 credit cards, of which 11,200,000 were still valid at the time of the theft.[175] Later, in its own investigation, Visa found that 94,000,000 cards were stolen.[176] The thieves stole the data from every transaction conducted between December 31, 2002 and September 2, 2003 where TJX had stored "all card data," the data scanned from the magnetic strip on payment cards without encryption.[177] In addition to the credit card information, other personal information was stolen, such as drivers' license, and military and state identification numbers along with related names and addresses.[178]

Moreover, the stolen data was apparently utilized before TJX learned of the breach. The police in Florida arrested part of a ring of people who had committed fraud using data previously stolen from TJX.[179] Members of the ring bought $8 million worth of merchandise at various Wal-Mart stores in Florida.[180] Fraudulent transactions occurring in Georgia, Louisiana, Sweden, and Hong Kong have also been linked to the TJX breach.[181]

---

172. *See* TJX Investor Information, http://www.tjx.com/investor_landing.asp (last visited May 11, 2010).

173. Larry Greenemeier, *TJX Stored Customer Data, Violated Visa Payment Rules*, INFORMATIONWEEK, Jan. 29, 2007, http://www.informationweek.com/story/showArticle.jhtml?articleID=197001447 (criticizing the length of time TJX stored its customer data and detailing how information can be intercepted).

174. TJX COS., 2006 ANNUAL REPORT (Form 10-K), at 7 (2007) (Mar. 28, 2007), *available at* http://thomson.mobular.net/thomson/7/2394/2625/print/print.pdf.

175. *Id.* at 9.

176. Gerson Lehrman Group, TJX Proposes $40.9 Million Settlement with Visa Inc. in the Largest Data Breach of 94 Million Cardholders, http://www.glgroup.com/News/TJX-Proposes-$40.9-Million-Settlement-With-Visa-Inc.-In-the-Largest-Data-Breach-of-94-Million-Cardholders-19656.html (last visited May 11, 2010).

177. TJX COS., *supra* note 174, at 9 (indicating that "track 2 data" was no longer stored in the TJX system after September 2, 2003).

178. TJX COS., *supra* note 174, at 8.

179. Jaclyn Giovis, *6 Held in Credit ID Theft Case; Authorities Link S. Florida Suspects to TJX Cos. Breach*, S. FLA. SUN-SENTINEL, Mar. 24, 2007, at 1D.

180. *Id.*

181. Tom Spoth, *Banks Caught in the Middle; Thousands of Debt, Credit Cards Must Be Replaced in Wake of TJX Cos. Security Breach*, LOWELL SUN, Jan. 28, 2007; *see also* Mark Jewell, *Suspect of Massive ID Theft Held in Turkey*, MSNBC, Aug. 21, 2007, http://www.msnbc.msn.com/id/20379162/ (describing a Ukrainian man who was arrested in Turkey with possible connections to the TJX breach).

The FTC charged that TJX "engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for personal information on its networks."[182] Specifically, the agency charged TJX with creating unnecessary risk to personal information by storing it and transmitting it in clear text (that is, without encryption), failing to use readily available security measures to limit access to wireless networks and card authorization computers, not requiring system administrators to use strong passwords, and employing insufficient measures to detect and prevent unauthorized access such as updating antivirus software and following up on security intrusion alerts.[183] The FTC brought this action using its authority under Section 5 of the Federal Trade Commission Act, claiming that the acts and practices of TJX constituted "unfair acts or practices in or affecting commerce."[184]

The settlement between TJX and the FTC had two main components: a change in practice and an outside auditing requirement.[185] With respect to practice, the FTC required TJX to designate employees who would be accountable for the information security program, perform a risk assessment, and design and implement reasonable safeguards to control the risks.[186] Despite the lack of monetary fines (which were unavailable under Section 5 of the FTCA), TJX faces large compliance costs; some estimate that costs range "anywhere from $500 million to nearly $1 billion in expenses [arising from settlements and compliance costs], not to mention a black eye with the public."[187] Nevertheless, many still view the FTC settlement to be "a very light slap on the wrist" for TJX.[188]

---

182. Complaint at 2, *In re* TJX Cos., 2008 F.T.C. Lexis 39 (Mar. 27, 2008) (No. 072-3055).

183. *Id.*

184. *Id.* at 3.

185. Decision & Order, *In re* TJX Cos., 2008 F.T.C. Lexis 76 (July 29, 2008) (No. C-4227).

186. *Id.*

187. Andy Patrizio, *How TJX Became a Lesson in Proper Security*, INTERNETNEWS.COM, Dec. 5, 2007, http://www.internetnews.com/ent-news/article.php/3714611.

188. Linda McGlasson, *Reaction to TJX Settlement: "A Very Light Slap on the Wrist"*, BANK INFO SECURITY, Mar. 28, 2008, http://www.bankinfosecurity.com/articles.php?art_id=793.

State Attorneys General, led by Massachusetts Attorney General Martha Coakley, also investigated the TJX security breach.[189] Ultimately, forty-one State Attorneys General joined in this multistate action.[190] TJX agreed to pay the states $9.75 million and to implement and maintain a comprehensive information security program designed to address weaknesses in the TJX systems in place at the time of the breach.[191]

In terms of private action, both financial institutions and consumers brought class action lawsuits against TJX for the security breach. Eventually, all class action lawsuits against TJX were consolidated in the District of Massachusetts with the case proceeding on two tracks: the Financial Institutions Track and the Consumer Track.[192] The financial institutions alleged breach of contract and claimed that TJX had violated state and federal laws relating to negligent misrepresentation and unfair and deceptive acts.[193] They also claimed that TJX was negligent in the retention and control of its databases.[194] Plaintiffs sought compensation for the reissued cards and all fraudulent transactions traced to the breach.[195] Consumer plaintiffs brought claims for negligence, breach of contract as third-party beneficiaries, and violations of Massachusetts' consumer protection laws.[196]

The Financial Institutions Track mostly settled. On December 19, 2007, financial institutions representing more than ninety-

189. *See* Press Release, Office of Mass. Att'y Gen., Massachusetts Attorney General Martha Coakley to Address Communication Law Conference on Privacy Protection (Nov. 12, 2008), http://www.mass.gov/?pageID=cagopressrelease&L=1&L0=Home&sid=Cago&b=pressrelease&f=2008_11_12_pli_convention&csid=Cago; *see also* Press Release, Office of Conn. Att'y Gen., Attorney General Warns Consumers of T.J. Maxx, Marshalls, Homegoods and A.J. Wright to Monitor Credit (Apr. 10, 2007), http://www.ct.gov/ag/cwp/view.asp?A=2341&Q=376584.

190. Press Release, Office of Mass. Att'y Gen., Attorney General Martha Coakley Announces Multi-State Settlement with the TJX Companies, Inc., over Massive Data Breach (July 30, 2009), http://www.mass.gov/?pageID=cagopressrelease&L=1&L0=Home&sid=Cago&b=pressrelease&f=2009_06_23_tjx_settlement2&csid=Cago.

191. *Id*.

192. AM. BANKERS ASS'N, OFFICE OF THE GEN. COUNSEL, STATUS OF IMPORTANT BANKING CASES 27 (2008), http://www.gabankers.com/e-Bulletin/Bank_Counsel.SIBC/2008/sibcjune2008.pdf.

193. *In re* TJX Cos. Retail Sec. Breach Litig., 564 F.3d 489, 491–92 (1st Cir. 2009).

194. Plaintiff's Class Action Complaint, *In re* TJX Cos. Retail Sec. Breach Litig., 584 F.Supp.2d 395 (D. Mass. 2007) (No. 07-10162-WGY).

195. *Id.*

196. Amended Consolidated Class Action Complaint, *In re* TJX Cos. Retail Sec. Breach Litig., 584 F.Supp.2d 395 (D. Mass. 2008) (No. 07-10162-WGY).

five percent of the breached Visa accounts approved a settlement that required TJX to pay up to $40.9 million in alternative recovery payments to Visa to compensate the banks that issued Visa cards that were potentially affected by the breach.[197] On May 14, 2008, TJX also announced its settlement with MasterCard whereby it would pay $24 million to compensate the banks that reissued MasterCard cards and were otherwise affected by the breach.[198] This result effectively shifted the financial institutions' costs from the data breach to the breaching entity.

The Consumer Track reached a settlement with TJX that was approved on July 15, 2008.[199] While TJX claimed that the settlement provided for over $200 million in theoretical benefits to the consumer class, as of October 30, 2008, class members claimed it was just over $6 million, a figure the judge says is "unlikely significantly to increase."[200] The initial settlement included: three years of credit monitoring and identity theft insurance for customers whose information was breached, reimbursement for any documented losses customers sustained arising from the breach, TJX store vouchers, and a customer appreciation event where prices will be reduced by fifteen percent.[201] Massachusetts Attorney General Coakley, joined by nine other Attorneys General, vehemently opposed the customer appreciation event and, in a letter to the district court judge, stated that the sale should not qualify as a class benefit because it "is nothing more than a retail sale, which would primarily benefit the defendant, TJX Companies."[202] The court, in agreement, struck that provision from the settlement.[203]

---

197. Press Release, TJX Cos., Inc., The TJX Companies, Inc. Announces Acceptance Rate Over 95% for Visa Settlement Agreement (Dec. 20, 2007), http://www.businesswire.com/news/tjx/20071220006052/en.

198. Press Release, TJX Cos., Inc., The TJX Companies, Inc. Completes Previously Announced MasterCard Settlement; Acceptance Rate Exceeds 99% (May 14, 2008), http://www.businesswire.com/news/google/20080514006313/en.

199. *In re* TJX Cos. Retail Sec. Breach Litig., 584 F. Supp. 2d 395, 398 (D. Mass. 2008).

200. *Id.* at 401.

201. Press Release, TJX Cos., Inc., The TJX Companies, Inc. Agrees to Settlement of Customer Class Actions; Subject to Court Approval; Estimated Costs of Settlement Already Reflected and Disclosed (Sept. 21, 2007), http://www.tjx.com/Press%20release%20electronic.pdf.

202. Letter from Martha Coakley, Mass. Att'y Gen., to William G. Young, U.S. Dist. Court Judge 1 (Nov. 16, 2007), http://www.legalnewsline.com/content/img/f204304/coakleyletter.pdf.

203. *In re TJX Cos. Retail Security Breach Litig.*, 584 F. Supp. 2d at 398 n.2.

## C. STATE VERSUS FEDERAL ENFORCEMENT

There are many reasons why states should continue taking the lead in data breach notification both through enactment of state laws and through enforcement. Historically, state legislatures have created most privacy protection laws.[204] Additionally, states serve as ideal laboratories for social and economic experiments.[205] California's data breach law became the model for other states after the ChoicePoint incident.[206] State data breach laws are so successful that many important FRCA protections originated in the states.[207]

Those who criticize the states for taking the lead in enforcing data breach notification laws point to the difficulty in navigating the maze of state laws to ensure compliance.[208] Yet state-created notification laws have effectively created a race to the top. Companies are developing protocols that satisfy the most stringent state statutes to ensure compliance with the various notification laws.[209] Additionally, states have taken the lead in enforcement because they are generally better able to pass statutes quickly in response to changing needs.[210] Though a few states are just beginning to pass data breach notification laws, many others are enacting cost-shifting statutes.[211] These statutes assign liability

---

204. Daniel J. Solove & Chris Jay Hoofnagle, *A Model Regime of Privacy Protection*, 2006 U. ILL. L. REV. 357, 380–81 (2006).

205. *Id.* (citing New State Ice Co. v. Liebmann, 285 U.S. 262, 311 (1932) (Brandeis, J., dissenting)).

206. *Developments in Banking and Financial Law: 2006–2007*, 26 ANN. REV. BANKING & FIN. L. 1, 42 (2007).

207. Solove & Hoofnagle, *supra* note 204, at 381.

208. *See, e.g.*, Joan Goodchild, *Federal Data Breach Law? No Time Soon*, PC WORLD, Dec. 11, 2008, *available at* http://www.pcworld.com/businesscenter/article/155337/federal_data_breach_law_no_time_soon.html.

209. *See* SAMUELSON LAW, TECH. & PUB. POLICY CLINIC, UNIV. OF CAL. AT BERKELEY SCH. OF LAW, SECURITY BREACH NOTIFICATION LAWS: VIEWS FROM CHIEF SECURITY OFFICERS 14–18 (2007), *available at* http://www.law.berkeley.edu/files/cso_study.pdf.

210. Richard Briffault, *Federalism*, *in* THE OXFORD COMPANION TO AMERICAN LAW 299, 303 (Kermit L. Hall ed., 2002) ("State-level decision-making makes it possible for government to be more responsive to diverse needs, preferences, and circumstances of our heterogeneous society. Different states may take different approaches — reflective of different local views — to the same problems.") .

211. *E.g.*, MINN. STAT. § 325E.64 (2010); TEX. BUS. & COM. CODE ANN. § 35.595 (Vernon 2010); TEX. FIN. CODE ANN. § 11.309 (Vernon 2010). There is a similar bill pending in New Jersey. S. 2440, 212th Leg., 1st Sess. (N.J. 2006), *available at* http://www.njleg.state.nj.us/2006/Bills/S2500/2440_I1.PDF. A similar bill in Illinois has been stayed without assigning a day for further hearing. H.B. 605, 95th Gen. Assem.,

for consequential costs from financial institutions to merchants who have been breached.[212] In comparison, proposed federal laws are a generation behind state laws, focusing mainly on notification rather than deterrence and prevention.

States also respond more quickly to complaints of local data breaches than the FTC.[213] Moreover, states are not limited to local actions; they can collaborate to effect national change that is just as comprehensive as federal enforcement.[214] The various state statutes and enforcement in the area of security breaches have been surprisingly successful in ensuring that consumers are protected in the absence of a uniform federal law.

Although the progression from passive notification requirements to active prosecution of businesses for poor data security has brought about better protection for consumers, it is only the start of what is needed to prevent data breaches. Whereas FTC or State Attorneys General actions merely affect the targeted company, regulations reach much further in requiring industry compliance.[215] Government enforcement under unfair or deceptive practice statutes has deterrent effects. However, shortages in enforcement result because the FTC or State Attorneys General "may never act against other companies committing the same

---

Reg. Sess. (Ill. 2007), *available at* http://www.ilga.gov/legislation/95/HB/PDF/09500HB0605lv.pdf. Merchant liability legislation was also vetoed in California, A.B. 779, 2007 Leg., Reg. Sess. (Cal. 2007), *available at* http://www.leginfo.ca.gov/pub/07-08/bill/asm/ab_0751-0800/ab_779_bill_20070914_enrolled.pdf, and is pending in: Connecticut, H.B. 5491, 2007 Gen. Assem., Jan. Sess. (Conn. 2007), *available at* http://search.cga.state.ct.us/2007/TOB/H/2007HB-05491-R00-HB.htm; and Massachusetts, S.B. 180, 185th Gen. Ct., Reg. Sess. (Mass. 2007).

212. *See, e.g.*, MINN. STAT. § 325E.64 (2010).

213. *See, e.g.*, Press Release, Office of Tex. Att'y Gen., Attorney General Abbott Launches Wide-Scale Investigation of Web Sites Selling Cell Phone Records (Jan. 26, 2006), http://www.oag.state.tx.us/oagNews/release.php?id=1425; Press Release, Office of Or. Att'y Gen., Myers Files Agreement with Providence Health System over Data Breach Issue (Sept. 26, 2006), http://www.doj.state.or.us/releases/2006/rel092606a.shtml (discussing Oregon State Attorney General Myers's settlement agreement over release of 365,000 patient records of mostly Oregon residents).

214. *See, e.g.*, Press Release, Office of N.Y. Att'y Gen., States Settle with Student Data Collection Company (Jan. 13, 2005), http://www.oag.state.ny.us/media_center/2005/jan/jan13a_05.html (discussing a forty-two-state settlement with the National Research Center for College and University Admissions, which was accused of falsely representing that it only shared data with educational institutions when it in fact sold personal data for commercial purposes).

215. Mark E. Budnitz, *The Federalization and Privatization of Public Consumer Protection Law in the United States: Their Effect on Litigation and Enforcement*, 24 GA. ST. U. L. REV. 663, 672 (2008).

offense for a variety of reasons."[216] Thus, it is necessary to shift from mere notification and spotty enforcement toward prevention by regulation. These regulations should be left up to the states because of their historic protection of consumers through notification statutes, their quicker response rate, and their role as effective laboratories for experimentation. Furthermore, the states are better equipped to regulate because Attorneys General already use unfair or deceptive practice statutes to protect against lax security measures. States, especially when acting in unison, are just as, if not more, effective than the federal government.

## V. FUTURE OF DATA BREACH LAWS

This Section will consider some trends in federal and state laws that have either been recently passed or are pending to give a sense of where security breach laws may be heading. This pending legislation demonstrates the shift from after-the-fact notification to the prevention of further fraud by attacking the source of the data loss.

### A. PROPOSED FEDERAL BILL H.R. 2221 — THE DATA ACCOUNTABILITY AND TRUST ACT

In various attempts to legislate a unifying notification statute, lawmakers debated whether federal or state agencies should enforce the new law, whether data security protections should be included, and what risk-of-harm threshold should be used (for example, "reasonable risk" of identity theft).[217] Some experts on privacy and security, such as Chris Wolfe, do not expect Congress to pass a federal law because of the tension between businesses that want a high threshold for notification (giving them discretion as to when they must notify consumers) and many consumer groups that worry too much discretion will mean consumers almost never receive notification.[218] Nevertheless, the House passed the Data Accountability and Trust Act ("DATA") on December 8, 2009.[219] Although the Senate has yet to pass a corres-

216. *Id.* at 671.
217. Covington & Musselman, *supra* note 90, at 648.
218. *Id.*
219. Data Accountability and Trust Act, H.R. 2221, 111th Cong. (2009).

ponding bill, DATA is the closest Congress has come to enacting a uniform notification law.[220]

DATA generally follows the core of the California data breach notification law. However, DATA goes further than the California law by prescribing some minimal requirements for system security, such as the requirements to dispose of obsolete data and to monitor for system breaches.[221] DATA covers entities engaged in interstate commerce that own or possess personal information in electronic form.[222] Thus, state notification laws would then only apply to intrastate data breaches. Under DATA, notification is triggered when the breach is discovered,[223] but an exemption exists when the entity "determines that there is no reasonable risk of identity theft, fraud, or other unlawful conduct."[224] Similar to the California law, encrypted data is subject to a rebuttable presumption that no risk of identity theft or fraud exists, and such data is therefore exempt from notification requirements.[225] DATA provides for written and electronic notification to the affected parties.[226] It also grants the FTC power to promulgate regulations concerning the circumstances that allow for substitute notification and to provide guidance regarding the content of notification.[227] Additionally, DATA requires notification to the FTC following a breach.[228] The FTC is primarily responsible for enforcement because DATA specifically codified violations of notification provisions as unfair and deceptive acts or practices.[229] State Attorneys General may also bring civil actions for injunctive relief or damages not to exceed $5 million dollars.[230] Nevertheless, DATA does not limit the authority of the State Attorneys General under their state consumer protection laws.[231] For affected consumers, there is no remedy other than notification of the breach

220. Personal Data Privacy and Security Act of 2009, S. 1490, 111th Cong. (2009).
221. H.R. 2221 § 2.
222. § 3(a).
223. *Id.*
224. § 3(f)(1).
225. § 3(f)(2).
226. § 3(d)(1)(A).
227. § 3(d).
228. § 3(a). There are additional requirements for data information brokers. § 2(c).
229. *See* § 4(b)(1).
230. § 4(c).
231. § 6(b)(2).

and reception of quarterly credit reports for two years thereafter.[232]

DATA has a few shortfalls. The bill does not address how it would interact with existing federal laws, particularly the GLBA, as it also requires notification after a security breach.[233] Additionally, DATA places the burden on consumers both to request their personal information from data brokers and to ensure the accuracy of that information; however, the law does not provide consumers with any remedy if that information is breached.[234] Although DATA has a few minimal system security requirements, it is still focused on notification rather than prevention of data breaches. Furthermore, by preempting state notification laws that have more advanced features, like shifting the cost of the breach from financial institutions to the breaching entity, DATA erodes many deterrent mechanisms currently in place. Just as DATA hints at the need to shift from mere notification to prevention by requiring some security measures, the following section will illustrate how state breach laws are much more cutting-edge in terms of the shift toward preventing data breaches.

## B. PROPOSED STATE BILLS AND NEW STATE LAWS

A new area of state law development is merchant liability provisions whereby businesses that accept credit or debit cards are prohibited from retaining information from the card's magnetic strip beyond a prescribed time.[235] If an entity retains that information and is subsequently subjected to a security breach, it is liable for financial institutions' expenses, such as expenses for notification, canceling and reissuing cards, closing accounts, blocking transactions, and refunding customers.[236] This provision

232. § 6(b)(1).

233. *See* Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 Fed. Reg. 15,736, 15,743 (Mar. 29, 2005) (to be codified at 12 C.F.R. pts. 30, 208, 225, 364, 568, 570). Some have proposed strengthening existing legislation to address this issue by dealing with some of the opt-outs in the GLBA. *See* Oliver Ireland & Rachel Howell, *The Fear Factor: Privacy, Fear, and the Changing Hegemony of the American People and the Right to Privacy*, 29 N.C. J. INT'L L. & COM. REG. 671, 681–82 (2004).

234. *See* § 2(b)(3)(B).

235. *See* Morrison Foerster LLP, Merchant Liability for Security Breaches, http://www.mofo.com/news/updates/files/12393.html (last visited May 11, 2010).

236. *Id.*

is included in a recently passed Minnesota law[237] and a California legislative bill that was ultimately vetoed.[238]

The Minnesota law has two sections and applies to any "person or entity conducting business in Minnesota" that accepts credit cards, debit cards, stored value cards, or similar cards issued by a financial institution.[239] The first part took effect August 1, 2007 and prohibits entities doing business in Minnesota from storing full track data (that is, information stored on the card's magnetic strip) for more than forty-eight hours.[240] The track data includes the card verification value ("CVV"), which is a unique authentication code embedded on the magnetic strip, the three to four digit security code on the back of the card (also known as "CVV2"), and any PIN verification code number.[241] The CVV, CVV2, and PIN are highly "sought after by hackers and when compromised can expose the payment system to undue risk" because a duplicate card can easily be made that will appear indistinguishable from the original card during the authorization process.[242] In this regard, the Minnesota statute goes further than previous laws, not only in expanding the definition of what information is protected, but in specifically targeting the prevention of credit card fraud through data breaches.

The second part of the Minnesota law took effect August 1, 2008, requiring companies to reimburse card-issuing financial institutions for the "costs of reasonable actions undertaken by the financial institution as a result of the breach in order to protect the information of its cardholders."[243] For example, it requires notification of breach, cancellation and reissuance of cards, closing or reopening accounts and stop payments, and refunds to

---

237. See James T. Graves, Note, *Minnesota's PCI Law: A Small Step on the Path to a Statutory Duty of Data Security Due Care*, 34 WM. MITCHELL L. REV. 1115 (2008), for a more detailed discussion of this law.

238. Evan Schuman, *Governor Kills California Data Protection Law*, EWEEK, Oct. 15, 2007.

239. MINN. STAT. § 325E.64 (2010).

240. *Id.*

241. *Id.*

242. Visa CISP Bulletin, Top Five Data Security Vulnerabilities Identified to Promote Merchant Awareness, http://www.uschamber.com/NR/rdonlyres/eyzkc6zyokejn5n64o7vpmgvqxyd7dodczrpuc5tpqzoinz5gq7mpy3puuct43h6cgtr4kf3hmpx6hugw5kiktflzyh/top_5_alert.pdf (last visited May 11, 2010).

243. § 325E.64.

cardholders for unauthorized transactions.[244] If the financial institution pays damages to the consumers due to the breach, the statute provides that institution with a cause of action against the breaching merchant to recover the costs.[245]

Even though California's proposed security breach statute was eventually vetoed, it contained exemplary provisions that established merchant liability and shifted the cost of breaches from financial institutions to the entity that experienced the breach.[246] The proposed statute was even broader than Minnesota's law: in addition to prohibiting storage of sensitive authentication data, it also restricted employee handling of "payment-related data."[247] Moreover, the bill forbade sending unencrypted payment-related data over open public networks and required entities to limit access to payment-related data to people whose jobs require access.[248] Finally, similar to Minnesota's statute, the California bill included a provision that allowed financial institutions to be reimbursed for the "reasonable and actual costs" of providing data breach notification from entities that maintain but do not own or license breached personal information.[249] From the recent state and federal legislative developments, it is clear that the future of data breach laws must address the area of prevention.

## VI. PROPOSAL: INCREASE DATA BREACH LIABILITY BUT PROVIDE A PCI DSS-BASED SAFE HARBOR

While notification allows consumers to take action to prevent further fraud, it essentially only tells people that their data are gone.[250] Merchant liability laws, which states only recently have begun to adopt, merely affect credit or debit card data and incentivize companies to invest in prevention by placing the costs of a

244. *Id*.
245. *Id*.
246. *See* A.B. 779, 2007 Leg., Reg. Sess. (Cal. 2007), *available at* http://www.leginfo.ca.gov/pub/07-08/bill/asm/ab_0751-0800/ab_779_bill_20070914_enrolled.pdf.
247. § 1.
248. *Id.* These provisions may have been aimed at recent data breaches over wireless networks, such as TJX, and at situations where an insider steals or accidentally releases customers' personal information.
249. *Id.*
250. *See* Letter from the Nat'l Ass'n of Att'ys Gen. to Members of Cong. 2 (Oct. 27, 2005), http://financialservices.house.gov/AttorneysGeneralInfoSecurityIDTheftLetter.pdf (noting that early notification is the key to preventing loss).

breach on the breaching entity. The problems with the current approaches are threefold: enforcement on a case-by-case basis may lead to ambiguity in data security standards and spotty enforcement; victims who suffered actual harm are not compensated; and most personal information is not covered. Thus, it is necessary to focus more on prevention through new two-prong legislation.

First, new laws must build upon the existing notification and merchant liability statutes by defining a minimum security standard as a safe harbor to prevent new laws from becoming too onerous for businesses. Moreover, new laws must expand the scope of personal information that is covered and assist victims in receiving compensation. Finally, this legislation should be implemented at the state level because states strongly protect consumer rights, respond more quickly than the federal government, and serve as ideal laboratories to test new solutions.

### A. PCI DSS-BASED SAFE HARBOR

In addressing the shortfalls of notification-plus-merchant liability regimes, this proposal is based on foundational principles in the Payment Card Industry Data Security Standard ("PCI DSS"). PCI DSS is an extensive industry security standard designed by major credit card companies (Visa, MasterCard, Discover, American Express, and JCB) to prevent identity theft.[251] Major credit card issuers impose PCI DSS on merchants that store, process, or transmit cardholder data.[252] According to the current version of the standard, version 1.2, there are twelve requirements for compliance, one of which prohibits storing track data from credit cards (as was recently legislated in Minnesota).[253] Although these

251. About the PCI Data Security Standard (PCI DSS), PCI Security Standards Council, https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml (last visited May 11, 2010).

252. Jaikumar Vijayan, *Befuddled Companies Get Checklist for Complying with PCI Security Standard*, COMPUTER WORLD, Mar. 9, 2009, http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9129277.

253. About the PCI Data Security Standard (PCI DSS), PCI Security Standards Council, *supra* note 251 (noting the 12 requirements to: 1) "[i]nstall and maintain a firewall configuration to protect cardholder data[; 2) d]o not use vendor-supplied defaults for system passwords and other security parameters . . . [; 3) p]rotect stored cardholder data[; 4) e]ncrypt transmission of cardholder data across open, public networks . . . [; 5) u]se and regularly update anti-virus software[; 6) d]evelop and maintain secure systems and appli-

requirements will not completely prevent security breaches, if strictly followed they would likely have made a difference in recent data breach cases. For example, TJX may have avoided the largest data breach in history if it had followed all twelve — rather than merely three — of the PCI DSS requirements.[254] Even though PCI DSS is tailored for credit or debit cards, some of its principles can be expanded to securing all forms of data currently covered by data breach notification laws.

To effectively impose PCI DSS principles, the desire to prevent data breaches must be balanced with the significant costs of prevention and the financial limitations of companies. To accomplish such balance, this Note proposes that a new data breach prevention statute should provide compliant businesses a safe harbor from any increased liability. The question, therefore, is what businesses must do to qualify for the safe harbor.

Instead of an absolute standard to reach the safe harbor, state legislatures should adopt a tiered system of requirements, holding businesses with more personal data to higher security requirements and merchants with less personal data to more minimal measures.[255] For example, every business would be prohibited from storing personal information longer than necessary and be required to change default passwords, maintain an updated antivirus program, and run a firewall; companies with more personal data would additionally be required to track and monitor their systems, develop a security information policy, and have periodic third-party auditing of system integrity.

Moreover, legislatures should strive to codify the security principles embodied in PCI DSS, rather than requiring specific

---

cations . . . [; 7) r]estrict access to cardholder data by business need-to-know[; 8) a]ssign a unique ID to each person with computer access[; 9) r]estrict physical access to cardholder data . . . [; 10) t]rack and monitor all access to network resources and cardholder data[; 11) r]egularly test security systems and processes . . . [; and 12) m]aintain a policy that addresses information security").

254. *See* Gerson Lehrman Group, TJX Proposes $40.9 Million Settlement with Visa Inc. in the Largest Data Breach of 94 Million Cardholders, *supra* note 176.

255. Visa has four categories of merchants; the first two categories are merchants who process more than one million Visa transactions a year and whose transactions account for about two-thirds of Visa's U.S. transaction volume. *Visa Reports Mid-Sized Merchants Are Making PCI Progress*, DIGITAL TRANSACTIONS NEWS, Jan. 22, 2008, http://www.digitaltransactions.net/newsstory.cfm?newsid=1652; *see also* Visa Cardholder Information Security Program, http://usa.visa.com/merchants/risk_management/cisp_merchants.html (last visited May 11, 2010).

technology, to avoid having to constantly update the law. For example, requiring businesses to change default passwords or restrict employee access does not require a specific technology; businesses may use sophisticated biometrics to limit physical access to computers with sensitive data or they might simply lock the computer room and give the key to a trusted employee.

Codifying the minimum security standards businesses must meet to enjoy safe harbor protection resolves the first problem of spotty enforcement and ambiguous standards. Businesses who comply with the standard are assured that, if a data breach occurs, they will only be liable under the current notification and merchant liability laws. Moreover, by implementing tiered requirements, the new laws will not be overly burdensome for businesses. Additionally, by adopting principles rather than simply requiring businesses to comply with PCI DSS,[256] legislatures avoid the criticisms that private organizations are creating public law,[257] and private organizations responsible for promulgating the standards avoid the criticism of possible self-dealing.[258]

## B. INCREASING COVERAGE AND LIABILITY FOR BREACHING ENTITIES

The safe harbor based on PCI DSS principles will not incentivize businesses to comply without increasing the coverage and liability of the new prevention laws. Although the safe harbor will provide ascertainable standards, it is the assurance that compliance will preclude heavy additional penalties that will truly force businesses to comply. In other words, businesses that fall

256. In 2007, the Texas legislature proposed a bill that generically codified PCI DSS by requiring businesses that collect or maintain sensitive personal information in connection with credit or debit cards to "comply with payment card industry data security standards." H.B. 3222, 80th Leg., Reg. Sess. § 48.102(c) (Tex. 2007).

257. Nevertheless, generally, "if some official of the state is independently responsible for the final promulgation of the law, the fact that statutes or regulations were originally prepared and submitted by private or non-governmental groups does not invalidate the legislation." 1 SUTHERLAND STATUTES AND STATUTORY CONSTRUCTION § 4:11 (6th ed. 2009).

258. Arguably, the credit card industry's regulations are less like Enron and more like the technical industries that have multiple parties who develop the regulations and donate intellectual property to allow free access to the protocol. Additionally, because there are monetary penalties and potential lawsuits involved, businesses that must comply with this standard help to deter the credit card industry's opportunistic behavior.

within the safe harbor will not be subjected to the increased liability described below. The proposed additional liability will come from expanding the definition of personal information and making it easier for consumers to prove damage as a result of a data breach and from increasing coverage in merchant liability laws.

Currently, most data breach laws define personal information as a name in conjunction with some other identifying information — such as a social security or driver's license number — that would allow access to financial information.[259] This definition must be broadened to include *any* information that could lead to fraud or identity theft, such as the maiden name of the individual's mother and biometric information. Expanding what qualifies as personal information protects a larger population of consumers when data is compromised. Additionally, individuals in this larger population of consumers are empowered to bring claims against entities that experience a data breach, thereby exposing them to greater liability.

This liability could not be realized, however, without overcoming the difficulty of establishing causation to demonstrate that victims suffered actual harm as a result of the breach. One way to remedy this problem is to shift the burden of proof by creating a rebuttable presumption that would require the breaching entity to prove that the consumers' harm was *not* a result of the data breach, rather than requiring the consumer to prove that the harm *was* caused by the data breach.[260] This solution provides a light yoke for compliant businesses and a significant burden for non-compliant entities that potentially face multiple consumer lawsuits after a data breach.

In addition, new prevention statutes should expand merchant liability laws. Instead of merely holding breaching entities liable to financial institutions for the cost of reissuing credit cards, they should also be liable to all organizations that are affected by the data breach. For example, a breaching business would not only be required to pay for reissuing credit cards, but also for updating government records and police costs due to identity theft and fraud. Thus, expanding coverage increases the number of poten-

259. *See supra* note 39.
260. Graves, *supra* note 237, at 1144–45.

tial claimants and, when combined with the rebuttable presumption for consumer lawsuits, also creates a tremendous economic incentive for businesses to comply with the PCI DSS-based safe harbor to escape increased liability.

## VII. CONCLUSION

Although it is unknown exactly how much is lost each year due to fraud associated with data breaches,[261] it is clear that a wide gap exists in the current data breach notification laws. Despite this gap, State Attorneys General and the FTC protect consumers under unfair or deceptive practices statutes, which allow the government to prosecute businesses that have experienced a breach due to their substandard data security measures and protocols. But this regime is an inadequate solution. Because enforcement is currently case-by-case, there are issues of spotty enforcement and unclear standards. Thus, states, which have traditionally been on the forefront of security breach legislation, are now addressing such losses by shifting the cost of reissuing cards and other expenses related to the breach from financial institutions to the merchant who experienced the breach. In contrast, the federal DATA bill focuses mainly on notification. It is unclear, however, whether this bill will actually become law and how it will interact with current federal statutes that require notification after a data breach.

On the cutting edge of security breach laws is the codification of parts of the PCI DSS. In particular, Minnesota prohibits the storage of track data. It is unclear how this law has changed business practice because measuring prevention (as opposed to enforcement) is difficult. This Note, however, proposes that state legislatures go further than the Minnesota law by adopting principles from PCI DSS where, based on the amount of personal data an entity has, compliance with heightened security specifications provides a safe harbor from increased liability through expanding the definition of personal information, creation of a rebuttable presumption of causation for consumer lawsuits, and increased

261. *But see* Press Release, CyberSource, Fraudsters Filch $4 Billion Online in 2008 (Dec. 10, 2008), http://www.cybersource.com/news_and_events/archive/view.php?page_id=1721 (estimating $4 billion loss to merchants due to online fraud in 2008).

coverage of merchant liability laws. When this proposal is adopted in conjunction with current data breach notification and merchant liability laws, consumers will be protected not only by the opportunity to prevent further fraud after a data breach, but also by decreasing the number of security breaches at the outset. This Note urges state legislatures to advance security breach laws from notification to prevention. While there is no easy fix to the problem of data breach, the ounce of prevention proposed here may turn out to be a pound of cure for consumers who will receive greater protection over their personal information.