3-2007

Notification of Data Security Breaches

Edward J. Janger
Brooklyn Law School, edward.janger@yale.edu

Paul M. Schwartz

NOTIFICATION OF DATA SECURITY BREACHES

Paul M. Schwartz[*]
Edward J. Janger[**]

The law increasingly requires private companies to disclose information for the benefit of consumers. The latest examples of such regulation are state and federal laws that require companies to notify individuals of data security incidents involving their personal information. These laws, proposed in the wake of highly publicized data spills, seek to punish the breached entity and to protect consumers by requiring the entity to notify its customers about the security breach. There are competing approaches, however, to how the law is to mandate release of information about data leaks. This Article finds that the current statutes' focus on reputational sanction is incomplete. An important function of breach notification is mitigation of harm after a data leak. This function requires a multi-institutional coordinated response of the kind that is absent from current policy proposals. This Article advocates creation of a coordinated response architecture and develops the elements of such an approach. Central to this architecture is a coordinated response agent (CRA) that oversees steps for automatic consumer protection and heightens mitigation. This Article also proposes a bifurcated notice scheme that lets firms know that the CRA is watching and is scrutinizing their decision whether or not to disclose information about a breach to the affected individuals. Moreover, the CRA will set in motion automatic protective measures on behalf of the breached consumers. Finally, the CRA will regulate the content of notification messages to reflect the nature of the data breach.

TABLE OF CONTENTS

---

* Professor of Law, Boalt Hall, University of California-Berkeley; Director, Boalt Center for Law and Technology. For their helpful comments and suggestions, we would like to thank Kathy Abrams, David Caron, Anupam Chander, Martin Flaherty, Lauren Gelman, Chris Hoofnagle, Molly Van Houweling, Lance Liebman, Ronald D. Lee, Ronald Mann, Deirdre Mulligan, Gideon Parchomovsky, Anna Paulson, Chris Sanchirico, Stacey Schesser, Daniel Solove, Stephen Sugarman, William Treanor, Teresa Wang and David Yang. This Article also benefited from suggestions at faculty workshops at the University of California-Berkeley (Boalt Hall), Fordham Law School, and the University of Pennsylvania School of Law. We thank Dean Joan Wexler and Dean Christopher Edley for support of this project.

** Professor of Law, Brooklyn Law School.

INTRODUCTION

The law increasingly requires private companies to disclose certain information for the benefit of consumers. Hospitals must publicize performance results for certain medical procedures.[1] Manufacturers of household appliances must label their products with energy-efficiency ratings.[2] Factories must disclose information about toxic releases and workplace injuries.[3] Writing in 1999, Cass Sunstein termed this trend "regulation through disclosure" and characterized it as "one of the most striking developments in the last generation of American law."[4]

The latest example of regulation through disclosure is a requirement that companies notify individuals of data security incidents involving their personal information. Leading the nation, California enacted the first breach disclosure statute, S.B. 1386, which took effect in 2003.[5] The California statute requires a breached entity to perform certain actions after a security breach involving personally identifiable consumer information. Most importantly, the breached organization must notify affected individuals and self-identify as the party responsible for the data leak.[6] Following a series of highly publicized data spills, thirty-three other states and one major metropolitan area, New York City, have enacted similar legislation,[7] and Senator Dianne Feinstein has proposed federal legislation based on the California

1. For analysis of this process of publicizing hospital performance results, see Aaron Twerski & Neil B. Cohen, *The Second Revolution in Informed Consent: Comparing Physicians to Each Other*, 94 NW. U. L. REV. 1 (1999).

2. Regarding the energy efficiency ratings, see, for example, About Energy Star, http://www.energystar.gov/index.cfm?c=about.ab_index (last visited Oct. 10, 2006).

3. Regarding information about toxic releases and workplace injuries, see Cass R. Sunstein, *Information Regulation and Information Standing: Akins and Beyond*, 147 U. PA. L. REV. 613, 614 (1999).

4. *Id.* at 613.

5. CAL. CIV. CODE §§ 1798.29, .82, .84 (West Supp. 2006).

6. *Id.* § 1798.82.

7. *See* Appendix. For a discussion of legislative developments at the state level, see Brian Krebs, *States Keep Watchful Eye on Personal-Data Firms*, June 1, 2005, WASH. POST, at A1.

law.[8] These statutes seek to punish the breached entity and protect consumers by mandating corporate information disclosure.

There are also critics of this approach. A major objection is that the current requirement for customer notice generates too many breach disclosure letters.[9] Critics focus on the disclosure trigger in the California statute and related legislation which requires the sending of notification letters whenever there is a reasonable likelihood that an unauthorized party has "acquired" personal information. These critics point to Aesop's fable, "The Boy who Cried Wolf." As Fred Cate writes, "if the California law were adopted nationally, like the boy who cried wolf, the flood of notices would soon teach consumers to ignore them. When real danger threatened, who would listen?"[10] The *Washington Post* has joined this chorus in editorializing against these laws as creating "tedious warnings" that will cause people to "ignore the whole lot."[11]

A federal guideline for breach notification by financial institutions proposes an alternative paradigm. This document, the Interagency Guidance, takes a two-track approach. Its first track uses a higher disclosure trigger for customer notice: the test is whether there is a reasonable likelihood of "misuse" of the leaked personal information.[12] Its second track uses a lower trigger for notice to the financial institution's supervisory regulatory agency: the test here is whether there is a reasonable likelihood of "unauthorized access" to the breached data.[13] The idea is that a breach letter should not be sent to the affected public unless there is a more significant likelihood of harm. Some observers reject this approach, however, as creating an opportunity for obstruction and delay; they defend the California statute's lower threshold for consumer notification.[14]

Thus, the policy debate about notification considers, among other concerns, the best way to mandate the release of information about data leaks in

---

8. Notification of Risk to Personal Data Act, S. 751, 109th Cong. (2005). As an international example, Japan is the first nation to include a breach notification requirement in a federal law. For a discussion, see Miriam Wugmeister et al., What You Need to Know About Japan's New Law Concerning the Protection of Personal Information, http://www.mofo.com//mofo_dev/news/updates/files/update02019.html (last visited Oct. 10, 2006).

9. *See, e.g.*, Fred H. Cate, *Another notice isn't answer*, USA TODAY, Feb. 27, 2005, at 14A, *available at* http://www.usatoday.com/news/opinion/2005-02-27-consumer-protection-oppose_x.htm; Editorial, *Have You Been Stolen?*, WASH. POST, June 30, 2005, at A22 [hereinafter *Have You Been Stolen?*].

10. Cate, *supra* note 9.

11. *Have You Been Stolen?*, *supra* note 9.

12. Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 Fed. Reg. 15,736, 15,743 (Mar. 29, 2005).

13. *Id.* at 15,741.

14. *See, e.g.*, Anita Ramasastry, *Do Banks and Other Businesses Have a Duty to Notify Customers of Computer Security Breaches?*, FINDLAW (July 13, 2005), http://writ.news.findlaw.com/ramasastry/20050713.html. For an editorial in favor of the California statute's approach, see Editorial, USA TODAY, *Few companies have to tell when identity thieves strike*, Feb. 28, 2005, at 14A.

the private sector.[15] The stakes for consumers are high—a single data spill may compromise the personal data of millions of individuals.[16] The stakes are also high for companies: the Federal Trade Commission (FTC) has engaged in high-profile enforcement actions involving a multimillion dollar settlement in one case,[17] and data leaks, once exposed, will negatively affect customer trust in the breached entity.[18] Yet the jurisprudential issues involved in breach notification have been left largely unexplored. This lack of attention is unsurprising given that little was known about such failures until recently. In the past, companies were able to keep tight control of information about their data security failures.[19] Put differently, there was no perceived need for scholars to think about the jurisprudence of breach notification until California and other states mandated such disclosure and heightened the public's awareness of data security.

A significant focus of the emerging legal regime has been to impose a reputational sanction on breached entities. By forcing a breached firm to notify the consumers whose data have been lost, the law imposes a reputational cost on this entity.[20] However, breach notification serves another, often overlooked function: it can help both customers and business entities mitigate the harm caused by a leak. We seek to distinguish the different aspects

---

15. Two important caveats about the scope of this Article are required. First, it concentrates on data security breaches in the private sector. To be sure, the government and other public sector entities, such as state universities, also maintain large databases containing sensitive information about individuals, including their Social Security Numbers (SSNs), tax records, healthcare records, educational records, and other important personal data. *See generally* Paul M. Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, 80 IOWA L. REV. 553 (1995). Some of this Article's analysis may hold promise for the public as well as the private sector. Nevertheless, the role of reputational sanctions and other incentives are likely to differ in important ways in the private and public sectors. As a result, we reserve examination of issues of data security for governmental databases for another day.

Second, we do not attempt to reinvent the overall system for verification of identity in the United States in this Article. Ambitious and competing academic proposals have been made in this area. *See* Lynn LoPucki, *Human Identification Theory and the Identity Theft Problem*, 80 TEXAS L. REV. 89, 114–30 (2001); Daniel J. Solove, *Identity Theft, Privacy, and the Architecture of Vulnerability*, 54 HASTINGS L.J. 1227, 1243–51 (2003). We are not fully convinced by these existing proposals, however, and choose to concentrate on one area—the issue of informing consumers of data leaks involving their information.

16. The Privacy Rights Clearinghouse has been keeping a running tally of data leaks since early 2005. Privacy Rights Clearinghouse, Chronology of Data Breaches Since the ChoicePoint Incident, http://www.privacyrights.org/ar/ChronDataBreaches.htm (last visited Oct. 10, 2006).

17. News Release, FTC, ChoicePoint Settles Data Security Breach Charges (Jan. 26, 2006), *available at* http://www.ftc.gov/opa/2006/01/choicepoint.htm [hereinafter ChoicePoint News Release].

18. For a discussion of the negative impact of data leaks on consumer trust, see PONEMON INST., NATIONAL SURVEY ON DATA SECURITY BREACH NOTIFICATION 2–4 (2005).

19. Vincent R. Johnson, *Cybersecurity, Identity Theft, and the Limits of Tort Liability*, 57 S.C. L. REV. 255, 265 (2005).

20. Bruce Schneier, a prominent security expert, refers to the method of these statutes as relying on "the 'public shaming' method of security enhancement." Tom Zeller Jr., *The Scramble to Protect Personal Data*, N.Y. TIMES, June 9, 2005, at C1 (noting how many companies persist in sending sensitive data using "tapes and trucks").

of breach notification and to identify trade-offs that arise when a notification approach emphasizes one or another.

This Article argues that the reputational sanction from breach notification can be important, but not for the reasons conventionally discussed. Moreover, mitigation of harms after a breach, another important function of breach notification, requires a multi-institutional, coordinated response of the kind that is absent from current policy proposals. To fill this gap, this Article advocates creation of a coordinated response architecture as well as a critical organization, the Coordinated Response Agent (CRA).[21] In brief, this Article argues for greater automatic protection for consumers, clearer consumer notification, coordinated sharing of information about data incidents among affected entities, and heightened oversight of the decision by breached entities whether to inform consumers or other entities.

I. How We Live Now: The New Risk Environment of Data Security Breaches and Identity Theft

Newsweek has identified a new category of "Letters You Never Want to See."[22] The old kind of letter informed one of a tax audit, rejection from a college, or bad news about a cholesterol reading.[23] The new kind of letter reveals a security breach involving one's personal information. *Newsweek* calls such a missive the "pain letter."[24] No one is immune from being a recipient of such a missive; even the chairman of the FTC, an agency that has an important oversight role over identity fraud, has received such a notification letter.[25] Data spills have occurred for years,[26] but the awareness of data security problems has been heightened by new state laws and a federal regulation that obliges breached companies to mail these "pain letters."

This Part examines the regulatory landscape for firms that process personal data. In a short period of approximately three years, the United States has created significant legal obligations to implement reasonable data security practices for an increasing number of companies. In Section I.A, we consider the legal sources of the requirement of reasonable data security. One of the striking elements of this requirement is the extent to which it represents a delegation of regulation that mixes broad standards ("reasonable data security") with sometimes quite precise rules (whether for certain

---

21. *See infra* Section IV.A.

22. Steven Levy & Brad Stone, *Grand Theft Identity*, Newsweek, July 4, 2005, at 38, *available at* http://www.msnbc.msn.com/id/8359692/site/newsweek/.

23. *Id.*

24. *Id.* at 40. Newsweek notes that this kind of letter informs its recipient that "[s]omeone may have taken possession of your credit-card info, Social Security number, bank account or other personal data that would enable him or her to go on a permanent shopping spree—leaving you to deal with the financial, legal and psychic bills." *Id.* at 38.

25. *Id.* at 40.

26. *See, e.g.*, ID Analytics, National Data Breach Analysis 6 (2006) ("Most likely, breaches occurred for years prior to the passage of SB 1386 [the California Breach statute] and were simply not reported.").

kinds of outside audits, password policies, or staffing requirements). This approach both delegates discretion to the regulated entity and requires it to meet sometimes highly specific legal requirements.

The puzzle that this Article seeks to solve is the likely impact of breach notification on the process of providing data security for personal data. As part of answering this question, we must think about how firms decide how much data security is "reasonable." Section I.B discusses different factors that will shape a company's culture of compliance.

A. *The Legal Environment for Data Security*

While many entities are under a duty to follow reasonable practices for data security, the legal sources of this obligation vary from firm to firm. Because the law gives some leeway in specifying what is reasonable, the regulated entity as well as the specific data processing industry can have a role in shaping the norms of appropriate data security. The obligation of "reasonable" data security represents an example of "delegated regulation." Regarding this concept, a number of scholars have analyzed the fashion in which the government delegates important decisions about the pursuit of public goals to private firms as well as industry organizations. As Jody Freeman argues, "[p]rivate actors are deeply involved in regulation, service provision, policy design, and implementation."[27] Or, as Kenneth Bamberger proposes, a consequence of this delegation of authority is that regulated firms should be viewed as part of the administrative process.[28]

Delegated regulation does not permit firms to make unfettered decisions. But it should be contrasted with the "command and control" approach, in which the government mandates highly specific targets, and regulated entities either obey or suffer civil and/or criminal penalties.[29] Delegated regulation involves a more fluid process.[30] The government and the regulated entity, in effect, negotiate certain elements of governance.[31]

There is also a particular twist for delegated regulation in the law of data security. This area of law delegates by drawing on a mixture of both standards and rules.[32] A standard mandates a decision based on either an

---

27. Jody Freeman, *The Private Role in Public Governance*, 75 N.Y.U. L. REV. 543, 551 (2000) [hereinafter Freeman, *Private Role*]; *see* Jody Freeman, *Extending Public Law Norms Through Privatization*, 116 HARV. L. REV. 1285, 1290 (2003) (discussing private actors' need to determine "when it makes sense to condition private participation in service delivery upon adherence to public law norms, and figuring out how best to implement appropriate terms").

28. Kenneth Bamberger, *Regulation as Delegation: Private firms, Decision-making and Accountability in the Administrative State*, 56 DUKE L.J. 377, 384 (2006); *see* Gillian E. Metzger, *Privatization as Delegation*, 103 COLUM. L. REV. 1367, 1369 (2003).

29. Timothy F. Malloy, *Regulating by Incentives: Myths, Models, and Micromarkets*, 80 TEX. L. REV. 531, 531–33 (2002).

30. *See* Freeman, *Private Role*, *supra* note 27, at 551–53.

31. Bamberger, *supra* note 28, at 398.

32. For an introduction to the jurisprudence of standards and rules, see, for example, Louis Kaplow, *Rules Versus Standards: An Economic Analysis*, 42 DUKE L.J. 557 (1992); Duncan Kennedy, *Form and Substance in Private Law Adjudication*, 89 HARV. L. REV. 1685 (1976); Paul M.

open-ended decision-making principle or a multifactor test. A rule limits discretion through hard-edged decisional criterion. A classic illustration of this dichotomy considers the possibilities for regulating the behavior of an automobile driver at a train crossing: (1) proceed with reasonable caution (the standard); or (2) stop, look, and listen (the rule).[33] The law of data security creates leeway for the regulated entity through its mixture of standards and rules. We examine the regulations for data security in the United States according to a typology based on the nature of the breached entity. Our categories are (1) Business to Consumer–Financial (B2C-Financial); (2) Business to Consumer–Retail (B2C-Retail) and other non-financial entities; (3) outsourcing entities; and (4) data brokers.

1. *B2C-Financial*

Financial institutions in the United States face explicit regulations for data security. Title V of the Gramm-Leach-Bliley Act (GLB Act) requires financial institutions to develop procedures for protecting the security of customer data and empowers the Federal Deposit Insurance Corporation, Office of Comptroller of the Currency, Federal Savings and Loan Insurance Corporation, and other bank regulatory agencies to promulgate data security regulations.[34] These agencies have, in turn, issued two "Interagency Guidances" pursuant to the GLB Act; one requires financial institutions to maintain reasonable data security, and the other requires them to develop a formal response program to deal with data security breaches.[35]

The GLB Act's security regulations oblige companies to use any appropriate measures reasonably designed to protect "the security and confidentiality of customer information."[36] The regulations also articulate certain rules: a financial institution is required to conduct periodic risk assessments, develop a data security program to manage and control risks, apply sanctions against employees that fail to comply with the data security program, and use disclosure and other safeguards when security breaches do occur.[37] The ultimate test remains a broad one, that of reasonableness.[38]

Schwartz, *Voting Technology and Democracy*, 75 N.Y.U. L. REV. 625, 655–57 (2002); Edward J. Janger, *Crystals and Mud in Bankruptcy Law*, 43 ARIZ. L. REV. 559 (2001); Edward J. Janger, *Muddy Property: Generating and Protecting Information Privacy Norms in Bankruptcy*, 44 WM. & MARY L. REV. 1801, 1871–72 (2003).

33. Schwartz, *supra* note 32, at 655.

34. Gramm-Leach-Bliley Act of 1999 § 5, 15 U.S.C. § 6801, 6805 (2000).

35. Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 Fed. Reg. 15,736, 15,743 (Mar. 29, 2005); Interagency Guidance Establishing Information Security Standards, 69 Fed. Reg. 77,610 (Dec. 28, 2004).

36. Interagency Guidance Establishing Information Security Standards, 69 Fed. Reg. 77,610, 77,611.

37. *Id.* at 77,610.

38. *Id.*

2. *B2C-Retail*

Unlike financial institutions, B2C entities do not in general fall under a broad statutory scheme that imposes data-handling responsibilities. Healthcare providers and facilities must follow specialized federal guidelines regarding personal medical information.[39] Moreover, certain companies are obliged to comply with guidelines set through industry self-regulation, which, thus far, have largely proved to have "more public relations bark than actual bite."[40]

The FTC has acted in this regulatory vacuum on nine occasions since 2002.[41] Its basic theory is that a merchant's failure to take reasonable measures to protect customer data is an unfair practice in violation of the Federal Trade Commission Act of 1914 (FTC Act).[42] In a typical data security complaint, the FTC argues that the firm's data-handling practices constituted unfair acts or practices in violation of Section 5 of the Federal Trade Commission Act.[43] In settling its enforcement actions, the FTC has required both

---

39. Sectoral regulations exist for healthcare facilities and health insurers and other medical entities, which are subject to information privacy and data security regulations promulgated pursuant to the Health Information Portability and Accountability Act (HIPAA). HIPAA Regulations, 45 C.F.R. pts 160–64 (2006). In summary, federal regulations explicitly require financial institutions and HIPAA "covered entities" to have reasonable data security, but all other companies operate outside these requirements.

40. Eric Dash, *Credit Card Rivals to Unite in Data Protection Effort*, N.Y. TIMES, Jan. 12, 2006, at C3.

41. In chronological order, these enforcement actions were (1) Eli Lilly & Co., *see* News Release, FTC, Eli Lilly Settles FTC Charges Concerning Security Breach (Jan. 18, 2002), *available at* http://www.ftc.gov/opa/2002/01/elililly.htm; (2) Microsoft Corp., *see* News Release, FTC, Microsoft Settles FTC Charges Alleging False Security and Privacy Promises (Aug. 8, 2002), *available at* http://www.ftc.gov/opa/2002/08/Microsoft.htm; (3) Guess, Inc., *see* News Release, FTC, Guess Settles FTC Security Charges; Third FTC Case Targets False Claims about Information Security (June 18, 2003), *available at* http://www.ftc.gov/opa/2003/06/guess.htm; (4) Petco, *see* News Release, FTC, Petco Settles FTC Charges (Nov. 17, 2004), *available at* http://www.ftc.gov/opa/2004/11/petco.htm; (5) Superior Mortgage Corp., *see* News Release, FTC, Mortgage Company Settles Information Security Charges (Sept. 28, 2005), *available at* http://www.ftc.gov/opa/2005/09/superior.htm [hereinafter Superior Mortgage News Release]; (6) BJ's Wholesale Club, *see* News Release, FTC, BJ's Wholesale Club Settles FTC Charges (June 16, 2006), *available at* http://www.ftc.gov/opa/2005/06/bjswholesale.htm [hereinafter BJ's News Release]; (7) DSW Shoe Warehouse, *see* News Release, FTC, DSW Inc. Settles FTC Charges (December 1, 2005), *available at* http://www.ftc.gov/opa/2005/12/dsw.htm; (8) ChoicePoint, *see* ChoicePoint News Release, *supra* note 17; (9) CardSystems, *see* Agreement Containing Consent Order, In re CardSystems Solutions, Inc, and Solidus Networks, Inc., File No. 052 3148 (F.T.C. Feb. 23, 2005), *available at* http://www.ftc.gov/os/caselist/0523148/0523148consent.pdf.

42. Complaint of FTC at 3, BJ's Wholesale Club, Inc., File No. 042 3160 (June 26, 2005), *available at* http://www.ftc.gov/os/caselist/0423160/050616comp0423160.pdf; Complaint of FTC at 3, DSW Inc., File No. 052-3096 (Dec. 1, 2005), *available at* http://www.ftc.gov/os/caselist/0523096/051201comp0523096.pdf [hereinafter FTC-DSW]; Complaint of FTC at 8, United States v. ChoicePoint, File No. 052-3069, Civil Action No. 06-CV-0198 (Jan. 30, 2006), *available at* http://www.ftc.gov/os/caselist/choicepoint/0523069complaint.pdf [hereinafter FTC-ChoicePoint].

43. 15 U.S.C. § 45(a) (2000). Thus, as one FTC Complaint stated, the "failure to employ reasonable and appropriate security measures to protect personal information and files caused . . . substantial injury to consumers that is not offset by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers." FTC-DSW, *supra* note 42, at 3.

general and specific pledges of reasonable data security.[44] There is more than a fair amount of leeway for entities in deciding what data security measures to take.

3. *Outsourcing Entities*

There is no explicit data security regulation for firms that carry out back-office and other administrative operations involving personal information. But statutory and other regulations applicable to the original data processing entity generally apply to outsourcing entities as well.[45] In addition, the GLB Act data security regulations explicitly oblige financial institutions to "require [their] service providers by contract to implement appropriate measures designed to protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer."[46] Note that this broad language ("appropriate measures") creates a standard. Moreover, the reliance on the contract drafted by the original data collector is a further example of a delegation from the government to a private party.

Self-regulatory efforts by financial institutions also extend to outsourcing companies. As an example, six of the largest financial institutions in the United States have developed joint requirements for the telecommunications companies and data-service hosting companies that they use.[47] These industry requirements, through the Financial Institution Shared Assessments Program, establish standards for security as well as a standard process for assessing security levels.[48] Yet, as has been the case for B2C retailers, self-regulatory restrictions over outsourcing entities have fallen short.

4. *Data Brokers*

In the past, the regulatory hand fell lightly, if at all, on the information-handling practices of data brokers.[49] Data brokers are in the business of col-

---

44. *See* BJ's News Release, *supra* note 41; ChoicePoint News Release, *supra* note 17.

45. A firm that processes personal data for a healthcare facility regulated by HIPAA is required to follow the HIPAA regulations. 45 C.F.R. §§ 164.104, 164.105 (2005).

46. *E.g.*, 12 C.F.R pt. 30, app. B.

47. BITS Financial Services Roundtable, Financial Institution Shared Assessments Program, Frequently Asked Questions, http://www.bitsinfo.org/FISAP/Forms/18SharedAssessmentsFAQ.pdf (last visited Oct. 5, 2006).

48. *Id.*

49. The Fair Credit Reporting Act (FCRA) applies to at least some transactions of data brokers, namely, those that concern a "consumer report," as the FCRA defines this term. 15 U.S.C. § 1681a(d) (2000). But data brokers sell other kinds of information and engage in activities that they view as falling outside the FCRA's jurisdiction. Letter from Elec. Privacy Info. Ctr. (EPIC) to the FTC, Request for investigation into data broker products for compliance with the Fair Credit Reporting Act (Dec. 16, 2004), *available at* http://www.epic.org/privacy/choicepoint/fcraltr12.16.04.html. Regardless of the extent to which the FCRA does or does not apply to the database industry, however, the FCRA itself lacks any data security requirements. 15 U.S.C. § 1681o (2000).

lecting personal information, maintaining it in databases, and extracting value from it by comparing and combining it with other information and then reselling it.[50] They gather information from a variety of sources, including public records and companies that do have direct B2C relations.[51] This gap represented an especially large regulatory vacuum, one in which the FTC took decisive action through an enforcement action against ChoicePoint. Its successful settlement of this action in January 2006 effectively imposes a standard of reasonable security on data brokers.[52]

In settling these charges, ChoicePoint did more than agree to pay $10 million in civil penalties and $5 million into a consumer redress fund. It promised changes to its business and improvements to its security practices. These changes took a shape that will be familiar by now: a mixture of standards and rules. In its settlement with the FTC, ChoicePoint agreed to "establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers."[53] Here, too, a delegation of authority through a standard was supplemented by a handful of rules that provided a greater degree of specificity. Thus, in maintaining this "comprehensive information security program," ChoicePoint promised to engage in risk assessments and to design and implement regular testing of the effectiveness of its security program's key controls, systems, and procedures. It also agreed to obtain an initial and then biennial outside assessment of its data security safeguards from an independent third-party professional.[54]

5. *Tort Law, Sarbanes-Oxley, and State and City Breach Notification Laws*

The final elements in the emerging framework of data security regulations are tort law, the recently enacted Sarbanes-Oxley amendments to federal securities laws, and state breach notification statutes. In tort law, under a general negligence theory, litigants might sue a company after a data security incident and seek to collect damages.[55] Too few cases have occurred to provide any strong basis for predictions about the future of tort actions for data security breaches.[56] Claimants will likely have trouble convincing

---

50. For two recent accounts of these entities, see ROBERT O'HARROW, JR., NO PLACE TO HIDE 145–52 (2005); DANIEL J. SOLOVE, THE DIGITAL PERSON 19–21 (2004).

51. O'HARROW, *supra* note 50, at 51.

52. In its complaint against ChoicePoint, the FTC based its action on the FCRA as well as its statutory authority under the FTC Act. FTC-ChoicePoint, *supra* note 42, at 1.

53. *Id.* at 14.

54. *Id.* at 19.

55. *See* Johnson, *supra* note 19, at 296–310.

56. For cases rejecting tort liability following a data breach, see *Bell v. Acxiom Corp.*, No. 4:06CV00485-WRW, 2006 U.S. Dist. LEXIS 72477 (E.D. Ark. Oct. 3, 2006); *Giordano v. Wachovia Securities LLC*, Civil No. 06-476 (JBS), 2006 U.S. Dist. LEXIS 52266 (D.N.J. July 31, 2006); *Guin*

courts that the data processing entities owe a duty to the identity theft victims. Thus, a South Carolina court declared in 2003 that "[t]he relationship, if any, between credit card issuers and potential victims of identity theft is far too attenuated to rise to the level of a duty between them."[57] This conclusion ignores the reality, however, that the credit card issuer's customer is a foreseeable victim.

Regarding the Sarbanes-Oxley Act, its Section 404 requires the CEO and CFO of a public company to sign off on the company's financial statements. In particular, those officers are required to certify that the company has "adequate internal controls" on corporate data. While the focus of the certification is on the accuracy of financial reporting, one requirement is that these officers certify that these internal controls "[p]rovide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of the issuer's assets that could have a material effect on the financial statements."[58] This single requirement has led software firms to generate products for auditing data security practices, and accounting firms and the various accounting standards boards to develop standards for data security.[59]

Finally, as noted in this Article's Introduction, thirty-three states and one city have enacted notification legislation within a few short years.[60] We have listed these statutes in this Article's Appendix and have analyzed each according to the following criteria: (1) the entities that the law covers; (2) the law's trigger for notification; (3) any exceptions to the law's notification requirement; (4) the party to whom disclosure is required under the law; (5) whether there is a substantive requirement for data security; and (6) the presence or absence of a private right of action. This chart reveals the strong influence of the California breach notification statute. It also provides an overview of trends in the law of breach notification. To summarize our findings, the chart indicates that twenty-three states follow the California approach and rely on the acquisition standard for breach notification. Only seven states have adopted a higher standard. New York City has its own idiosyncratic standard and requires "unauthorized possession" of personal

---

v. Brazos Higher Education Service Corp., Civ. No. 05-668 (RHK/JSM), 2006 U.S. Dist LEXIS 4846 (D. Minn. Feb. 7, 2006); *Stollenwerk v. Tri-West Healthcare Alliance*, No. Civ. 03-0185-PHX-SRB, 2005 U.S. Dist. LEXIS 41054, at *2–3 (D. Ariz. Sept. 8, 2005); *Smith v. Citibank, N.A.*, No. 00-0587-CV-W-1-ECF, 2001 WL 34079057, at *2–4 (W.D. Mo. Oct. 3, 2001), *Polzer v. TRW, Inc.*, 628 N.Y.S.2d 194, 195 (N.Y. App. Div. 1998). In a case involving economic losses following from an identity theft, a California court did award restitutionary damages to a victim, *People v. Ware*, No. H025167, 2003 WL 22120898, at *2-3 (Cal. Ct. App. Sept. 11, 2003). For a case awarding damages following a data breach, see *Bell v. Michigan Council 25 AFSCME*, 2005 Mich. App. LEXIS 353, at *1-2 (Feb. 15, 2005) (finding under "the unique circumstances of this case," a union owed plaintiffs, its members, a duty due to the presence of a special relationship).

57. Huggins v. Citibank, N.A., 585 S.E.2d 275, 277 (S.C. 2003).

58. 17 C.F.R. § 240.13a-15 (2006).

59. *See, e.g.*, Bruce I. Winters, *Choose the Right Tools for Internal Control Reporting*, J. ACCT., Feb. 2004, at 34, *available at* http://www.aicpa.org/pubs/jofa/feb2004/winters.htm.

60. *See supra* note 7 and accompanying text.

information.[61] A mere three states provide a private right of action for individuals whose information has been breached. Finally, only eight of the state statutes create a substantive duty to take reasonable steps to safeguard data.

We wish to say a few more words about these emerging state requirements for reasonable data security. While public and press attention has largely been devoted to these statutes' requirements for informing consumers of data leaks involving their personal information, a few of these laws also explicitly require reasonable data security. Breach notification statutes in Arkansas, California, Nevada, North Carolina, Rhode Island, Texas, and Utah establish such a requirement.[62] These seven state statutes prove to be the most standard-like of all the regulations for data security; they provide open-ended, general standards, such as a requirement to provide "reasonable security procedures and practices appropriate to the nature of the information."[63] In California, such standards are supplemented by nonbinding, albeit more rule-like, recommendations from the Office of Privacy Protection.[64]

B. *Regulatory, Economic, and Reputational Pressures on the Firm*

The "black-box" paradigm assumes, as Timothy Malloy has summarized, that an "organization is a monolithic entity that essentially makes decisions as a natural individual would."[65] In rejecting the black-box concept, this Article views the firm as acting through choices made by the different individuals and different groups who work there. Indeed, within many firms that process personal information, there is an important set of individuals: chief privacy officers (CPOs), chief security officers, chief information officers, all of whom are responsible for a wide range of policy issues regarding data security. There is no standardized job description of where the lines between these different jobs begin and end, and no standardized pattern of corporate adoption of all, some, or none of these different officers. For purposes of simplification, therefore, this Article will refer to these employees with responsibilities for policy issues regarding data security as CPOs.

---

61. NEW YORK, N.Y. ADMIN. CODE § 20-117 (2005). Any impact of the New York City law vanished, however, because the New York State law on breach notification has preempted the City law. See N.Y. Gen. Bus. Law § 899-aa(9) (McKinney 2005) ("No locality shall impose requirements that are inconsistent with or more restrictive than those set forth in this section.").

62. ARK. CODE ANN. § 4-110-104 (2006); CAL. CIV. CODE § 1798.81.5 (West Supp. 2006); Act of June 17, 2005, ch. 485, 2005 Nev. Stat. 2496; N.C. GEN. STAT. § 75–64 (2005); R.I. GEN. LAWS § 11-49.2-2 (2006); TEX. BUS. & COM. CODE ANN. § 48.102 (2005); Consumer Credit Protection Act, 2006 Utah Laws 343 (codified at UTAH CODE ANN. § 13-42-201) (effective January 1, 2007).

63. CAL. CIV. CODE § 1798.81.5(b) (West Supp. 2006).

64. CAL. DEP'T OF CONSUMER AFF., OFF. OF PRIVACY PROT., RECOMMENDED PRACTICES ON NOTICE OF SECURITY BREACH INVOLVING PERSONAL INFORMATION 8 (2006) [hereinafter CALIFORNIA PRIVACY OFFICE, RECOMMENDATIONS].

65. Malloy, *supra* note 29, at 532–33.

The legal benchmark of reasonable data security can lead to ongoing interactions between regulators, different kinds of industry organizations, and CPOs in identifying and implementing processes and practices. But how will companies decide on the kinds of practices that, taken together, constitute reasonable data security? How will companies create policies for notification of consumers after data breaches? This Article separates pressures on firm decision-making into three distinct categories: regulatory, economic, and reputational.[66] In evaluating a regime for data security and breach notification, one should view the collective effect of these three forces within a given firm as forming its overall culture of compliance.

1. *Regulatory Forces*

In making decisions about data security and breach notification, companies are obliged to respond to applicable law and regulations. The law mandates the kinds of behavior that it wishes, and the firm is required to follow its orders. For example, breach notification law requires a company that discovers a security incident involving personal data to give notice to affected parties. Yet one cannot simply assume that the law precisely commands and companies perfectly obey.

Some firms have already demonstrated that they will disregard their legal obligations to disclose material information. One need look no further than the Enron affair for proof of this point.[67] Or consider Superior Mortgage, a lender with branch offices in ten states and multiple web sites. In 2005, Superior Mortgage became the subject of an FTC enforcement action.[68] As a financial institution, Superior Mortgage is subject to the jurisdiction of the GLB Act. Yet this company neglected its obligations, large and small, under these regulations. Its failures included the absence of: (1) any formal assessment of risks to customer information, (2) appropriate password policies to protect company systems and sensitive documents, and (3) an appropriate response program.[69] The law of data security does not, however, rely on simple commands. Rather, it delegates considerable decision-making authority to the regulated entities. If the regulated entities are inclined to resist their obligations, delegated discretion is a troubling choice.

Two further points can be made about the resulting flexibility in the emerging legal commands for data security. First, the precise pattern of standards and rules for data security proves highly context-specific. As an example of a rule, a firm might be required to have one or more specific

---

66. *See* NEIL GUNNINGHAM ET AL., SHADES OF GREEN: BUSINESS, REGULATION, AND ENVIRONMENT 95–134 (2003); *see also* Neil A. Gunningham et al., *Motivating Management: Corporate Compliance in Environmental Protection*, 27 LAW & POL'Y 288 (2005) [hereinafter Gunningham et al., *Motivating Management*]; Neil Gunningham & Robert A. Kagan, *Regulation and Business Behavior*, 27 LAW & POL'Y 213 (2005).

67. Edward J. Janger, *Brandeis, Business Ethics, and Enron*, *in* ENRON: CORPORATE FIASCOS AND THEIR IMPLICATIONS 63 (Nancy B. Rapoport & Bala G. Dharan eds., 2004).

68. Superior Mortgage News Release, *supra* note 41.

69. *Id.*

employees coordinate the firm's data security program, or to utilize certain kinds of password policies.[70] As an example of a standard, FTC enforcement actions require that firms identify "reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information."[71]

Second, data security regulations raise normative issues because they exemplify the phenomenon of delegated regulation. For example, Ian Ayres and John Braithwaite propose a need for "enforced self-regulation" in which the state retains the power of public enforcement (specifically, detection and punishment).[72] More recently, and in a similar vein, Michael Dorf proposed a "rolling regulatory regime" in which regulators draw on information from regulated entities and local experimentalism.[73] Dorf envisions a process in which "performance standards are continually ratcheted up as local experimentation reveals what is possible."[74] We return to these proposals below; important here is simply the idea that any delegation of data security regulation raises important normative questions.

2. *Economic Forces*

Firms seek to maximize profits and are always under economic pressures to do so. Indeed, according to Ronald Coase's seminal analysis, even the boundaries of a company are set in response to these pressures.[75] In his famous rhetorical question, he asks: "[w]ill it pay to bring an extra exchange transaction under the organizing authority?"[76] Firms will grow in size to take on new tasks that are profitable for them, or else simply make contracts with others. As for data security, one can generally expect companies to invest in it from the perspective of wealth-maximizing entities. In other words, firms will seek to calibrate security expenditures according to the level of legal liability and the financial risks that they bear from leaked information. Data security law also acknowledges, at least as a general matter, the legitimacy of economic constraints. It only requires data safeguards that are reasonable—not ones that are perfect, flawless, or otherwise airtight.

---

70. Regulations sometimes create a web of demands on certain companies—this observation is particularly true for financial institutions and the handful of companies with which the FTC has settled its enforcement actions. These rules contain both procedural and substantive requirements. Interagency Guidance Establishing Information Security Standards, 69 Fed. Reg. 77,610, 77,620 to 77,621. (Dec. 28, 2004).

71. Complaint of FTC at 2, Superior Mortgage Corp., File No. 052-3136 (Dec. 14, 2005), *available at* http://www.ftc.gov/os/caselist/0523136/051216comp0523136.pdf.

72. IAN AYRES & JOHN BRAITHWAITE, RESPONSIVE REGULATION 101–20 (1992).

73. Michael C. Dorf, *The Domain of Reflexive Law*, 103 COLUM. L. REV. 384, 398–400 (2003).

74. *Id.* at 399; *see also* Michael C. Dorf & Charles F. Sabel, *A Constitution of Democratic Experimentalism*, 98 COLUM. L. REV. 267, 318–23 (1998).

75. R.H. COASE, THE FIRM, THE MARKET, AND THE LAW 33–55 (1988).

76. *Id.* at 55.

Yet, any assumption that firms act perfectly according to economic self-interest would be simplistic. As an initial general example, firms do pass up a host of profitable and cost-reducing projects on a regular basis.[77] More specifically for data security, companies may fail to (1) fully bear the costs of data breaches or (2) precisely calibrate costs and benefits in deciding their investments in data security.

As to the first point, many entities are not held responsible for the full cost of data breaches, which creates two related externalities. We term these the data security externality and the disclosure disincentive. The data security externality reflects the fact that a data security breach at one company may cause harm at another company in a way that is untraceable or for which there is no legal recourse.[78] Stolen data are likely to lack any provenance, that is, any information about their place of origin. Thus, if we assume the breached entity's silence, any member of the public will be unlikely to be able to identify the place from which data were stolen. As a consequence, consumers may not associate the harm that they suffer with the institution that leaked that data. The institution may also escape financial liability to other financial institutions, because the law generally assigns the financial risks for certain data breaches to the entity that mistakenly relied on the fraudulently-presented information—that is, issued a new credit card, granted a loan, or credited an electronic transfer—rather than the entity at which the breach took place.[79]

The "disclosure disincentive" follows from the nondisclosure externality. Disclosure may increase the risk of liability, because it makes traceable an otherwise untraceable security breach. Furthermore, disclosure also brings publicity to an event and might thereby prompt costly legal action or regulatory scrutiny.

As to the point regarding the calibration of data security levels, evidence from other fields shows how firms can be less than cool calculators of economic investment in compliance. As an example, a large-scale empirical study of corporate environmental behavior by Dorothy Thornton, Neil A. Gunningham, and Robert A. Kagan found that persons responsible for compliance at more than 200 studied facilities were ignorant of the specific penalties their employers faced.[80] At best, corporate compliance officials tend to rely on rough estimates and rules of thumb.

---

77. Malloy, *supra* note 29, at 586–92.

78. For a discussion of how harms occur at locations other than the breached entity, see ID ANALYTICS, *supra* note 26, at 14–18; Tom Zeller Jr., *Black Market In Credit Cards Thrives on Web*, N.Y. TIMES, June 21, 2005, at A1.

79. Section 133 of the Truth in Lending Act, 15 U.S.C. § 1643(a)(1) (2000), limits the liability of a cardholder to $50 for unauthorized charges. For debit cards, the result is similar under the Electronic Funds Transfer Act. 15 U.S.C. § 1693g(a) (2000).

80. Dorothy Thornton et al., *General Deterrence and Corporate Environmental Behavior*, 27 LAW & POL'Y 262, 271–72 (2005).

3. *Reputational Forces*

The third and final pressure on organizational behavior comes through reputational forces and the related concerns of individuals at a company about reputational capital. A host of scholars have demonstrated that individuals, businesses, and other organizations can be profoundly affected by the circulation of information about their prior behavior. In separate works, David Charny and Eric Posner discuss this point from the perspective of norm theory. In Charny's pathbreaking work, for example, sanctions to reputations play an important role in enforcing commitments by a wide range of market participants.[81] More recently, Eric Posner proposes that reputational information plays a key role more generally in structuring a wide variety of cooperative endeavors.[82]

Companies sometimes invest in data security because they care about the regard in which they are held by outsiders, whether consumers, citizens, communities, or social activists.[83] The related literature on information privacy, for example, reveals how some decision-makers are highly sensitive to the risks of a privacy meltdown that would tarnish their company's reputation with the public. A privacy meltdown is the revelation of a firm-wide collection, storage, use, or transfer of personal information that shocks the public and turns it against the company. For example, Laura Gurak shows how reputational concerns played a role in the retreat by Lotus in 1990 from its planned introduction of a database called "MarketPlace: Households."[84] The database was to contain sensitive information about millions of individuals.[85] A well-orchestrated public protest in cyberspace led approximately thirty thousand people to contact Lotus and request that their names be removed from the database.[86] Lotus ultimately abandoned the product; Gurak concludes that the company was concerned not only about its "profit margins," but also "consumer attitudes" towards it.[87] At that time, consumers were likely disturbed by the prying into their lives represented by the compilation and release of this personal information for direct marketing. Today, fear of unauthorized access to such information and the possibility of identity theft would add another level of concern.

Thus, decision-makers at companies frequently care about the reputational capital of their firms and seek both to avoid social sanctions against

---

81. David Charny, *Nonlegal Sanctions in Commercial Relationships*, 104 HARV. L. REV. 373, 393–94 (1990).

82. ERIC A. POSNER, LAW AND SOCIAL NORMS 18–25 (2000).

83. *See* BEN SMITH & BRIAN KOMAR, MICROSOFT WINDOWS SECURITY RESOURCE KIT 4 (2003) (noting that the loss of an "asset" through a security incident includes the cost of the "loss of public trust or confidence").

84. LAURA J. GURAK, PERSUASION AND PRIVACY IN CYBERSPACE 19–31 (1997).

85. *Id.* at 19–20. The database included names, addresses, and detailed information on the spending habits of 120 million Americans. *Id.* at 19, 21–22.

86. *Id.* at 29.

87. *Id.* at 43.

them and to gain social approval. But concerns about reputation do not exist only at the organization level. Reputational concerns also operate at the level of individuals within the firm. In the United States, in notable contrast to Canada and Germany,[88] *information privacy* law has not generally required the creation of enterprise-wide CPOs.[89] Nonetheless, a wide variety of companies in the United States have created such positions within their ranks.[90] Moreover, *data security* law recently has started to require companies to designate specific employees as responsible for their data-handling practices and breach-response programs.[91] A trend has been to fold at least some of these data security obligations into existing offices of the CPO.

In a more immediate way than anyone else in a firm, the CPO has her professional reputation on the line for issues regarding both information privacy practices and data security leaks. This direct link should lead this corporate officer to focus on the effectiveness of data security systems. Moreover, when a firm creates these officers, it brings a higher profile within the organization to the underlying task of providing data security. Where the stakes are high enough, however, reliance on CPOs, industry self-regulation, and cooperation or confession by the corporation may not provide an adequate solution to the data security problem.[92]

Reputation is not everything, and concerns about reputation do not have a uniform impact on different individuals or firms. For one thing, larger and more established firms, like Lotus in 1990, are likely to place a higher value on their reputation than smaller, newer companies.[93] In addition, CPOs may be more concerned with quotidian pressures from within a firm than with their reputation among their peers or regulators. Moreover, the sharing of reputational information about a firm, even a classic "bad apple," may not lead to effective public sanctions against it. And to the extent that the bad

---

88. *See* Personal Information Protection and Electronic Documents Act., 2000 S.C., ch. 5 (Can.); Bundesdatenschutzgesetz [BDSG, Federal Data Protection Act], Jan. 1, 2003, RGBl. I at § 4f (F.R.G.). Regulations in Japan require only that financial institutions appoint a CPO. Wugmeister et al., *supra* note 8.

89. The two exceptions are regulations issued under the Gramm-Leach-Bliley Act and the Health Insurance Portability and Accountability Act (HIPAA). The Gramm-Leach-Bliley Act has safeguard provisions for financial institutions over which the Federal Trade Commission (FTC) has jurisdiction. These institutions must "[d]esignate an employee or employees to coordinate [its] information security program." 16 C.F.R. § 314.4(a) (2002). HIPAA requires "covered entities," which are predominately health plans, healthcare clearinghouses, and healthcare providers, to designate an individual as a "privacy official," who will be responsible for the implementation and development of the entity's privacy policies and procedures. 45 C.F.R § 164.530 (a)(1)(i).

90. *See* COLIN J. BENNETT & CHARLES D. RAAB, THE GOVERNANCE OF PRIVACY 203 (2003) ("[D]ata protection officers are rapidly becoming ubiquitous in private sector organizations' managerial structures . . . . ").

91. Interagency Guidance Establishing Information Security Standards, 69 Fed. Reg. 77,610, 77,621. (Dec. 28, 2004).

92. Alexander Pfaff and Chris Sanchirico have carefully documented grounds for similar concern in the context of self-auditing by companies pursuant to the Environmental Protection Agency's audit policy. Alexander Pfaff & Chris William Sanchirico, *Big Field, Small Potatoes: An Empirical Assessment of EPA's Self-Audit Policy*, 23 J. POL'Y ANALYSIS & MGMT. 415 (2004).

93. *See* Gunningham et al., *Motivating Management*, *supra* note 66, at 313.

apple learns that such sanctions will not occur, it may invest less in its reputation.[94]

Our previous comments about social sanctions have centered on the extent to which this force may have too little impact. Yet, there is another aspect to the influence of social sanctions on the reporting of data security breaches: fear of reputational harms may also have too great an impact. If a firm controls whether disclosure will occur, it has the ability *not* to share relevant information with the marketplace. No one likes to admit a mistake, and a company that suffers a data security breach may be hesitant to disclose information about this event. We have already traced economic reasons for this phenomenon, which we call the disclosure disincentive. In contrast, this Article will now consider three distinct concerns that drive this disincentive in the context of reputation.

First, other businesses may fear loss of customers and other opportunities if a breach is publicized and the responsible institution's reputation is harmed. As Beth Givens of the Privacy Rights Clearinghouse has predicted, an institution is likely to suffer a "negative backlash" following notification to customers that their data have been hacked.[95] Customers may vote with their feet (not to mention their checkbooks, ATM cards, and credit cards) and end their relationship with the entity.[96]

Second, due to leaked information's lack of provenance, a business might never be blamed for the leak for which it is responsible, and therefore might never bear a reputational cost from it. Third, and as a related matter, many organizations lack a B2C relationship with the persons whose data they lose or allow to be leaked. Some outsourcing entities and data brokers do not merely lack a direct relationship with the consumers whose data they handle; the consumers may not even know they exist. For these organizations, the disclosure disincentive is especially strong. In the absence of information about a data leak, these businesses would be able to continue operations with scant scrutiny.

In summary, reputational sanctions are likely to influence firm behavior in providing data security. But these influences can be quite complex. Bad apple companies will not be sensitive to social sanctions, and a wide range of other entities may prove resistant to social pressure, especially if sanctions are not fully imposed in any "reputational market."[97] Finally, reputational sanctions rely to a large extent on self-reporting of data security failures. This reliance in turn may create a disincentive for reporting.

---

94. Posner and Charny, for example, come to similar, mixed conclusions about the circulation of reputational information. Posner is agnostic about whether the circulation of reputational information will lead to more social cooperation. *See* POSNER, *supra* note 82, at 20–24. Charny generalizes that "some markets are better suited than others to enforce commitments by reputational sanctions." Charny, *supra* note 81, at 418.

95. Privacy Rights Clearinghouse, California Security Breach Notification Law Goes into Effect July 1, 2003, http://www.privacyrights.org/ar/SecurityBreach.htm (last visited Oct. 10, 2006).

96. PONEMON INST., *supra* note 18, at 2.

97. On the difficulty of regulating "bad apples," see Thornton et al., *supra* note 80, at 275–83.

* * *

In this Section, we have opened up the black box of firm behavior and discussed different factors that shape a given company's culture of compliance. Understanding these factors is important because of the lack of agreement as to the best legal model for informing the public about data security breaches.

II. THREE MODELS OF INFORMING ABOUT DATA SECURITY LEAKS

In this Part, we discuss three approaches to informing about data security leaks. The first two are based on existing legal standards: our first model ("Model One") is exemplified by the pathbreaking California disclosure statute, and our second model ("Model Two") reflects the Interagency Guidance promulgated by the federal agencies responsible for oversight of financial institutions. The final model is suggested by certain comments of the Chicago Federal Reserve Bank (Chicago FRB) in response to the Interagency Guidance.

This Article elaborates, modifies, and operationalizes these regulatory approaches. This Part examines each model along six dimensions. We look at the extent to which each respective regulation: (1) provides for sharing of reputational information about the breached entity; (2) delegates discretion to the regulated data processor, including how it should establish appropriate data security and notify consumers of breaches; (3) coordinates post-breach mitigation efforts; (4) permits delay to allow law enforcement investigation before consumer notification; (5) provides for damages and other enforcement rights; and, finally, (6) fosters an overall culture of compliance.

In all three models, disclosure of information is a central regulatory tool. As Sunstein observed in 1999, "informational strategies are displacing (and have significant advantages over) command-and-control approaches."[98] Sunstein also predicted that "informational regulation" would "become all the more central in the coming decade, when there will likely be a great deal of experimentation in this direction."[99] These three models demonstrate that much experimentation is already taking place regarding sharing information about data security breaches.

A. *The Three Models in a Nutshell*

The first model for regulating notice about security breaches centers on mandatory, particularized notice to customers of the breached entity. By particularized, we mean that the notification letter must identify the *source* of the breach and the *victim* of the breach, to whom the letter will be ad-

98. Sunstein, *supra* note 3, at 617.

99. *Id.* at 618.

dressed. Model One is exemplified by S.B. 1386, the California Security Breach statute.[100] It is marked by a low threshold for notification. It also lacks a coordination infrastructure to mitigate the harm flowing from a data security incident. In this sense, it should be thought of as a pure notification model.

Beyond the California statute and Model One, there is a second approach—our Model Two—that grants greater flexibility to businesses regarding the reporting of breaches to customers, but that also offers a more nuanced approach to data security practices within the firm and provides opportunity for coordinated mitigation efforts. As an embodiment of Model Two, we look to the consumer-notification provisions of a recently issued regulation promulgated by four federal agencies with oversight authority over financial institutions. These agencies issued the "Interagency Guidance on Response Programs" pursuant to their authority under Section 501 of the GLB Act.[101]

Rather than focusing solely on notice and reputational information, the Interagency Guidance imposes requirements on financial institutions that specify the manner in which they are to organize themselves to handle data. For example, each must designate an officer who will be accountable within the company for data security practices.[102] The Interagency Guidance also requires financial institutions to conduct risk assessments, implement reasonable data security procedures, and have incident-response programs in place to handle any security breaches.[103] With regard to notice, Model Two adopts a two-tier approach that contemplates distinct types of notice and notice thresholds. The first tier of notice concerns the financial institution's oversight agency, and, like the California statute, uses the relatively low threshold of "unauthorized access." The second tier of notice involves notification of the affected customers and requires action only after the relatively higher threshold of a "likelihood of misuse" is met.

Published comments by the Chicago FRB provide the inspiration for this Article's Model Three. The Chicago FRB offered its observations in response to publication of an early draft of the Interagency Guidance.[104] In its

---

100. CAL. CIV. CODE §§ 1798.28, .82, .84 (West Supp. 2006).

101. Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 Fed. Reg. 15,736 (Mar. 29, 2005); Gramm-Leach-Bliley Act § 501(b), 15 U.S.C. § 6801(b) (2000). While the California disclosure statute has a broad jurisdictional sweep and applies to any private business, CAL. CIV. CODE § 1798.82 (West Supp. 2006), the Interagency Guidance affects only "financial institutions" as defined by the GLB Act. Pursuant to the Federal Trade Commission's Privacy Rule, a financial institution is "any institution the business of which is engaging in financial activities as described in section 4(k) of the Bank Holding Company Act of 1956." 16 C.F.R. § 313.3(k)(1) (2006) (citation omitted).

102. Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 Fed. Reg. 15,736, 15,751 (Mar. 29, 2005).

103. *Id.*

104. Letter from Michael H. Moskow, President of the Fed. Reserve Bank of Chicago, to Jennifer J. Johnson, Sec'y of the Bd. of Governors of the Fed. Reserve Sys. (Oct. 10, 2003), *available at* http://www.chicagofed.org/bankwide_public_policy/files/programs_for_unauthorized_access_to_customer_information_and_notice.pdf (attaching response to Interagency Guidance).

comment paper, the Chicago FRB suggests that a third-party intermediary might be an appropriate entity with whom to share information about data breaches in certain circumstances. This intermediary, "a trusted, neutral third party," would forward information from the breached entity to other financial institutions in cases of massive data breaches and also help financial institutions coordinate the sharing of information with consumers.[105]

The trusted neutral party would facilitate a coordinated response to the security breach and also mitigate the disclosure disincentive. The Chicago FRB notes the likely reluctance to become a first-mover in breaking bad news to customers following an industry-wide data leak. It expresses this concern in these terms: "no affected institution wants to be the first to notify customers" subsequent to "a widespread compromise of customer information."[106] Moreover, industry competitors, such as Bank of America and Citibank, may be reluctant to share information about a data leak with each other. Ultimately, then, the Chicago FRB's trusted third party would step in to assist the financial entities in coordinating a "proactive, unified notification of affected customers."[107]

As noted, the Chicago FRB was commenting on the Interagency Guidance's two-track disclosure model. Its observations are limited, therefore, solely to financial institutions. We build, in turn, on the Chicago FRB's own proposal and posit a stand-alone "Anonymizing Disclosure Intermediary" (ADI) as this Article's Model Three. The Chicago FRB makes a somewhat delphic statement about financial institutions seeking to "leverage the ability" of a trusted, neutral third party "to facilitate anonymous information sharing" among the organizations.[108] It is from this brief suggestion that we elaborate a vision of a trusted third party, or ADI, which would notify consumers and other financial institutions of security breaches without revealing the identity of the breached party.

This third model highlights the fact that breach notification serves both an ex ante and an ex post function. We use this model to distinguish the prospective and retrospective functions of breach notices. Until now, this Article has described the reputational sanction that a breach notice causes as essentially forward-looking: it seeks to influence consumers to shop for data security based on information about security incidents and to encourage firms to safeguard their data to avoid reputational sanction. Mitigation looks backward; it seeks to minimize the harm caused by breaches that have already occurred. The focus here should be on preventing future harm, and in particular on generating coordinated responses to security breaches after they have occurred. The proposed ADI would forward information about a

105. *See id.* ("[W]e suggest that financial institutions develop a means to coordinate customer notification through a trusted, neutral third party such as the Financial and Banking Information Infrastructure Committee (FBIIC) or the Financial Services Information Sharing and Analysis Center (FS/ISAC).").

106. *Id.*

107. *Id.*

108. *Id.*

data breach to other financial institutions, and to affected consumers as well. It would share this information, however, without identifying the locus of the data breach. The open question is whether removing a reputational sanction through use of Model Three will significantly improve the law's ability to mitigate harm. Through a consideration of this third model, we weigh the benefits of reputational sanction against its costs in terms of harms to the flow of information. Similarly, consideration of this model permits us to focus on the other ways in which information about security breaches can limit future harm.

B. *Comparing the Models*

In this Section, we compare the three models along several axes: (1) the role of reputational information; (2) the location and supervision of decision-making authority; (3) the ability to coordinate efforts to mitigate harm; (4) the extent to which law enforcement delays impair the scheme; (5) the coordination of public and private remedial schemes; and (6) the extent to which the respective Model helps to create an overall culture of compliance.

1. *Reputational Information*

The central goal of Model One is to impose a reputational sanction. An initial difference between Model One and Model Two lies in their disclosure trigger, and reflects this central focus on reputation and in particular on sanctions. Under the California statute, disclosure follows upon a reasonable belief of unauthorized access to the consumer's personal information. Under the higher threshold of the Interagency Guidance, however, a business is to decide whether or not misuse will occur.[109] As the Interagency Guidance states: "[i]f the institution determines that misuse of its information about a customer has occurred or is reasonably possible, it should notify the affected customer as soon as possible."[110] As we shall see shortly, however, this requirement does not stand alone. Model Two also contains a second disclosure track for notification of regulators, which is similar to, and perhaps even more stringent than, Model One's lower trigger. In contrast, under the misuse trigger, there must be the likelihood of some other action by a fraudster, such as an opening of fraudulent accounts, before consumer notification. Model Two distinguishes security breaches where a reputation sanction is necessary from those where it is not.

More important, however, under Model One, notice is particularized. In other words, the institution that suffers the breach is obliged to reveal its identity to the consumer whose data was compromised and to acknowledge that it is the source of the breach.[111] This approach imposes a reputational

109. Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 Fed. Reg. 15,736, 15,752 (Mar. 29, 2005).

110. *Id.*

111. CAL. CIV. CODE § 1798.82(a) (West Supp. 2006).

sanction on the business. The statute's insight is that disclosure causes a useful embarrassment: to avoid notice and the accompanying reputational loss, a business will invest ex ante in data security and, ex post, will respond more effectively and vigorously to a breach due to increased public and regulatory scrutiny of its practices.

The California statute's focus on the reputational sanction is highlighted by its treatment of massive security breaches. Where notice to individuals is impractical, the statute still imposes a reputational sanction through so-called "substitute notice."[112] Substitute notice is allowed if providing particularized notice will cost more than $250,000, the affected class numbers more than 500,000 persons, and the breached entity lacks sufficient contact information.[113] Businesses have three obligations when providing substitute notice: (1) to give e-mail notice to customers where possible, (2) to post a notice of the breach on their web sites, and (3) to notify major statewide media.[114] These steps are calculated to insure a flood of publicity about any company that suffers a major security leak, but accomplish little more. Substitute notice does not identify the victims of the breach. Customers are unlikely to know that they are affected by this general news and are, therefore, unable to take steps to self-protect.

Similar to Model One, Model Two provides particularized notice to consumers. Model One and Model Two share the view that disclosing information about a data security failure will cause a useful embarrassment. Both Model One and Model Two rely on reputational pressures, and both must contend with the resulting disincentive to disclose a security breach.

Although both models rely on the disclosure of reputational information through particularized notice, an initial difference between the approaches is that Model Two's "misuse" threshold is likely to lead to fewer notification letters and less use of reputational sanction.[115] A second difference between the two approaches concerns the potential positive role of a firm's CPO under Model Two. Third, as noted above, the Interagency Guidance's two-track system allows a CPO who discovers an unauthorized use of data to report it to the relevant regulatory agency without fully confronting the issue of customer notification. The stakes are lower for this report than for breach notification to customers; for one thing, the oversight agency may decide, along with the breached entity, that unauthorized use is not likely and that consumer disclosure is unnecessary.

Models One and Two view the threat of consumer notification as central to inducing investment in data security. In contrast, Model Three gives a free ride to breached entities on this score: the ADI discloses the fact of the breach without identifying the locus of the leak. Particularized notification

---

112. *Id.* § 1798.82(g)(3).

113. *Id.*

114. *Id.*

115. The Interagency Guidance sets a higher disclosure trigger for notice to consumers. Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 Fed. Reg. 15,736, 15,752 (Mar. 29, 2005).

disseminates reputational information about the breached entity for ex ante purposes. It seeks to encourage investment by the company in reasonable data security practices and to permit consumers to choose companies based on information about their history of data security breaches. Notification about security breaches also serves ex post function of mitigation. It seeks to permit consumers and other data processing institutions to protect themselves from harm caused by a data spill that has already occurred.

Model Three turns on the insight that the threat of reputational sanction may serve to chill a company's willingness to inform about a security breach. This inhibiting effect may limit the ability of customers, other institutions, and regulators to reduce the harm flowing from the breach. Models One and Two grant considerable discretion to the information-processing organization. Yet to the extent that these two models use a reputational sanction, firms have an incentive to exercise this discretion regarding breach notification in a manner that may undercut the regulation's effectiveness. Model Three's ADI seeks to overcome this problem by freeing the breached entity from reputational harm.

There are important trade-offs when one chooses a notification regime that favors mitigation over reputational sanction. The key question here is the role of particularized notice. To what extent does the customer need to know the source of the breach? If the purpose of the notice is to impose a reputational sanction, then identifying the source of the breach is essential. If, however, the goal is to allow the customer to take steps to safeguard her data, knowing the location of the security breach is much less important. Whether the lack of reputational information matters in any significant fashion will turn on the availability of alternative means for encouraging firms to comply with appropriate data security practices, and the ability of customers to change their market behavior based on information about security practices.[116] In short, if the focus of regulation is mitigation, then very little may be lost by abandoning particularized notices, and much may be gained in terms of a firm's willingness to disclose. By contrast, if the focus is on reputational sanction, then identity is an indispensable element of the regulatory scheme.

2. *Delegation of Discretion*

The California statute's notification trigger is a standard. Recall that it turns on a breached entity's reasonable belief that there was unauthorized acquisition of personal data. This approach grants considerable discretion to the breached entity in its decision whether or not to notify the affected individual. Furthermore, it is possible for information to be lost without an unauthorized acquisition ever occurring. For example, in early December 2005, the international delivery company DHL lost a backup tape with

116. Customers do not currently shop for services based on a company's data security practices. *See infra* Section III.A. In addition, many of the steps that customers need to take after a breach, such as requesting a credit report, do not require knowledge of where their data was leaked. *See infra* Section III.B.

residential mortgage information that it was transporting for ABN-Amro Mortgage group.[117] The lost tape contained detailed account information, including SSNs, of approximately two million individuals.[118] After a month, DHL found the missing tape, to which no outside party had gained access.[119]

To be sure, any threshold for disclosure will provide at least some kind of inherent delegation; in particular, the unauthorized acquisition test permits leeway to the breached entity to decide how, when, and whether to conclude that data have been acquired. This level of discretion is, nonetheless, lower than under the "misuse" trigger, which we discuss in the next Section. The question under Model One is simply whether an unauthorized person has *acquired* notice-triggering information, not whether this person will go on to *misuse* it. Misuse requires the institution to conclude that further activity, such as the opening of fraudulent accounts, is likely. Thus, while the issue of acquisition may seem rule-like, it is, in fact, a standard. One is reminded of Duncan Kennedy's observation that an apparent rule may actually be "a covert standard."[120]

The reliance of the California statute on particularized notification has the important benefit of bringing breaches to light. But the focus on reputation may also have the unintended consequence of heightening the disclosure disincentive that this Article identified earlier. The disclosure disincentive may cause breached entities to err on the side of nondisclosure, and the net effect of the disincentive may hamper response to data leaks.

There are, however, similarities between Models One and Two. For one thing, the language of the Interagency Guidance, like that of the California statute, is primarily driven by standards and not rules. As an initial example, the Interagency Guidance suggests that "[a]t a minimum, an institution's response program should contain procedures for [a]ssessing the nature and scope of an incident . . . [and] taking appropriate steps to contain and control the incident to prevent further unauthorized access to or use of customer

---

117. Lucas Mearian, *Update: Missing ABN Amro tape with 2 million names found*, COMPUTERWORLD, Dec. 20, 2005, http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=107230.

118. *Id.*

119. *Id.*

120. Kennedy, *supra* note 32, at 1701. As we have observed, moreover, these and other recommendations of the California Office of Privacy Protection regarding breach notification are nonmandatory. And even these non-binding guidelines have further wiggle room built in, as the Office of Privacy Protection illustrates:

> Information-handling practices and technology are changing rapidly, and organizations should continuously review and update their own situation to ensure compliance with the laws and principles of privacy protection. It is recognized that specific or unique considerations, including compliance with other laws, may make some of these practices inappropriate for some organizations.

CALIFORNIA PRIVACY OFFICE, RECOMMENDATIONS, *supra* note 64, at 8. This wiggle room may become problematic because the statute necessarily relies on the breached entity to discover the breach, and then to subject itself to a reputational sanction.

information."[121] As for the primary standard in the Interagency Guidance, it is the "misuse" trigger for notification. The relevant language delegates broad discretion. Moreover, the standard sets a higher threshold for consumer notification than the California statute does. The preamble to the Interagency Guidance explains its tactic in these terms: "[T]he Agencies do not want customers of financial institutions to receive notices that would not be useful to them."[122]

This language regarding notices that are not "useful" alludes to two potential problems. First, notification might "needlessly alarm customers where little likelihood of harm exists."[123] Second, "frequent notices in non-threatening situations would be perceived by customers as routine and commonplace, and therefore reduce their effectiveness."[124] The two concerns are related—the approach of the regulators reflects a fear that too many notices where harm does not follow are the modern equivalent of the shepherd crying wolf.

As noted in the Introduction, Fred Cate, a critic of the California statute and similar legislation, argues that consumers, dulled by frequent cautions about harms that never materialize, will fail to act when important warnings finally arrive.[125] More generally, Cass Sunstein, in his work regarding information regulation, points to the danger of information overload.[126] Sunstein concludes that "[w]ith respect to information, less may be more."[127]

Like Model One, however, Model Two's heightened threshold for disclosure might provide a loophole for organizations already reluctant to share information about data breaches. Indeed, the discretion under Model Two's "misuse" standard is, if anything, greater than under Model One's "acquisition" standard. A finding of misuse requires a determination beyond acquisition, namely that the breached information will be used in fraudulent activities. The raised threshold permits additional discretion to the breached entity; this broader delegation, coupled with the existence of the disclosure disincentive, might bias the business's investigation of a data leak and lead to a facile conclusion that misuse of information was unlikely and consumer notification was not required.

---

121. Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 Fed. Reg. 15,736, 15,740 (Mar. 29, 2005). Even the lengthy, nonbinding preamble to the Interagency Guidance discusses institution action in the language of standards. *See, e.g., id.* at 15,741 ("[T]he Agencies contemplate that a financial institutional will notify regulators as quickly as possible . . . . "); *id.* at 15,742 ("[T]he Agencies believe that institutions should be mindful of industry standards when investigating an incident.").

122. *Id.* at 15,743.

123. *Id.*

124. *Id.*

125. Cate, *supra* note 9.

126. Sunstein, *supra* note 3, at 626–29.

127. *Id.* at 627–28. ("[C]onsumers . . . treat a large amount of information as equivalent to no information at all. Certainly this is true when disclosure campaigns are filled with details that cannot be processed easily." (footnote omitted)).

The Interagency Guidance provides an intriguing response to the notion that businesses might exploit the misuse standard: it creates a further disclosure obligation. The Interagency Guidance requires notification to a breached institution's oversight agency. And it sets a low threshold for sending this information to the agency, one similar to, and perhaps even stricter than, the California statute's standard for consumer notification. Pursuant to this second track, a breached entity must notify "its primary Federal regulator as soon as possible when the institution becomes aware of an incident involving unauthorized access to or use of [personal] information."[128] Note that this quoted language calls for a disclosure standard of mere "unauthorized access." This second track provides an "early warning," which is "to allow an institution's regulator to assess the effectiveness of an institution's response plan, and, where appropriate, to direct that notice be given to customers if the institution has not already done so."[129]

Through this two-track approach, the Interagency Guidance provides for a government overseer to review the financial institution's decision whether to disclose to individuals. It also gives the agency an opportunity to consider steps other than notice to mitigate the harm caused by the breach. But the Guidance provides no explanation as to when the agency should override the institution's decision not to disclose, or what other steps the agency might take. It also leaves open questions as to the form of any mandated notice.

Model Three's ADI seeks to use a carrot, rather than a stick, to overcome the danger that firms will exercise discretion in a way that undercuts the effectiveness of breach notification. By providing for anonymous disclosure, Model Three allows a firm to limit the harm caused by a breach—and hence any potential exposure—by notifying customers and other financial institutions. The firm thereby obtains the benefits of disclosure without suffering the costs.

3. *Coordination of Post-Breach Mitigation Efforts*

We have termed the California law a pure notification statute. This observation reflects both what the law does and what it does not do. The statute's emphasis is on disclosure, as exemplified by its comparatively low threshold for notification and also by the scant attention paid to coordination of post-breach mitigation efforts. Its attention is to the moment of notification, but not to what comes afterwards.

In its Sections 4 and 5, the California statute only requires that affected consumers be notified. It does not require placing information on a fraud list, notice to other institutions, or any other type of coordinated response. It

128. Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 Fed. Reg. 15,736, 15,752 (Mar. 29, 2005).

129. *Id.* at 15,741.

does not even require automatic notification of law enforcement officials.[130] The statute permits notification of these officials, however, and we turn now to this topic.

In contrast to Model One's pure notification approach, the Interagency Guidance seeks to coordinate post-breach mitigation efforts. One way that it does so is by a two-track system for notification. The creation of an intermediate form of disclosure may limit the extent to which breached entities can manipulate the "misuse" standard for consumer notification. While this delegation is broader than Model One's pure notification standard, it does not result in a complete lack of supervision.

Under this model, the oversight agency becomes aware of the breach at the financial institution and may be able to scrutinize the institution's decision whether or not to disclose to customers. Moreover, the sharing of information with an agency sets up a formal mechanism for an information flow back to an external, independent third party—one able to generate information about past breaches and whether or not certain kinds of acquisitions lead to misuse. As Dorf states regarding his model of rolling regulation, government entities can disseminate key information "about what works and what does not . . . back to the regulated entities so that they may learn from each other's successes and failures."[131]

As for Model Three, the Chicago FRB's comment reflects a hope that an intermediary can provide a degree of coordinated response beyond mere notification of customers. The focus of Model One is solely on giving notice to customers. Such notice has many benefits, but it may actually do less to protect against harm than if the breached entity were to inform an intermediary. The intermediary could, in turn, disclose to other financial institutions and related entities, such as institutions involved in clearing charges on credit and payment cards. The key difference is that, under Model Three, information flows from the intermediary to other institutions and customers, rather than from the breached entity to other institutions and customers.

The intermediary might serve as a clearinghouse for information about usurped identities. If an organization were to disclose a breach to an ADI, this entity also would receive information about the identity of the consumers whose information was leaked.[132] The ADI could then serve two anonymizing functions. With regard to other financial institutions, the identity of the consumer could be shared in the form of a fraud watch list.[133] The other institutions would not be informed about the source of the breach.

---

130. *See* CAL. CIV. CODE § 1798.82 (West Supp. 2006). Here, the statute encourages such action by permitting a delay in notification of affected individuals when necessary to facilitate the investigations of law enforcement officials.

131. Dorf, *supra* note 73, at 398–99.

132. A flaw in Model Three, however, is that this new entity, the ADI, might be the target of hackers. For this reason, we advocate a policy of data minimalization in our Model Four's coordinating response architecture. *Infra* Section IV.A.

133. Such lists would raise privacy concerns, however, and concerns about additional data security breaches. Later in this Article, we suggest a strategy of data minimalization in response to such concerns. *Infra* Section IV.A.

Similarly, customers would be notified that their information was compromised; the consumers could then request credit reports and examine their own account statements with added care.

4. *Delay to Allow Investigation*

One of the California statute's findings of fact concerns the importance of "expeditious notification" to identity theft victims.[134] The statute's judgment on this score is bolstered by empirical findings that demonstrate the benefits of rapid detection of identity theft.[135] The longer an instance of identity theft goes undetected, the greater the damage that usually follows.[136]

Despite the value of rapid notification, the California law allows a delay in reporting data leaks "if a law enforcement agency determines that the notification will impede a criminal investigation."[137] The policy judgment behind this aspect of the California statute considers two interests: (1) the individual benefit from rapid disclosure of a data leak; and (2) the public benefit from the arrest of criminals who hacked or otherwise obtained personal information. By permitting a law enforcement delay, the California statute favors the general public interest in apprehending the criminal when it conflicts with immediate notification, and, hence, protection for the individuals whose data were stolen. This choice is a sensible one.

Unfortunately, the law enforcement delay can allow a further opportunity for business foot dragging regarding disclosure of information about a data breach. As an example, a Los Angeles police task force accused ChoicePoint of delay in making the disclosure to the affected public once the police cleared it to share information with consumers.[138] In short, while the availability of the law enforcement delay may encourage breached entities to notify law enforcement officials, this regulatory choice hardly constitutes a coordinated effort to mitigate the harm caused by the data spill and may even prove an obstacle to such coordinated response.[139]

According to the Interagency Guidance, which forms the basis for this Article's Model Two, the breached institution is to file a "Suspicious Activity Report" (SAR) with "appropriate law enforcement authorities" pursuant to existing federal regulations regarding financial fraud.[140] This requirement of law enforcement notification is tied to the same kind of delay mechanism

---

134. 2002 Cal. Stat., ch. 915, § 1.

135. SYNOVATE, FEDERAL TRADE COMMISSION—IDENTITY THEFT SURVEY REPORT 8 (2003), http://www.ftc.gov/os/2003/09/synovatereport.pdf.

136. *Id.*

137. CAL. CIV. CODE, § 1798.82(c) (West Supp. 2006). Notification proceeds only once the law enforcement entity determines that disclosure "will not compromise the investigation." *Id.*

138. Tom Zeller Jr., *Release of Consumers' Data Spurs ChoicePoint Inquiries*, N.Y. TIMES, Mar. 5, 2005, at C2.

139. For a discussion of how other methods of responding to security breaches might mitigate the harm caused by this delay, see Section IV.B of this Article.

140. Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 Fed. Reg. 15,736, 15,752 (Mar. 29, 2005).

as in the California statute. The applicable language in the Interagency Guidance permits customer notification to be postponed "if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation and provides the institution with a written request for the delay."[141] The risk, as under Model One, is that the delay for law enforcement activity may cause harm to the consumer whose personal information has been leaked.[142]

As for Model Three, ideally, this Model can eliminate, or, at least reduce, the extent to which any law enforcement delay is necessary after a data leak. The ADI would generate anonymous notification messages that inform consumers that a leak has taken place, but withhold information regarding the locus of this event. As a result, notification under Model Three may be less likely to tip off a criminal hacker and compromise an ongoing investigation. Model Three might, therefore, allow law enforcement investigations to occur simultaneously with more information being shared with other data processing organizations and affected consumers.

5. *Damages and Other Enforcement Rights*

The California statute provides a private right of action for violations of its notification and reasonable data security provisions.[143] Violations of these provisions can also be enjoined.[144] Finally, the California law provides that the "rights and remedies available" under it "are cumulative to each other and to any other rights and remedies."[145] In addition to California, other states, such as Tennessee and Washington, provide private rights of action for violation of their notification statutes.[146]

Concerning Model Two, the Interagency Guidance does not provide for a private right of action. Power to enforce the Guidance itself is conferred solely on the financial institutions' primary federal regulator.[147] Thus, failure to comply with the Interagency Guidance does not create liability to customers.

As for Model Three, if a disclosure regime is focused on "anonymous" disclosure, private rights of action are problematic. The victims of identity theft may know that they are victims of a security breach, but they are unlikely to know where the breach occurred. For data processing entities, one of the attractions of the anonymous disclosure model would likely be

---

141. *Id.* The financial institution is to inform consumers "as soon as notification will no longer interfere with the investigation." *Id.*

142. *See* SYNOVATE, *supra* note 135, at 34.

143. CAL. CIV. CODE § 1798.84(b) (West Supp. 2006).

144. *Id.* § 1798.84(e).

145. *Id.* § 1798.84(g).

146. TENN. CODE ANN. § 47-18-2107(h) (West 2001); WASH. REV. CODE ANN. §§ 19.255.010(10)(a) (West Supp. 2006); *Id.* § 42.17.31922(10)(a) (West 1999).

147. Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 Fed. Reg. 15,736, 15,753 (Mar. 29, 2005).

the lack of individual enforcement. The lack of individual legal actions would follow either because the third regime did not provide a private right of action, or, as a practical matter, because the data leak victim did not know where the breach occurred.

Yet if the intermediary shields the financial institution from liability, the law must carefully craft an incentive for the breached entity to share information with the ADI about data breaches.[148] Failure to disclose a breach to the ADI might give rise to statutory damages, while if a breached entity discloses to the ADI, it might have its damages capped at a particular level, or shielded from class action liability. Conceptually, liability for failure to disclose to the ADI might be termed a failure to mitigate. As such, a failure to disclose to the ADI might be made subject to full compensatory or statutory damages, possible punitive damages, and attorney fee shifting.[149]

6. *The Culture of Compliance*

The California statute makes the kinds of delegations to private actors that are frequently found in the modern regulatory landscape. Yet it suffers from a number of shortcomings. As a delegated regulation, it falls short of the kind of "rolling regulatory regime" that Dorf proposes. In particular, there is no structure in place for regulators to draw on information from regulated entities about local experimentalism. Regulated entities will develop their data security practices and, over time, refine the scope of the "reasonable data security" obligation, but, under the current regime, the regulators—and by extension the rest of the industry—have no means of benefiting from this experience. There is also no mechanism for using new information, based on this experience, to shape and give content to the notification triggers of "reasonable data security" or "unauthorized access." Moreover, due to the disclosure disincentive, economic pressures may cause breached entities to be hesitant to notify customers or even to investigate breaches that may give rise to an obligation to give notice.

Model One also seeks to draw on reputational sanctions through its requirement for particularized notice. Yet the effectiveness of such sanctions depends on a well-functioning consumer-side market for data security. As we discuss in this Article, there are shortcomings at present in the ability of

---

148. Payment law already contains a carefully calibrated allocation of risk for unauthorized use of checks or credit cards. Generally, the risk of forged checks lies with the account holder's bank. U.C.C § 4-401 (1999); *id.* cmt. 1. For stolen checks with forged endorsements, risk of loss falls on the first solvent party to trust the forger (usually the depositary bank). *Id.* §§ 4-207, 4-208. For credit cards and debit cards, the Truth in Lending Act as well as the Electronic Funds Transfer Act generally places the risk of unauthorized use, at least in the first instance, on the issuing bank. 15 U.S.C. §§ 1643(a), 1693g (2000).

149. One example of such an approach, in an analogous context, is the Fair Credit Reporting Act. 15 U.S.C §§ 1681–1681u (2000). Where a credit bureau fails to comply with the requirements of the Act, the agency is held liable for actual damages, and where the noncompliance is willful, there is a statutory minimum of $100 per violation in damages. *Id.* § 1681n(a)(1)(A). In order to encourage attorneys to take such cases, a victorious party may also be entitled to have their attorneys' fees paid. *Id.* §§ 1681n(c), 1681o(b).

an individual to shop for services from information-processing companies according to their data security practices.[150]

Like the California statute, the Interagency Guidance delegates authority to private actors through use of a standard. Yet by requiring disclosure to oversight agencies, regulators may be able to draw on information from regulated entities and affect decision-making about "reasonable data security" and the conditions under which "access" or "misuse" are likely to occur. Economic pressures may also contribute to a breached entity's desire not to disclose information about a breach. The Interagency Guidance also sets up a different kind of information flow to the public; whereas information about a breach is shared with a regulator once a low threshold is met, this knowledge stays with the agency unless a higher threshold is reached. This result is notable, and there is potential for a positive impact on the disclosure disincentive. We return to and develop this point further in Part IV.

Regarding reputational pressures, Models One and Two both require particularized notice to the individual whose information is leaked. While there may be resistance within the firm to providing this notice, due to the disclosure disincentive, CPOs may also emerge as advocates for full investigation and consumer notification. Model Two may strengthen the hand of the CPO within the firm, moreover, by giving her a formal role to play in providing notification to oversight agencies. The importance of a responsible corporate officer in fostering a culture of compliance has received a surprising yet instructive demonstration through an unintentional aspect of the Sarbanes-Oxley Act, which we mentioned earlier in this Article. The Act's requirement regarding adequate internal legal controls on corporate data has led to the development of security standards and heightened internal corporate attention to issues regarding data security.[151]

Model Three has a different mix of promise and peril than the other approaches. The ADI would interact with a firm once a breach took place, and would itself take on the role of contacting the individual whose information was lost. By removing any reputational harm from the breached entity, it would presumably reduce the unwillingness of the firm to share information about the security event—whether with the ADI or with the public. Recourse to an ADI would remove any reputational sanction on the breached institution, and might also improve the ability of the breached institution, affected consumer, and other parties to mitigate the harms flowing from a data leak. Indeed, the ADI as information intermediary might serve as a clearinghouse for usurped identities and seek in other ways to coordinate responses to data security breaches. Another positive impact of Model Three would be to reduce the need for any law enforcement delay. A possible weakness of Model Three, however, is that a lack of individual enforcement rights and information about breaches might permit breached entities to skirt any information sharing obligations towards the ADI.

---

150. *See infra* Section III.A.

151. *See, e.g.*, Winters, *supra* note 59.

III. Defining Ideal Behavior for the Consumer and the Data Processor

In the previous Part, this Article set out three models for consumer notification. These models differ in important ways. However, all three approaches aim to influence the same two entities: the consumer whose information is processed, and the business entity that processes information. Models Two and Three also consider a third set of entities—the other institutions that might be affected by a data leak. In this Part, we describe the nature of the sought-after behavior by positing an ideal consumer and ideal data processor. We also analyze the extent to which breach notification is likely to induce this behavior.

A. *The Ideal Consumer and Reputational Information: Shopping for Data Security*

Put simply, the ideal consumer is expected to shop for data security. Moreover, this behavior is expected to occur both before and after a breach. Here is the rosy scenario: if one firm has a bad reputation for data security, the ideal consumer will shun it and patronize another company. Moreover, should a data leak occur, the consumer will receive valuable reputational information through the notification letter. The ideal consumer will again take action by fleeing the offending company and rewarding a company with a reputation for good security practices by switching her business to it.[152]

This story embodies various assumptions about consumer behavior upon notification that we believe are inaccurate or, at least, excessively sanguine. Under current market conditions and notification practices, consumer shopping for data security will at best be erratic.[153] In our judgment, there are, nonetheless, real merits to customer notification, but they are indirect and generally not linked to the affected consumer. In this Section, we explore why consumers have not drawn on the reputational information in breach disclosure letters to apply direct sanctions to breached companies.

1. *Lack of B2C Relationship*

One set of difficulties with consumer shopping for data security follows from the frequent lack of any B2C relationship between the individual whose data are stolen and the entities that play a major role in processing her information. As a result of the lack of a direct relationship, a consumer cannot fire CardSystems, an outsourcing entity that processes payments; UPS or DHL, outsourcing entities that transport data; Iron Mountain Stor-

152. The ideal consumer would also take a number of self-protective steps, but we reserve discussion of this behavior for this Part's next Section. *See infra* Section III.B.

153. For an argument about the difficulties in shopping for information privacy under current market conditions, see Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 Harv. L. Rev. 2055, 2076–84 (2004).

age, an outsourcing entity that stores data; or ChoicePoint, a data broker. It is also unlikely that the consumer will be able to switch accounts successfully in order to avoid any indirect relationship with these entities.[154] Financial institutions and other kinds of businesses do not advertise the extent to which they contract data processing functions to other entities.

2. *Consumer-Side Shortcomings and Fuzzy Notification Letters*

Even when a B2C relationship exists, as with a credit card company or a bank, additional problems arise regarding the ability of consumers to shop for data security. First, a consumer may face considerable switching costs associated with changing his banking and credit relationships. While it is easy enough to cancel a credit card, or apply for another one, it is much more difficult to move one's bank accounts from one institution to another. Consumers often have relatively entrenched relationships with a principal bank. They may have depositary accounts, a mortgage, an investment account, uniform transfer to minors accounts, an online payment system, and so on, all accumulated over a period of banking at a specific institution. One letter about a security incident may not cause such an individual to sever this banking relationship, even if it is feasible.

Second, a consumer generally has good information about price (such as the cost of a checking account), but bad information about non-price terms (such as the full range of investment by a company in data security and whether such investment is likely to be effective). Even if somehow supplied with complete information about how a company manages data security, the average consumer—indeed, anyone who is not an information security professional—would be hard pressed to make sense of it.[155]

Notification letters are not likely to alter this situation. Notification letters supply only incomplete, discontinuous, and non-comparative information about data security. To use Eric Posner's terminology, a pooling equilibrium exists around notification letters.[156] Under the circumstances of a pooling equilibrium, good and bad types alike engage in the same behavior and send the same signal.[157] Breach notification obliges companies to send a negative signal, but the resulting letters provide only a fuzzy signal about future behavior and the likelihood of additional data security breaches. These missives are required to inform a consumer that her personal data have been leaked, and the name of the breached entity (at least under Models One and Two). This information provides neither background as to how the company has fared in the past nor comparative data to permit

---

154. *See generally* Zeller, *supra* note 20 (noting that it is a common practice for businesses to outsource data delivery to independent couriers such as UPS).

155. To make matters difficult, even for an IT professional, security updates and fixes are required on a continuous basis, so evaluation of a company's practices must likewise be made on a continuous basis. SMITH & KOMAR, *supra* note 83, at 12.

156. For a description of how signals can "pool," see POSNER, *supra* note 82, at 19–20.

157. *Id.* at 19–21.

evaluations across companies or industries. Moreover, the letters do not point to any way to impose reputational costs on any third party that might be involved in the breach.

To be sure, some companies now advertise their concern for data security. Here, another kind of fuzzy, if not outright misleading, signal can be sent. As a notable example, a journalist explained that Visa "already had a response ready" for public concerns once it discovered its credit cards were implicated in the CardSystems breach.[158] Visa responded with a media blitz: "[i]t simply increased the frequency of existing spots, like those featuring fraud-fighting superheroes and a fireman clad in layers of protective gear."[159] To its credit, Visa also investigated and then severed its ties with CardSystems—a fact that, perhaps paradoxically, it does not advertise.[160] As a further example of the limits of advertising, Citibank is touting its attention to identity theft in print and television advertisements. Yet, one of Citibank's major subsidiaries, CitiFinancial, recently suffered a significant data breach.[161] In response, Citigroup "put back into rotation several ads for its identity theft services."[162]

Upon notification, a Visa customer would be hard-pressed to decide whether to switch to MasterCard, which also advertises about its data security, and which was also implicated in the CardSystems breach.[163] A Citibank customer would be in a similar quandary regarding whether better data security awaits her at another financial institution, such as Bank of America, Wachovia, or Wells Fargo. Indeed, the well-informed consumer would know that all these banks suffered major data breaches in a single year.[164] Under these conditions, a consumer might be reluctant to incur the switching costs involved in terminating a bank account or credit card. Why go to all this effort if there is a good chance at ending up no better off?

Consumers, therefore, face information imperfections, cognitive limitations (how well will any lay person evaluate data security?), information costs, switching costs (assuming that an alternative is available) and other transaction costs. To foreshadow a final point, the notification letter itself frequently comes in a form that may lead the consumer to discard the letter without even opening it. We expand on this idea below under the concept of "envelope triviality."

---

158. Eric Dash, *Advertising: From Data Holders, Lots of Reassurance*, N.Y. TIMES, July 18, 2005, at C6.

159. *Id.*

160. Eric Dash, *A Matter of (Fading) Trust: Banishing One Payment Processor Was Just the Start for Visa*, N.Y. TIMES, Aug. 25, 2005, at C1.

161. *Citi notifies 3.9 million customers of lost data*, MSNBC.COM, June 7, 2005, http://www.msnbc.msn.com/id/8119720/; *see* Associated Press, *Bank data theft could hit more than 700,000*, MSNBC.COM, May 23, 2005, http://www.msnbc.msn.com/id/7954620; *US bank 'loses' customer details*, BBC NEWS, Feb. 26, 2005, http://news.bbc.co.uk/2/hi/business/4300371.stm.

162. Dash, *supra* note 158; *see also* Liz Moyer, *Citi Whacked Again*, FORBES.COM, June 6, 2005, http://www.forbes.com/services/2005/06/06/cx_lm_0606citi.html.

163. Dash, *supra* note 158.

164. *See supra* Section I.A.

B. *The Ideal Consumer and Mitigation: From Self-Protection to Automatic Protection*

This Article now considers how an ideal consumer should act to avoid harm from a breach that has already occurred. The California Office of Privacy Protection explains the protective goal of the California statute in these terms: the law is "intended to give individuals early warning when their personal information has fallen into the hands of an unauthorized person, so that they can take steps to protect themselves against identity theft or to mitigate the crime's impact."[165] This early warning function is, however, largely ineffective at present.

1. *The Shared Recommendations*

What are the steps, according to current wisdom, that the consumer is to take upon notification of an information leak? The FTC, the California Office of Privacy Protection, the Privacy Rights Clearinghouse, Consumer Reports, and various self-help guides (including *Preventing Identity Theft for Dummies*) have independently made a similar set of recommendations of best practices upon notification.[166]

The list of recommendations for the consumer upon notification turns out to be short:

- Carefully monitor all accounts for suspicious activity;
- Request free credit reports from the three main credit-reporting agencies;
- Place a fraud alert on one's credit file; and
- Contact the FTC to put a complaint into its ID Theft database.[167]

This information can be conveyed clearly and concisely, and it will be highly salient because it accompanies news regarding a leak of one's personal information. If breach notification letters clearly conveyed these recommendations and consumers trusted these letters, these missives would have a highly positive effect. Next, we must consider whether the notice needs to be particularized as well as the best practices for consumers independent of a data leak.

---

165. CALIFORNIA PRIVACY OFFICE, RECOMMENDATIONS, *supra* note 64, at 5.

166. For the key sources, see MICHAEL J. ARATA, JR., PREVENTING IDENTITY THEFT FOR DUMMIES (2004); CALIFORNIA PRIVACY OFFICE, RECOMMENDATIONS, *supra* note 64; FTC, TAKE CHARGE: FIGHTING BACK AGAINST IDENTITY THEFT (2005); and ROBERT HAMMOND, IDENTITY THEFT: HOW TO PROTECT YOUR MOST VALUABLE ASSET (2003).

167. ARATA, *supra* note 166, at 153–63; CALIFORNIA PRIVACY OFFICE, RECOMMENDATIONS, *supra* note 64, app. 2 at 19; FTC, *supra* note 166, at 4–9; HAMMOND, *supra* note 166, at 97–108.

2. *Particularized Notice*

The initial list of recommendations requires consumer notification, but, at least generally, does not require knowledge of where a data breach took place. A large set of notification-triggering personal information simply involves name, date of birth, address, SSN, and other information that can lead to identity theft. Knowledge of where this information was leaked may not help the consumer protect herself. The consumer can monitor personal accounts, request a credit report, place a fraud alert on her credit file, and contact the FTC without specifically knowing it was her MasterCard as opposed to a Visa account that was hacked. Moreover, in breaches where no B2C relationship exists, as was the case with ChoicePoint or CardSystems, the consumer cannot pay extra scrutiny to or cancel any personal account. Thus, this list seems, at least initially, to be consistent with use of Model Three's ADI, which notifies consumers without sharing information about the locus of a breach.

A significant limitation exists, however, on the ADI. Consumers, upon receiving notice, will make certain guesses about where the breach occurred. These guesses will, in many instances, be wrong. As we pointed out above, many of the entities that have been subject to data spills do not have direct relationships with consumers. These shadow entities, including the firms that provide back-office services, may suffer breaches, but a customer may not even know that these companies exist. To give another example, a consumer with only one credit card is likely to assume that the breach occurred at the issuing bank. The data leak may have actually occurred at the entity that processed the credit card, or the online merchant where the individual purchased goods.

In addition to this concern about false positives, consumers will have a strong proprietary sense regarding their personal information. They will want to know about leaks of their personal data and oppose the creation of an ADI. As a political matter, such opposition is likely to doom creation of any anonymized disclosure organization.[168]

3. *Best Practices Independent of Notification*

Finally, we must determine the best practices for consumers even when there has been no data leak and notification letter. More generally, the organizations and self-help guides listed above make similar recommendations regarding good housekeeping practices for consumers. The core list here, once again, is short:

- Shred correspondence that is no longer needed and contains financial information and key identifiers (name, address, SSN, and other identifiers);

---

168. A further reason for doubts about an ADI is the "private-to-public-information" argument. *See infra* Section III.C.

- Keep documents with identifying information in a secure location;
- Opt out of pre-certification of credit card offers;
- Opt out whenever possible of data sharing by one company with another.[169]

Ideally, a breach notification letter should also inform consumers of these good housekeeping practices.

It is also worth considering the last two recommendations from the list. Under current law, many kinds of information sharing take place unless a consumer "opts out," that is, indicates a preference *not* to have her information shared.[170] The benefit of opting out is to reduce the amount of one's personal information that is in circulation. The result should be at least some reduction in the risk of identity fraud.

It is particularly important that lawmakers reform the current practice of requiring consumers to opt out of credit card pre-certification offers. Pre-certification currently leads to the mailing of millions of credit card offers.[171] The circulation of these offers creates a target rich environment for identity thieves who steal mail or search garbage for unshredded personal information. The latter activity is known as "dumpster diving."[172] The Fair Credit Reporting Act permits credit bureaus to share information about individuals with credit-issuing entities unless the targeted consumer has opted out.[173] This law should be amended to block credit bureaus from sharing information for pre-certification unless a consumer has agreed to this practice, or "opted in."

4. *Fuzzy Notification Letters Redux*

In the previous section, we examined a set of problems that consumers face in shopping for data security with information from breach-disclosure letters. These shortcomings concerned both how consumers are ill-equipped to negotiate for data security and how notification letters at their best currently provide only incomplete, discontinuous, and non-comparative information about data security.

There are also significant problems that arise from the process of conveying information within the notification letters themselves. First, in assigning the task of sending disclosure letters to commercial entities, the

---

169. ARATA, *supra* note 166, at 39, 50, 100; FTC, *supra* note 166, at 12–18; HAMMOND, *supra* note 166, at 73–84; California Office of Privacy Protection, Top 10 Tips for Identity Theft Prevention, http://www.privacy.ca.gov/sheets/cis1english.htm (last visited Oct. 10, 2006).

170. *E.g.*, Gramm-Leach-Bliley Act § 2(b), 15 U.S.C. § 6802(b) (2000) (preventing financial institutions from sharing information with non-affiliated entities).

171. *See* BOB SULLIVAN, YOUR EVIL TWIN 75 (2004) (arguing that pre-certified credit applications are "an identity thief's best friend.").

172. ARATA, *supra* note 166, at 8.

173. 15 U.S.C. § 1681b(e) (2000).

law inadvertently creates a new way for identity thieves to harm consumers. Breach notification letters provide a new ground for "phishing." This term refers to the sending of a message that falsely claims to be from an established legitimate enterprise in order to trick an individual into surrendering private information that can be used for identity theft.[174] Phishing attacks already occur via e-mails that inform recipients of account breaches.[175]

Second, notification letters may seem insignificant because they are indistinguishable from junk mail. We call this problem, "envelope triviality." After receiving a notification letter from ChoicePoint, for example, one consumer reported that he almost threw the letter out unopened because he "thought it was going to be a credit card solicitation or a reduced rate mortgage scam."[176] The Ponemon Institute's survey on data breach notification found that over thirty-nine percent of respondents thought their breach notice "was junk mail, spam or a telemarketing phone call."[177] Americans are so inundated by various forms of junk mail that envelope triviality is a permanent condition. What good is a notice if the envelope is never opened? Note as well that the debate about whether letters should be sent under an "unauthorized access" or "misuse" trigger does not address this problem.

Finally, notification letters frequently have problematic content. The initial difficulty can be thought of as "content triviality," which is closely related to envelope triviality. Just as we may discard a letter from a commercial entity without reading it, once the letter is open, its content may confuse us or bore us, rather than compel us to act. Indeed, ChoicePoint's notification letters adopted a tone that suggested that the data spill in question was not a big deal.[178] More generally, the Ponemon Institute survey found that "[a] majority of respondents [were] not satisfied with the quality of the notification and communication process."[179] Complaints included difficulties in understanding the notice, a lack of adequate details in it, and continuing confusion about "the facts of the incident even after receiving notification of the breach."[180]

A further difficulty is that notification letters can contain recommendations for self-protection that are phrased in passive, almost nonchalant terms.[181] Current letters focus more on damage control for the breached en-

---

174. ARATA, *supra* note 166, at 118–19, 169–71.

175. *See id.* at 118–19.

176. Bob Sullivan, *Data theft affects 145,000 nationwide*, MSNBC.COM, Feb. 18, 2005, http://www.msnbc.msn.com/id/6979897/ (quoting anonymous e-mail to MSNBC.com).

177. PONEMON INST., *supra* note 18, at 3.

178. *See* Letter from J. Michael de Janes, Chief Privacy Officer, ChoicePoint (Feb. 9, 2005), *available at* http://www.epic.org/privacy/choicepoint/cp_letter_020905.pdf; Letter from J. Michael de Janes, Chief Privacy Officer, ChoicePoint (Feb. 25, 2005), *available at* http://www.epic.org/privacy/choicepoint/cp_letter_022505.pdf [hereinafter Second ChoicePoint Letter].

179. PONEMON INST., *supra* note 18, at 3.

180. *Id.*

181. *See, e.g.*, Second ChoicePoint Letter, *supra* note 178 ("You may request one free report containing information from all three national credit reporting companies.").

tity rather than convincing consumers to take appropriate steps. A better notice would clearly state the action that consumers are to carry out and use bullet points or other ways to convey the urgency of the requirement.

Receiving letters from a commercial entity, whether CardSystems, ChoicePoint, or Citibank, may also raise consumer suspicions as to whether another attempt is being made at a sales pitch—a suspicion that is not unfounded. Some companies are making commercial solicitations in disclosure letters and attaching hidden strings to some "free" offers.[182] As an initial example, ChoicePoint has offered to sell consumers access to some of their compromised information.[183] Other companies, such as Wells Fargo and Washington Mutual, are charging a whopping $155.88 and $120 a year respectively for credit monitoring and identity theft insurance.[184] Given that the maximum liability for unauthorized use of a credit card is $50,[185] and that the practices of these companies play a role in permitting data breaches, one wonders whether there are any limits to shamelessness (or chutzpah). We also note that less incentive will exist for companies to improve data security if data leaks become a new profit center for them.[186] Notification letters are problematic, therefore, in the current context in which they are being used.

C. *The Ideal Data Processor: Private-to-Public Information and the Improvement of Organizational Practices*

Just as the ideal consumer is expected to engage in certain kinds of behavior regarding data security, the ideal data processing entity is expected to take certain actions. Emerging legal authority, including statutes and regulations, already points to a favored approach.[187] As we have described, applicable laws and regulations require businesses to utilize reasonable data security procedures that are expressed in an enterprise-wide plan. We now summarize the most important legal requirements in this area and then discuss how particularized breach notices can have a positive impact on the data-handling practices of organizations.

---

182. Joseph Menn, *Firms Hit by ID Theft Find Way to Cash In on Victims*, L.A. TIMES, Aug. 22, 2005, at A1.

183. *Id.*

184. *Id.*

185. 15 U.S.C. § 1643(a)(1) (2000).

186. This point was also made by one identity theft victim: "They're cashing in on this, so there's no incentive to make it go away." Menn, *supra* note 182 (quoting attorney Mari Frank). For a detailed account of how credit bureaus are now deriving "a fast-growing revenue stream" from selling consumer information to consumers, see Christopher Conkey, *Extreme Makeover*, WALL ST. J., Mar. 15, 2006, at B1.

187. *See* 12 C.F.R. pt. 30, app. B (2006) (Office of the Comptroller of the Currency regulations for financial industry security issued by regulatory agencies pursuant to the GLB Act); HIPAA Security and Privacy, 45 C.F.R. pt. 164 (2005) (regulations for data security for "covered entities" under HIPAA); Guidelines Establishing Standards for Safeguarding Customer Information, 66 Fed. Reg. 8816 (Feb. 1, 2001) (to be codified at 12 C.F.R. pt. 30).

1. *Notification and Reasonable Data Security*

Companies ultimately are to use "any security measure" reasonably designed to achieve reasonable data security.[188] This standard is also supplemented with rules. Under a reasonable program for data security, a business that processes personal information might:

- Conduct periodic risk assessments;
- Develop a data security program to manage and control these risks;
- Assign one person at the company the responsibility for the security program;
- Apply sanctions against employees that fail to comply with the security program;
- Implement procedures to review records of information security activity and monitor the security program for effectiveness;
- Engage in regular audits;
- Establish a password program for employees;
- Respond promptly to any unauthorized access to information;
- Reassess and modify the data security program in light of any data breaches as well as any changes in overall risk.[189]

These rules are expressed through guidelines in certain sectors and have also been imposed on certain companies as part of FTC enforcement actions.

The law is placing more companies under an obligation to develop and maintain reasonable data security procedures. What is the role of notification under this approach? As we have seen in this Article's discussion of consumer behavior, evidence suggests that consumers are not likely to be effective in shopping for data security, or, as notification letters are currently constituted, engaging in post-breach self-protection. Nevertheless, notification has encouraged a flurry of positive indirect effects, including legislative activity, intense media scrutiny, and new requirements for notification and data security.[190] Some companies have also improved their practices and policies.[191]

---

188. As Bruce Schneier states, data security is to be viewed as "a process, not a product." BRUCE SCHNEIER, SECRETS & LIES: DIGITAL SECURITY IN A NETWORKED WORLD xii (2000).

189. *E.g.*, HIPAA Security Standards, 45 C.F.R. pt. 164.

190. For discussion of the intense public interest in the topic, see Krebs, *supra* note 7.

191. *See, e.g.*, Moyer, *supra* note 162 (noting that CitiFinancial is now encrypting data that it had previous sent unencrypted with courier services, such as UPS); CALIFORNIA PRIVACY OFFICE, RECOMMENDATIONS, *supra* note 64, app. 6 (reporting the results of a study by Dr. Larry Ponemon in which one-third of the corporate respondents reported changes in intrusion detection systems, encryption technologies, and the perimeter control process in response to California breach notification statute).

Thus, notification letters have already made a difference. But why have the letters led to these positive changes? Developing an understanding of how notification affects a data processor's behavior is important, moreover, because it can point to ways to improve the process of notification and ameliorate data security. In our judgment, breach notification letters have two important roles. One of these functions takes place outside the breached firm, and one takes place inside it. The letters can transform information about firm practices into publicly-known information as well as alter practices within an organization.

2. *Private-to-Public Information*

A notification letter contains information about the occurrence of a breach, its specific dimensions, and even the existence of hitherto unknown data processing businesses, such as data brokers.[192] Particularized notice allows consumers, the media, and legislators to hear a story about data security gone awry. Forced to convey a certain kind of particularized bad news, the breached entity becomes a focal point for consumer resentment, media attention, and legislative scrutiny.

In short, breach notification letters transform private-sector information usually kept confidential into public information. Other areas of law have also adopted this technique.[193] Breach notification is a specific example, moreover, of "regulation through disclosure," which Sunstein has termed "one of the most striking developments in the last generation of American law."[194] Despite information regulation in other areas, companies had kept tight control of information about data security failures and other risk events until enactment of the California breach notification law. As a specific example, ChoicePoint had suffered an earlier breach that pre-dated the California obligation to notify affected consumers.[195] In the absence of a legal duty to inform, however, the company kept public knowledge of the incident to a minimum.[196] As our previous discussion of the disclosure disincentive demonstrates, moreover, these entities have a powerful interest in keeping this information as secret as possible.[197]

Fortunately, notification letters have altered this situation and have created a new stock of public information. This public knowledge is highly salient. Consumers have a strong proprietary sense regarding their personal

192. *See* Robert Cooter, *Innovation, Information, and the Poverty of Nations*, 33 FLA. ST. U. L. REV. 373 (2006) (explaining that a general function of competition is to convert valuable private information into public information).

193. For a pathbreaking discussion of different contexts in which consumers are given information about a wide range of potentially hazardous products, see WESLEY A. MAGAT & W. KIP VISCUSI, INFORMATIONAL APPROACHES TO REGULATION (1992).

194. Sunstein, *supra* note 3, at 613.

195. David Colker & Joseph Menn, *ChoicePoint Had Earlier Data Leak*, L.A. TIMES, Mar. 2, 2005, at C1.

196. *See id.*

197. *See supra* text accompanying notes 77–80.

data and feel personally involved if this information is leaked.[198] Regarding this sense of ownership, *Money* magazine speaks to its readers in these terms regarding personal information held by data brokers: "It's your data, after all; these guys just figured out how to sell it."[199]

The proprietary sense that *Money* magazine identifies is not one that the law fully protects or recognizes.[200] But in the context of data leaks, it is enough, even in the absence of formal property rights, that most people believe that they have such a proprietary interest in their personal information. As a result of this belief, the public information created by notification letters has enjoyed a special resonance. Elected representatives, acting as norm entrepreneurs, have, in turn, been eager to draw on this information and public sentiment to propose new regulations.[201]

This movement of information from private to public is highly significant. When consumers learn of data breaches that involve their own information, they may not know what to do about the data leaks and may not even take the steps that the breach letter suggests, but they will be sensitized to the issue of data security. They may also be disturbed enough to complain to their elected representatives, government agencies, and the media. The media, in turn, will investigate specific breaches, explore different data processing industries and businesses, and publicize examples of organizational misbehavior in data handling. As information about data security breaches and industry practices becomes public, the public, media, and legislators learn about the kinds of errors that lead to data breaches and the types of mistakes that companies make. This situation creates an opportunity for legislators to suggest new regulations and for governmental agencies to provide pressure as to the appropriate content of existing legal standards.

Thus, one large payoff of mandated breach disclosure is that it can trigger legislative and other regulatory activity. This information can improve both regulation and company practices. It also can help create an evolving notion of the appropriateness of different practices, which will help shape the content of the emerging reasonableness standard of data security law and the interplay of this standard with any rules. One of the coauthors of this article, Paul Schwartz, has already argued, in the context of the regulation of voting technology, that a legal response to high tech areas is likely to require

---

198. This sense of involvement can add to emotional harm that sometimes follows an identity theft. *See* IDENTITY THEFT RESOURCE CENTER, IDENTITY THEFT: THE AFTERMATH 2003 35–39 (2003), *available at* http://www.idtheftcenter.org/idaftermath.pdf.

199. Pat Regnier, *Are You Terrified About Identity Theft Yet?*, MONEY, Sept. 2005, at 112, 116. Consider as well this consumer comment upon being informed of the ChoicePoint data breach: "[h]ow dare they even try to make money using my Social Security Number in the first place . . . Where did they get it from? I certainly didn't give it to them; I never heard of them before receiving the letter." Sullivan, *supra* note 176 (quoting anonymous e-mail to MSNBC.com).

200. Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 GEO. L.J. 2381, 2388–93 (1996).

201. *See, e.g.*, 151 CONG. REC. S7616-01 (June 29, 2005) (statement of Sen. Leahy).

both standards and rules.[202] The other coauthor, Edward Janger, has argued that in areas where technology is changing rapidly, such as the Internet, common understandings about behavior are not yet formed, and standard-based regulation may be required to allow courts and other decision-makers sufficient flexibility to develop and articulate principles in a common law fashion.[203] In particular, ongoing public information about data leaks will help to prevent the idea of a reasonable standard of data security from ossifying and will encourage the revision of any rules.

3. *Inside the Black Box*

Breach notification letters also have the potential to improve practices within the firm. These influences fall into three groups. Notification letters have the potential to (1) create a credible threat of negative costs or other punishments for the firm, (2) improve information flows within the firm, and (3) strengthen the position of the CPO.

The requirement that notification letters follow upon a data breach represents a highly significant compliance issue for a company and those who work at it. As Ayres and Braithwaite suggest as part of their work on enforced self-regulation, company performance improves significantly when some kind of credible punishment lurks outside the company.[204] One such "big gun" is a post-breach notification letter. This threat has the potential to improve performance across the board and to create ongoing pressure for innovation.

To be sure, all security incidents are not created equal. All do not create a firestorm of bad publicity. Moreover, consumers do not effectively use notification letters to shop for data security. Nevertheless, the reaction of the public, media, and government, and the consequences of these reactions will be hard for companies to predict in advance. By and large, therefore, companies will prefer to prevent negative publicity from data security breaches whenever possible. It is thus plausible to view the threat of sending customer notice as a "big gun" for regulatory purposes.

The breached entity faces costs in terms of managing the crisis, sending notices (if this step is taken), and seeking to regain the trust of its customers. Moreover, the customer notice creates an important feedback loop. The security breach becomes a news story in a way that anonymous notification and dry statistics do not. As in the ChoicePoint incident, for example, details regarding the breach may become part of the story. National media widely reported the ChoicePoint story when notice had only been given to individuals who had been affected by the breach.[205] The story was driven into

---

202. Schwartz, *supra* note 32, at 664–67.

203. Janger, *supra* note 32, at 1871–72.

204. *See* AYRES & BRAITHWAITE, *supra* note 72. at 25–27.

205. Joseph Menn and David Colker, *More Victims in Scam Will Be Alerted—Choicepoint says it will notify 110,000 people outside of California of the security breach*, L.A. TIMES, Feb. 17, 2005, at C1.

the headlines at this stage by the hitherto unknown nature of the data-broker industry, ChoicePoint's initial incredible assertions that non-Californians were not implicated by the breach, and the company's obvious stonewalling regarding other details of the incident.[206]

The public nature of the ChoicePoint story ultimately made the company a more attractive target for regulators who wished to act as policy entrepreneurs. In short order, the FTC pursued ChoicePoint and achieved a settlement that included a multimillion dollar fine as well as carefully targeted standards for improved firm behavior.[207] If, as Ayres and Braithwaite argue, the threat of severe sanctions assists government in its seeking of regulatory compliance, the FTC action against ChoicePoint leaves regulatory agencies involved in data security compliance in a far stronger position.[208]

Beyond creating a credible threat of negative costs or other punishments for the firm, a requirement of breach notification should improve the flow of information about data security throughout a firm. A variety of organization theorists have pointed out the extent to which the sharing of important information within companies can be suboptimal.[209] One major problem, as we have already seen in the context of consumer behavior, is information overload. As Malloy suggests, "[t]he environment in which most organizations and the individuals within them operate is constantly buzzing with enormous amounts of information and stimuli, generated both internally and externally."[210] Thus, attention itself is a scarce resource, and the merit of breach notification is that it represents a "big ticket" event that directs the attention of an organization and the individuals who work at it. It identifies data security as a clear priority.

Finally, breach notification letters should strengthen the position of CPOs and executives with related positions within the firm. Different projects and different individuals compete for the attention of top firm decisionmakers.[211] A company faces significant baseline choices in deciding how much to invest in data security compliance and where to locate CPOs in the firm hierarchy. As the requirement of sending a breach disclosure letter is extended to more firms, the internal significance of the CPO will be heightened. Moreover, as firm resources are increasingly devoted to data security, the issue which the CPO oversees, the CPO should increasingly be able to gain the attention of high executives in the company.[212]

---

206. Evan Perez, *ChoicePoint is Pressed to Explain Database Breach*, WALL ST. J., Feb. 25, 2005, at A6.

207. *See supra* text accompanying note 17.

208. *See* AYRES & BRAITHWAITE, *supra* note 72, at 40–47.

209. *See* RICHARD H. HALL & PAMELA S. TOLBERT, ORGANIZATIONS 148–53 (9th ed. 2005); Bamberger, *supra* note 28.

210. Malloy, *supra* note 29, at 555–56.

211. *See* HALL & TOLBERT, *supra* note 209, at 95–98.

212. Similar issues regarding the internal significance of the CPO arise as well in Germany, although the position and independence of the German equivalent of the CPO is explicitly protected

IV. NOTIFICATION AND MITIGATION

This Article concludes by presenting its own model for responding to data security breaches. Our Model Four seeks to go beyond simply informing consumers about security breaches; its goal is a coordination of the breach response by different entities both to mitigate the harm from the breach and to improve data security in the future. This model is a hybrid that draws on the best aspects of the three approaches already discussed, while avoiding, or at least minimizing, their weaknesses.

From Model One we learned that particularized customer notices serve an important role in making private information about security breaches and security practices publicly available. From Model One we also learned, however, that these notices rarely cause customers to change their behavior, and that these notices do little to mitigate harm flowing from the breach. Finally, from Model One we learned that the threat of particularized notice creates significant perverse incentives. Because notice of a security breach harms reputation and might also give rise to liability, data processing entities have an incentive to resist disclosure.

From Model Two, we learned about the possibilities of supervised delegation and of an institutionally supported coordinated response. Yet on its face, the Interagency Guidance leaves the decision to notify customers entirely in the hands of the breached entity. This Model, as embodied in the Interagency Guidance, is incomplete. It leaves open important questions about the role of both consumer and agency notification. For example, while the Interagency Guidance invokes a two-tiered standard for consumer and agency notification, it does not specify the manner of notification or the possibility of the oversight agency ordering notification when the data processor's investigation is insufficient or the results inconclusive. Similarly, the Interagency Guidance is silent about the actions that oversight agencies are supposed to take with information about security breaches which they receive through "first tier" notices. Should they maintain statistics? Should they communicate with other agencies? Should they communicate with other financial institutions?

Finally, from Model Three, we learned that breach notices serve two distinct functions that are often in tension with each other: reputational sanction and mitigation. The goal of reputational sanction creates a significant disincentive to disclose breaches, while the mitigation function generally gains little from the identification of the source of the breach. Nonetheless, Model Three's approach has significant costs. Particularized notice serves the benefit of transforming private information into a stock of public knowledge that is highly salient; it eliminates the problem of false positives; it sensitizes the public to data security issues, fuels media investigations, and creates pressure for regulation and oversight; and, as such, it can help improve internal firm practices.

---

by statute. *See generally* Spiros Simitis, *Beauftragter für den Datenschutz*, *in* KOMMENTAR ZUM BUNDESDATENSCHUTZGESETZ § 4f (Spiros Simitis ed., 6th ed. 2006).

A. *Model Four: The Coordinated Response Architecture*

Model Four develops a coordinated response architecture that seeks both to mitigate harm from breaches and to improve data security to prevent breaches. The key attributes of this architecture are: (1) supervised delegation of the decision whether to give notice, (2) coordination and targeting of notices to other institutions and to customers, (3) tailoring of notice content, (4) minimized data retention and decentralization, and (5) enforcement through both encouragement (carrot) and coercion (stick) of the data processing firm. Central to the architecture is a coordinated response agent (CRA) that oversees steps for automatic consumer protection and heightens mitigation. We begin the description of this Article's own approach, its Model Four, and the idea of the coordinated response architecture by describing the CRA and then turning to the nature of the particularized notice that will be sent to consumers.

1. *Supervised Delegation and Coordinated Response*

Model Four contemplates a bifurcated notice scheme similar to that contained in the Interagency Guidance: notification to the consumer follows upon a reasonable likelihood of "misuse" of notification-triggering information, and notification to the CRA requires a reasonable likelihood of "unauthorized access." This model differs from the current state trend, which, as we have noted earlier, generally follows the California model and relies on a simple "acquisition" standard. A small group of states have adopted a higher standard, that is, a more stringent one than California's, but no state has yet followed the path of the bifurcated notice scheme that this Article develops.

The initial disclosure would trigger a duty to investigate and report to the CRA. In consultation with the affected entity, the CRA would then determine whether there was a likelihood of misuse of the information. This two-tiered and interactive approach lets firms know that the CRA is watching and will scrutinize their decision whether or not to disclose information about a breach to the affected individuals.[213] It also increases the information that flows into a coordinated system for mitigation of breaches. In a nutshell, the CRA will coordinate the sharing of information about data security breaches, oversee the response of private sector entities to them, and supervise the decision of breached entities whether or not to disclose to consumers.

The CRA will also coordinate the notification effort. Here, a key point is that different notices serve different purposes. For example, the goal will be mitigation when the breached entity notifies the FTC and private credit-reporting agencies. In contrast, notice to individual customers will be shaped to allow customers to protect themselves as well as to make private

213. For a general discussion of the merits of such supervised delegation, see Bamberger, *supra* note 28.

information public. As such, the content of these various notices may differ based on the circumstances and the types of breaches. The CRA's role will be to supervise and coordinate rather than to store personal information or engage in notification of breached individuals.

In some regulatory areas, elements of these functions are already carried out by the FTC, the federal financial oversight agencies, and state attorneys general.[214] The proposed "Red Flags Rule" of the Department of Treasury and other federal agencies overseeing financial institutions offers a particularly intriguing example of information sharing to assist governmental oversight.[215] This regulation calls for information about "changing identity theft risks to customers and to the financial institution or creditor as they arise" to be part of a Red Flag list that the regulated organization maintained.[216]

Under the Red Flags Rule then, the organization and government would have access to information about emerging incidents and methods of identity theft. Similarly, New York and North Carolina require entities that send breach notifications to their customers also to inform the respective state attorney general's office.[217] Much more should be done, however, in these states to make this information publicly available. As in the Red Flag Rule, there is wisdom in making information about breaches accessible and giving multiple parties the chance to interpret the raw data and develop strategies to stop data leaks based on lessons from this information. More can also be done in the Red Flag Rule and these state approaches to introduce the element of coordinated response. In general, moreover, there is still no central entity that orchestrates notification and mitigation subsequent to a breach.

While there is a need for an entity in charge of coordinating actions after any particular breach, this Article also advocates flexibility regarding the different forms that a CRA might take. Although we speak of the CRA in the singular for simplicity purposes, its functions need not be centralized in any one stand-alone agency. In some circumstances, multiple agencies might carry out its tasks with benefits from this decentralization. A modest first step for the law would be to increase the powers under the Interagency Guidance of the different financial regulatory agencies in order to permit them to become CRAs with the powers that this Article sets out. Some of the functions of the CRA might even be delegated to the private sector and self-regulatory entities.[218]

---

214. *See supra* Section II.B.

215. Identity Theft Red Flags and Address Discrepancies under the Fair and Accurate Credit Transactions Act of 2003, 71 Fed. Reg. 40,786 (proposed July 18, 2006).

216. *Id.* at 40,791.

217. N.Y. GEN. BUS. LAW § 899-aa (8)(a) (McKinney 2005); N.C. GEN. STAT. § 75-65(f) (2005).

218. In tightly integrated industries, such as the securities business or banking, sometimes key participants are privately able to create coordinated structures that serve their needs. Similarly, private check clearinghouses might create their own data security and security breach regimes that might also have entities capable of serving as coordinated response agents in that industry. There are, nonetheless, risks to delegating too much authority to private entities. *See* Donna M. Nagy,

At the same time, however, certain core CRA functions should belong exclusively to a government agency, at least under current conditions of the law and the data security market. These functions are those related to the need for credible threats of enforcement.[219] A government agency—whether the FTC, financial oversight agencies, state attorneys general, or similar entities—is to be responsible for any ordering of notification or assessing of penalties.

By coordinating the sharing of information about security attacks with different organizations, the CRA is in a position to minimize the harm caused by the security leak without compromising the investigation. At present, there is an ad hoc approach to sharing information about data leaks. For example, the Los Angeles Police Department task force had jurisdiction over the investigation of the ChoicePoint incident but lacked authority to share relevant information with other data brokers or other governmental regulators.[220] In sharing information nationwide with law enforcement entities, other regulators, and even other companies, the CRA will increase the relevant knowledge base among the public and government entities.

In addition to coordinating the breached entity's internal investigation and its notification process, the CRA will set in motion automatic protective measures on behalf of the breached consumer. By statute, it will be authorized to request that (1) credit reports be sent to the consumer, (2) a fraud alert be placed on the consumer's credit file, and (3) information about the circumstances of the breach be placed in the FTC's identity theft database. Banks independently came to a similar conclusion regarding the wisdom of this last measure in July 2005 and agreed to share their data on identity theft directly with the FTC.[221] Yet, other breached entities at present do not share such information with any governmental entity. Having these measures take place without consumer action would both reduce the individual time spent responding to breach letters and heighten the amount of information about data breaches brought into the overall response system. Thus, in broad terms, the CRA will supervise the investigation into data security breaches, coordinate the sharing of information about these incidents, and orchestrate the systemic response to them.

2. *Tailoring Notice to Consumers*

The CRA will play an essential role in determining when and whether notification letters are sent to consumers. The CRA will also regulate the content of the notification in light of the nature of the data breach. To avoid customer confusion and to hold the entity accountable, the notice should in

---

Playing Peekaboo with Constitutional Law: The PCAOB and Its Public/Private Status, 80 NOTRE DAME L. REV. 975 (2005).

219. *See* AYRES & BRAITHWAITE, *supra* note 72, at 40–47.

220. Perez, *supra* note 206.

221. Joris Evers, *Banks to share ID theft data with FTC*, CNET NEWS.COM, July 6, 2005, http://news.com.com/Banks+to+share+ID+theft+data+with+FTC/2110-7348_3-5777098.html.

most cases identify the source of the breach. The notice will also state the protective measures that consumers should take to avoid identity theft. Moreover, these letters will detail certain automatic steps already taken to protect consumers, both internal, such as flagging accounts, and external, such as notifying credit reporting agencies and the FTC about the breach. This information will save the consumer time and inform them of FTC and other resources that are available. These letters will encourage consumers to engage in individual monitoring of whether these actions have, in fact, been carried out by the breached entity. Finally, notification will instruct consumers how to monitor their own accounts using the resources available.

The CRA will not only mandate certain content, but also will prohibit certain conduct by the breached entity. First, notification letters are often confusing and unclear; consumers may also confuse the letters with either junk mail, or, worse yet, phishing by fraudsters.[222] The CRA can take steps to combat concerns about both activities. In this area of rapid technological change, the CRA's goal should be to develop notification approaches while allowing industry groups to develop their own requirements. By permitting the development of self-regulatory guidelines and requiring them to be submitted to it for approval, the CRA will encourage both individual companies and the industry as a whole to develop innovative means to overcome the current weaknesses in notification.

Second, breached entities frequently use notice letters as an opportunity to market their own data security products. A statutory prohibition should block the marketing of commercial products and the making of solicitations in breach notices. As an example of this approach, the Specter-Leahy Personal Data Security and Privacy Bill of 2005 prohibits a breach notification from including: "(1) marketing information; (2) sales offers; or (3) any solicitation regarding the collection of additional personally identifiable information from an individual."[223]

3. *Minimizing Additional Data Storage and Decentralization*

A key aspect of the CRA is that it is designed to function without itself handling or storing much, if any, personal information. One of the great conundrums when seeking to structure a governmental role in responding to data security breaches is that the coordinating agency itself may become a repository of large amounts of personal data and, thereafter, a target for hackers.

To avoid this risk, the CRA will be designed around the principle of data minimization.[224] Consistent with this approach, it will draw on the resources

---

222. *See supra* text accompanying notes 174–175.

223. Personal Data Privacy and Security Act of 2005, S. 1332, 109th Cong. § 423(c) (2005).

224. *See generally* Spiros Simitis, *Reviewing Privacy in an Information Society*, 135 U. PA. L. REV. 707, 740 (1987) ("Personal information should only be processed for unequivocally specified purposes. Both government and private institutions should abstain from collecting and retrieving data merely for possible future uses for still unknown purposes.").

of existing data repositories rather than create its own new databases of personal information. For example, various credit-reporting agencies already maintain fraud watch lists. The CRA would not gather information about people subject to a breach, but would instruct the breached entity to communicate with the credit-reporting agencies. It would also coordinate investigations, oversee decisions made by breached entities of whether or not to send notification (though it would not send the notices itself), and help regulate the content of notices. Finally, the CRA would prepare comparative statistical information regarding data security events. This last activity is consistent, for example, with the governmental role, explored by Sunstein, in compiling statistical information along different dimensions to provide an overall measure of the national well-being.[225]

The creation of comparative statistical information will be useful on three levels. First, it will give the CRA and other government agencies the ability to distinguish good data security actors from bad ones. Over time, the government will be able to gain a better sense of the good and bad apples. Second, the comparative information will provide companies with a credible basis—a track record—for evaluating their data security and that of the rest of the pack. If an entity engages in damage control by buying advertisements that tout its security efforts, these claims will be more easily subjected to a reality check. Finally, such data will be useful in improving the consumer-side data security marketplace. These statistics would provide consumers with better comparative information about data security practices.

4. *Enforcement and the Disclosure Disincentive*

As for the disclosure disincentive, Model Four seeks to overcome it through judicious use of both carrot and stick. First, as the carrot, Model Four offers companies a chance to avoid consumer notice by early reporting to and cooperating with the CRA. As the stick, Model Four adopts the California statute's private right of action for failure to disclose and sets statutory damages of $500 for each failure to notify.[226] As noted earlier, most state statutes do not take this approach—only three states currently provide for a private right of action.[227] Model Four also draws on another important aspect of the Specter-Leahy Bill. This bill suggests a particularly strong alternative response to the disclosure disincentive. It creates criminal penalties for any company official who intentionally and willfully conceals the fact of a security breach for which the law requires individual notice to be given.[228] A CPO of anything but a rogue organization is unlikely to run the risk of these criminal penalties.

---

225. Cass R. Sunstein, *Well-Being and the State*, 107 HARV. L. REV. 1303 (1994).

226. *See* CAL. CIV. CODE § 1798.84(c) (West Supp. 2006).

227. *See* Appendix.

228. Personal Data Privacy and Security Act of 2005, S. 1332, 109th Cong. § 103 (2005).

Finally, regarding the law enforcement delay, the CRA can do much to keep any postponement of notification as short as possible and to limit the harm that it causes. Once information about a breach is shared with both the CRA and law enforcement officials, two things will happen. First, the CRA is to monitor the investigation, and second, since it has an interest in disclosure, it must ensure that the law enforcement delay is no longer than necessary. It can see that the delay is kept to an explicit short period, such as thirty days, unless investigators certify to the CRA in writing the special circumstances that require further delay.[229]

B. *Unpacking Model Four*

Having described our coordinated response architecture, we will conclude by fleshing out a few of its key attributes in greater detail, explicating a few of our choices, and, in particular, demonstrating how our model of supervised delegation, coordinated notice, and decentralization will foster a culture of compliance with data security norms.

1. *Reputational Information*

Model Four retains particularized notice as the norm, but adopts Model Three's anonymized disclosure as a tool in the limited situations where its benefits outweigh its costs. This decision is made notwithstanding the fact that the reputational sanction functions in an uncertain fashion at best when particularized notice occurs under Models One and Two. As a consequence, not much will be lost should consumers lack access to reputational information.

These concerns must, however, be balanced against some costs that result from anonymous disclosure. Consumer opposition to Model Three's ADI—due to a proprietary sense regarding personal information—is likely, as a political and practical matter, to make this approach infeasible in most contexts.[230] A further concern with the ADI is that it would stifle transformation of private-to-public information and block outside pressure capable of improving behavior of the firm. Also, under Model Three, the general public, the media, and the legislative branch would lack knowledge of the specifics of data leaks. The ADI might thereby cut off the flow of important information into the public sphere and squelch nascent and, indeed, necessary reforms of data security. Anonymous disclosure may also cause false positives through a likely misallocation of guilt by inference.[231] Most individuals will be likely to blame their bank or credit card issuer rather than some unseen entity, such as a data aggregator, payment processor, or

229. The Specter-Leahy Bill has a similar requirement. *Id.* § 422(c).

230. *See supra* Section III.C.

231. Individuals who receive non-particularized breach disclosure letters will nevertheless be likely to draw conclusions about the culprit's identity. *See supra* Section III.B.

data-storage company—or a lower profile entity, such as a typical bricks-and-mortar retailer.

2. *Supervised Discretion*

Model Four initially assigns the decision to disclose to the breached entity, but uses the CRA to limit and supervise this exercise of discretion. In this regard, Model Four follows the path of Model Two with a raised threshold (likelihood of misuse) for consumer disclosure, but a low threshold (unauthorized access) for disclosure to the CRA. While the higher threshold in isolation raises the possibility that a firm might use its power to investigate as a mechanism for stonewalling, Model Four, like Model Two, requires notification of a government agency, the CRA, on a lower track. This second track provides an early warning as well as a check on the firm's discretion whether or not to disclose to consumers.

In short, our view is that delegated discretion functions best when there is an ongoing dialogue between the firm and an agency. As Bamberger suggests generally, "Decision-makers can step outside existing knowledge structures when external stimuli prompt them to devote attention to particular situations they confront, to account for unexpected information, and to consider unfamiliar implications."[232] Model Four creates a way for such testing of existing "knowledge structures" within the firm.

The CRA oversees the decision whether or not particularized notice should be given to the consumer. It provides rolling regulatory inputs regarding the form that notice should take. It is also worth stressing that industry self-regulation, without these regulatory inputs, has proven ineffective thus far. As one example, Visa requires merchants that use its payment cards to meet its security standards. However, Visa acknowledges that only fifteen percent of the 215 largest retailers that accept its cards can certify that they meet the current standards.[233] Visa and MasterCard are also in talks to develop a private group that will establish and administer new industry-wide security standards.[234] Our hope is that with the CRA looking over the industry's shoulder, any new self-regulatory proposals for tightened data security will have not only public relations bark, but also some actual bite.[235] As two data security experts have stated regarding the need for a government role in oversight of the payment card industry, "A reminder that there is a cop on the beat for those who do not adhere to reasonable security pro-

---

232. Bamberger, *supra* note 28, at 446.

233. Dash, *supra* note 40.

234. *Id.*

235. *Id.* Concerning shortcomings of existing self-regulation by the payment-cards industry, consider the B.J. Warehouse Club data breach, *see* BJ's News Release, *supra* note 41, and the CardSystems incident, *see* Eric Dash, *Take a Number: How Electronic Thefts Revealed the Vulnerabilities of Payment Systems*, N.Y. TIMES, June 30, 2005, at C1.

cedures will be a good message for the industry."[236] Finally, Model Four takes some decisions off the table by refusing to delegate them. For example, legislation should prohibit any marketing within a breach-disclosure notification.

The CRA can serve an important role in solving the boy-who-cried-wolf problem, that is, the problem of consumers deluged with breach notices who decide to ignore them rather than take steps to protect themselves. It can ensure that notices are only sent when there is a risk of misuse of personal information. Moreover, it can help shape the content of notification letters to overcome the problem of content triviality. The CRA can help to see that clearly worded letters, or a combination of letters and telephone messages, inform affected consumers of a breach. A recent survey by the Ponemon Institute has indicated positive results in terms of consumer comprehension following combined means of notification.[237] More can also be done to make genuine notification letters distinguishable from phishing.[238] Finally, shifting to more automatic protection will help overcome the concern about consumer inaction as a consequence of too many notification letters.

Thus, this Article recommends the higher "likelihood of misuse" standard for consumer notification. We think that this standard will go a long way to reduce the danger of information overload. To return to the boy who cried wolf, the villagers may not need constant reminders that wolves are eyeing the sheep, or even that the shepherd has blocked attempted incursions. Rather, the villagers need to know when there is an open risk of a specific threat. Imagine that the shepherd wished to protect the sheep by calling on reinforcements from the villagers when necessary. This shepherd, in his role of the office of sheep security, would inform the villagers only of real attacks by wolves. He would not merely cry "wolf," but would describe the wolf's physical characteristics and the direction he was coming from, and provide other detail sufficient to advise the villagers of how best to protect the endangered sheep. This information is far from trivial, and the cry of "wolf" would not be shrugged off when presented in this manner.

---

236. Mark MacCarthy & John Shaughnessy, *Payment Card Industry Data Security Standard*, *in* PROSKAUER ON PRIVACY 16–39 (Christopher Wolf ed., 2006).

237. PONEMON INST., *supra* note 18, at 8–9.

238. There are two related problems here. If the notification is sent by snail mail, there is a risk that the communication will be confused with junk mail, such as unwanted credit card solicitations. If the notification is sent by e-mail, there is an even greater risk that it will be confused with phishing. A strategy that might help a CRA to overcome these problems is to send particularized notice along with a bill or other communication that contains sufficient information, perhaps about the account at the entity, to unambiguously indicate that the communication is from an authentic sender.

This solution does not help, however, where a "shadow entity" is involved, and here there is also a greater risk that the customer will likely ignore the communication because of the lack of an existing B2C relationship. In reaction, the notice from a shadow entity might be sent by a government agency or a credit-reporting agency whose correspondence would not be ignored by a consumer. It is important, however, that, consistent with our goal of data minimization, the notice should be sent only by an entity that already has sufficient data (for example, name and address) to send out the notice.

In other words, a key function of the CRA will be to ensure that consumers will not be informed except when the information about a breach will be useful to them or, more generally, to society. Moreover, we think that a lower standard for sharing information with the CRA will have the considerable benefit of increasing the overall information flow into it.

In the context of breach notification, the level of required supervision will turn on both the type of data processing entity involved and the type of data that has been stolen. We expect that entities directly subject to market forces, such as financial entities and B2C businesses, may prove more likely to cooperate with the CRA and, hence, more likely to disclose and investigate fully. By contrast, shadow entities like ChoicePoint may be likely to require more intrusive regulation—at least until government regulators use one or more "big gun" sanctions.

3. *Coordination of Post-Breach Mitigation Efforts*

In addition to overseeing the discretion of breached entities in deciding when to notify and regulating the content of breach notices, the CRA may help to determine who should receive notice and when. For example, assume that a financial institution discovers that an unauthorized party has gained access to a series of credit card numbers, expiration dates, and account holders' names. Such data can be used to make fraudulent charges on those particular accounts. At that moment, the institution may not know if the access was obtained by somebody who poses a risk (a thief), or merely an employee who should not have gained access but who will only make appropriate use of the data. The firm would naturally flag such accounts at its own institution, but under Model Four, it will also be required to notify the CRA.

The CRA will then take a number of actions. Its immediate concern will be making sure that the entity was conducting an investigation to gather more information about the nature of the security incident and the extent of any open risks. As more information comes in about the institution's investigation, the CRA might want to contact law enforcement in order to start outside attempts to identify and apprehend any wrongdoer. It might also wish to contact the FTC, credit-reporting agencies, and possibly other institutions or private entities in the same or related industries as the breached organization. At this juncture, the CRA might also permit a short delay in notifying customers. The coordinated nature of the response should help minimize harm to the account holder.

4. *Delay to Allow Investigation before Consumer Notification*

This Article has pointed to a law enforcement delay as possibly heightening a lag in consumer detection of identity theft. The ADI had the posited benefit of being able to reduce or even eliminate the law enforcement delay. The idea was that anonymous notification might take place simultaneously

with a law enforcement investigation.[239] While anonymous disclosure may sometimes be feasible and promising, we have also pointed to reasons why even anonymous disclosure may leave organizations still reluctant to share information with an ADI. This Article's preference is to develop a coordinated response architecture to keep postponement of notification as short as possible and to minimize any harm from this delay.

5. *Provision for Damages and Other Enforcement Rights*

As we have noted, Model Four adopts the California statute's private right of action for failure to disclose and sets statutory damages of $500 for each failure to notify.[240] The threat of class action lawsuits is likely, however, to exert a heavy force on companies to admit data leaks.

6. *The Culture of Compliance*

The notice-based approach of the California breach notification statute represents an important step toward creating a widespread corporate culture that takes data security seriously. The fear of reputational sanction is an important motivator, and we recognize its value. Similarly, the Interagency Guidance's mandating of a CPO and its requirements of risk assessments and response programs are important steps in creating norms within corporate entities with regard to data security.

In our view, moreover, Model Four and the CRA will build on this existing jurisprudence to create a more comprehensive and more nuanced culture of data security and customer notice. This Article advocates an approach that will provide greater ability to mitigate the harm associated with security breaches while also being sensitive to how businesses operate. One of the most attractive aspects of our coordinated response architecture is that it puts in place a system that has the capacity to learn from successes and failures, whether those of itself or others. CRAs will be repeat players in the world of security breaches, and commercial organizations will be repeat players with their respective CRAs.[241] Over time, these parties will learn what works and what does not. There will be accumulated wisdom, for example, about the forms of notice that work best, and the parties who should be notified at once when certain kinds of breaches occur.

Finally, it is important to recognize that the response architecture is just that—an organizing structure. It allocates responsibility and accountability, but remains open to gathering and sharing knowledge about particular practices with participants in the process of providing data security. In our view, these practices should evolve over time as technology and commercial

239. *See supra* Section III.C.

240. *See* CAL. CIV. CODE § 1798.84(c) (West Supp. 2006).

241. For a theoretical discussion of the importance of repeat play in political institutions, see DOUGLAS G. BAIRD ET AL., GAME THEORY AND THE LAW 159–88 (1994). For a concrete application of the implications of repeat play, see ROBERT C. ELLICKSON, ORDER WITHOUT LAW: HOW NEIGHBORS SETTLE DISPUTES 177–83 (1991).

practices change. Such evolution is permitted, if not guaranteed, by the presence of standards in the emerging law of data security and breach notification. As technology develops and then fails in unexpected ways, overarching standards are available to plug gaps in more specific rules. The resulting dynamic mixture of standards and rules permits a flexible development in the resulting pattern of legal commands.

CONCLUSION

Data security is a topic of almost daily headlines, and one that is garnering great attention from legislators. The current level of awareness is largely a function of state statutes that mandate consumer notification of security breaches and federal regulation of financial institutions. This Article evaluates the two main existing legislative models regarding mandatory consumer notification and finds that both have notable strengths and weaknesses. Model One, as reflected in the California breach notification statute, sets a low threshold for consumer notice (a reasonable belief of "acquisition" of leaked information) and has the advantage of narrowing business discretion as to whether or not to notify consumers. With regard to reputational sanctions, it has the further benefit of ensuring that information about breaches will be publicly disseminated. And, regarding the mitigation of harm, this standard has the potential of providing consumers with information to allow self-protection.

There are also disadvantages to this paradigm. Model One does not respond to the disclosure disincentive, envelope triviality, or content triviality. Companies may seek to avoid notification of consumers. In turn, consumers may not open notification letters or act on their information because they are already overwhelmed by communications from commercial entities and the letters themselves do not convey their content effectively. As such, the letters as currently constituted may not provide particularly useful information about a company's security practices, or about the steps customers should take to protect themselves from harm. Finally, beyond these threats, to the extent that these letters are intended to help people shop for data security, consumers are likely to be bad at making choices on the basis of such nonprice information.

Model Two, as embodied in the Interagency Guidance, establishes two tracks for notification. It has a high threshold for consumer notification (a reasonable belief of "misuse" of leaked information), and a low threshold for notification of the oversight agency (a reasonable belief of "acquisition" of leaked information). The advantage of this regime vis-à-vis Model One is chiefly that it contains a formal mechanism for involving a governmental entity in supervising the response to a data security breach. The chief comparative disadvantage of Model Two is that to the extent that it gives businesses discretion for notification, it will permit foot-dragging and obfuscation instead of prompt disclosure.

Model Three, our thought experiment based on comments of the Chicago FRB, has an almost entirely different set of strong and weak points. On

the plus side, it may be able to overcome the disclosure disincentive by withholding the identity of the breached entity. The sacrifice of the reputational sanction may also help with mitigating the harm from a data breach. If the ADI does lead to greater overall information about data leaks flowing into the system, it can facilitate a coordinated response by sharing information about the security breaches with other business entities, and, in anonymous form, with consumers.

While the costs of anonymous disclosure will often outweigh its benefits, this thought experiment demonstrates why particularized notification matters—and it is not the reason usually offered. Particularized disclosure alone is not likely to do much to perfect the market for data security. Instead, notification letters that name the breached entity serve to change the status of information from private to public knowledge and create positive pressure on organizational practices.

Important benefits flow from this transformation. The first occurs as consumers and the media learn of data breaches and an opportunity is created for norm entrepreneurs, including legislators, to suggest new regulations and approaches. The second benefit is the pressure that is then placed on businesses to improve their practices. The third benefit is greater awareness of the kinds of errors that lead to data breaches and the types of mistakes that companies make. This information can improve the quality of regulation and company practices. The fourth benefit is that this public information will shape legal notions of practices that are consistent with a reasonable standard for data security.

In response to the strengths and weaknesses of these three models, this Article has proposed a coordinated response architecture. In Model Four, an independent organization balances the reputation-based function of notice against the goal of mitigating harm. In brief, this model limits the disclosure disincentive and overcomes the boy-who-cried-wolf problem. Consumers should receive information about data security leaks, but in a fashion that is useful to them. The legal system should do far more to protect them from the harms that flow from data breaches.

STATE SECURITY BREACH NOTIFICATION LAWS

Jurisdiction	Entities Covered	Trigger For Notification	But Entities Do Not Have To Notify If:	Party to Whom Disclosure is Required	Substantive Requirement For Level Of Security?	Private Right Of Action For Violations Of The Statute?
				(Affected Individuals, Owner or licensee of information, and/or Credit Reporting Agencies)		(This refers to failure to notify unless statute also provides for substantive requirements for level of security)
Arizona S.B. 1338 (signed into law April 26, 2006, Chapter 232) ARIZ. REV. STAT. § 44-7501 Effective January 1, 2007	• Individuals • Businesses • State Agencies	Acquisition or access to personal information	After reasonable investigation, entity or law enforcement determines that breach has not occurred or is not reasonably likely to occur	• Affected Individuals • Owner or licensee of information		• No. Attorney General has exclusive right to enforce
Arkansas ARK. CODE ANN. § 4-110 *et seq.*	• Individuals • Businesses • State Agencies	Acquisition	After reasonable investigation the entity determines there's no reasonable likelihood of harm to individuals	• Affected Individuals • Owner or licensee of information	Reasonable security procedures and practices AND Reasonable steps to destroy data that are no longer necessary to retain	• No. Attorney General has exclusive right to enforce
California CAL. CIVIL CODE § 1798.29 CAL. CIVIL CODE § 1798.82	• Individuals • Businesses • State Agencies	Acquisition		• Affected Individuals • Owner or licensee of information	Reasonable security procedures and practices AND Reasonable steps to destroy data that are no longer to be retained	• Yes, to "any customer injured by a violation of this title" • Additional penalty for willful, intentional, reckless violations

Jurisdiction	Entities Covered	Trigger For Notification	But Entities Do Not Have To Notify If:	Party to Whom Disclosure is Required	Substantive Requirement For Level Of Security?	Private Right Of Action For Violations Of The Statute?
Colorado H.B. 1119 (signed into law April 24, 2006) COLO. REV. STAT. § 6-1-716 Effective September 1, 2006	• Individuals • Businesses • State Agencies	Acquisition	Investigation determines the misuse of information about a Colorado resident has not occurred and is not reasonably likely to occur	• Affected Individuals • Owner or licensee of information • Credit Reporting Agencies, if greater than 1,000 persons affected		• No. Attorney General has exclusive right to enforce
Connecticut S.B. 650 (signed into law June 8, 2005, Public Act 05-148) CONN. GEN. STAT. § 36a-701b Effective January 1, 2006	• Any person	"Access to or acquisition"	Investigation reveals no reasonable likelihood of harm to customers	• Affected Individuals • Owner or licensee of information		• No. Attorney General has exclusive right to enforce
Delaware DEL. CODE ANN. tit. 6, § 12B-101 *et seq.*	• Individuals • Businesses	Acquisition	Investigation determines that the misuse of information is not reasonably likely to occur	• Affected Individuals • Owner or licensee of information		• No. Attorney General has exclusive right to enforce
Florida FLA. STAT. ch. 817.5681	• Any person	Acquisition	Investigation reveals no reasonable likelihood of harm to customers	• Affected Individuals • Owner or licensee of information • Credit Reporting Agencies, if greater than 1,000 persons affected		• No, failure to notify subject to administrative fines (not generally applicable to state agencies)

Jurisdiction	Entities Covered	Trigger For Notification	But Entities Do Not Have To Notify If:	Party to Whom Disclosure is Required	Substantive Requirement For Level Of Security?	Private Right Of Action For Violations Of The Statute?
Georgia GA. CODE ANN. § 10-1-912	• Information Brokers Only	Acquisition		• Affected Individuals • Owner or licensee of information • Credit Reporting Agencies, if greater than 10,000 persons affected		• Does not specify
Hawaii S.B. 2290 (signed into law May 25, 2006, Act 135) To be codified at HAW. REV. STAT. tit. 26 Effective January 1, 2007	• Any person • Business	Illegal use of the information has occurred or is reasonably likely to occur or that creates a material risk of harm to the person	No reasonable likelihood of illegal use of information or material risk of harm	• Affected Individuals • Owner or licensee of information • Credit Reporting Agencies, if greater than 1,000 persons affected		• No. Enforcement by the Hawaii Attorney General or its Executive Director of the Office of Consumer Protection
Idaho S.B. 1374 (signed into law March 30, 2006, Chapter 258) IDAHO CODE §§ 28-51-104 *et seq.* Effective July 1, 2006	• Agency • Individual or • Commercial entity	Information was or is reasonably believed to have been misused	After reasonable and prompt investigation, the person determines that there is no reasonable likelihood the personal information has been or will be misused	• Affected Individuals • Owner or licensee of information		• Agency's, commercial entity's, or individual's primary regulator

Jurisdiction	Entities Covered	Trigger For Notification	But Entities Do Not Have To Notify If:	Party to Whom Disclosure is Required	Substantive Requirement For Level Of Security?	Private Right Of Action For Violations Of The Statute?
Illinois 815 ILL. COMP. STAT. 530/10 Effective January 1, 2006	• Any entity that collects or handles personal info	Acquisition		• Affected Individuals • Owner or licensee of information		• Statute says violations are "unlawful acts" under Consumer Fraud and Deceptive Business Practices Act, which itself provides any person who suffers actual damage can bring action, and Attorney General may enforce
Indiana IND. CODE ANN. § 4-1-11-1, *et seq.* (Applicable to state agencies) IND. CODE ANN. § 24-4.9-3-1 (Applicable to any database owner) Effective July 1, 2006	• Any database owner (formerly applicable only to state agencies; amended in March 2006 to include private entities, to exempt various state agencies, and to insert several new provisions)	Information acquired by an unauthorized person, if the person should know or should have known the unauthorized acquisition has resulted or could result in identity deception, identity theft, or fraud affecting the Indiana resident		• Affected Individuals • Owner or licensee of information • Credit Reporting Agencies, if greater than 1,000 persons affected		• No. Attorney General has exclusive right to enforce
Kansas S.B. 196 (signed into law April 19, 2006) (Yet to be codified.) Effective January 1, 2007	• Person • Business	Breach involving likelihood that personal information has been or will be misused	Reasonable and prompt investigation reveals misuse has not occurred or is unlikely	• Affected Individuals • Owner or licensee of information • Credit Reporting Agencies, if greater than 1,000 persons affected		• No. Attorney General has exclusive right to enforce, or insurance commissioner, in the case of an insurance company

Jurisdiction	Entities Covered	Trigger For Notification	But Entities Do Not Have To Notify if:	Party to Whom Disclosure is Required	Substantive Requirement For Level Of Security?	Private Right Of Action For Violations Of The Statute?
Louisiana LA. REV. STAT. § 51:3071 *et seq.*	Any person	Acquisition	Reasonable investigation reveals harm to be unlikely	• Affected Individuals • Owner or licensee of information		• Yes, for actual damages resulting from the failure to disclose
Maine ME. REV. STAT. ANN. tit. 10, § 1346 *et seq.* Amended by L.D. 2017 (signed into law April 14, 2006) Amendments to the law, effective January 31, 2007	• Any person or entity • Information Broker • Formerly only Information Brokers	Reasonable and prompt investigation determines that misuse of a state resident's personal information has occurred, or if it is reasonably possible misuse will occur	Reasonable and prompt investigation determines that misuse has not occurred or is unlikely	• Affected Individuals • Owner or licensee of information • Credit Reporting Agencies, if greater than 1,000 persons affected • State regulators within Department of Professional and Financial Regulation, or Attorney General		• No, enforced by Attorney General and Department of Professional and Financial Regulation • Civil fines also applicable
Michigan 2006 S.B. 309 Public Act 566 Effective July 2, 2007	• Individuals • Businesses • Agency that owns or licenses data (includes state agencies) • Exempts persons or agencies subject to Title V of the Gramm-Leach-Bliley Act	Access and Acquisition	Person or agency determines that the security breach has not or is not likely to cause substantial loss or injury to, or result in identity theft with respect to, one or more residents of this state	• Affected individuals • Credit reporting agencies, if more than 1000 residents are affected	Destruction of records no longer to be retained	• No. Person who knowingly fails to notify may be ordererd to pay a civil fine of not more than $250 for each failure to provide notice. Attorney general or a prosecuting attorney may bring an action to recover a civil fine under this section. The aggregate liability of a person for civil fines under subsection for multiple violations that arise from the same security breach shall not exceed $750,000

Jurisdiction	Entities Covered	Trigger For Notification	But Entities Do Not Have To Notify If:	Party to Whom Disclosure is Required	Substantive Requirement For Level Of Security?	Private Right Of Action For Violations Of The Statute?
Minnesota MINN. STAT. § 325E.61	• Any person or business • Exception: not applicable to "financial *institution" in* 15 U.S.C. § 6809(3), or entities subject to privacy and security regulations adopted under HIPAA	Acquisition		• Affected Individuals • Owner or licensee of information • Credit Reporting Agencies, if greater than 500 persons affected	"Each government entity shall conduct a comprehensive security assessment of any personal information maintained by the *government entity*"	• No. Attorney General has exclusive right to enforce
Montana MONT. CODE ANN. § 30-14-1704	• Any person or • Business	Acquisition		• Affected Individuals • *Owner or licensee of* information	Reasonable steps to destroy data that are no longer necessary to maintain	• No. Enforceable by Department of Justice, Attorney General, or *insurance commissioner (when* insurance companies are involved)
Nebraska L.B. 876 (signed into law April 6, 2006) (Yet to be codified.) Effective July 1, 2006	• Any person or • Commercial entity	If the investigation determines use of information about a Nebraska resident for an unauthorized purpose has occurred or is reasonably *likely to occur*	Use of information for an unauthorized purpose is not reasonably likely to occur	• Affected Individuals • Owner or licensee of information		• No. Attorney General has exclusive right to enforce

Jurisdiction	Entities Covered	Trigger For Notification	But Entities Do Not Have To Notify If:	Party to Whom Disclosure is Required	Substantive Requirement For Level Of Security?	Private Right Of Action For Violations Of The Statute?
Nevada NEV. STAT. § 52.603A	• Agency • Business	Acquisition		• Affected Individuals • Owner or licensee of information • Credit Reporting Agencies, if greater than 1,000 persons affected	"Reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification or disclosure" Reasonable steps to destroy data that are no longer necessary to maintain	• Attorney General has right to enforce; district attorneys can also bring injunctions • Breached entity may sue breacher
New Hampshire N.H. REV. STAT., tit. XXXI, §359-C:20 Effective Jan. 1, 2007	• Individuals • Businesses • State Agencies	Investigation leads to the determination that misuse of the information has occurred or is reasonably likely to occur, or if a determination cannot be made	Entity determines that there is no likelihood that misuse has occurred or is reasonably likely to occur	• Affected individuals • Owner or licensee of information • Credit Reporting Agencies, if greater than 1,000 persons affected • Persons engaged in trade or commerce, should notify the regulator that has primary regulatory authority of the involved trade or commerce; all other persons should inform the Attorney General		• Does not specify

Jurisdiction	Entities Covered	Trigger For Notification	But Entities Do Not Have To Notify If:	Party to Whom Disclosure is Required	Substantive Requirement For Level Of Security?	Private Right Of Action For Violations Of The Statute?
New Jersey N.J. STAT. ANN. § 56:8-163	• Business • Public entity	Access and Acquisition	"Entity establishes that misuse of the information is not reasonably possible"	• Affected Individuals • Owner or licensee of information • Credit Reporting Agencies, if greater than 1,000 persons affected • Division of State Police in the Department of Law and Public Safety	Reasonable steps to destroy data that are no longer to be retained	• Yes; Attorney General can enforce, but injured person can also bring action
New York State N.Y. STATE TECH LAW § 57-A:208 N.Y. GEN. BUS. § 899-aa	• State entities • Any person or business	Acquisition		• Affected Individuals • Owner or licensee of information • Attorney General, Consumer Protection Board, and State Office of Cyber Security and Critical Infrastructure Coordination must also be notified • If more than 5,000 persons must be notified at one time, consumer reporting agencies must also be notified		• No. Attorney General has exclusive right to bring actions • However, court can award actual damages to individuals harmed

Jurisdiction	Entities Covered	Trigger For Notification	But Entities Do Not Have To Notify If:	Party to Whom Disclosure is Required	Substantive Requirement For Level Of Security?	Private Right Of Action For Violations Of The Statute?
New York City NEW YORK CITY ADMIN. CODE § 20-117	• Persons or businesses required to be licensed by the Department of Consumer Affairs (DCA). Companies that must be licensed include 55 categories of small businesses • Persons required to be licensed by provisions of state law enforced by the DCA who own, lease, or maintain personal data	Personal information was or is reasonably believed to have been acquired by an unauthorized person		• Department of Consumer Affairs • Police Department • Affected individuals	Includes provision governing discarding personal records in a way that prevents retrieval by unauthorized persons	• Yes, but limited: upon conviction, person is subject to fine of no more than $500 and liable for civil penalty of no more than $100
North Carolina N.C. GEN. STAT. § 75-60	• Any business ("business" explicitly defined as not including state agencies)	Acquisition by an unauthorized person and unauthorized or illegal use of the personal information has occurred or is reasonably likely to occur	Unauthorized or illegal use of personal information is not reasonably likely to occur	• Affected Individuals • Owner or licensee of information • Credit Reporting Agencies, if greater than 1,000 persons affected	Reasonable measures to protect against unauthorized access to or use, including destruction of records	• Yes, if a person is injured as a result of a violation

Jurisdiction	Entities Covered	Trigger For Notification	But Entities Do Not Have To Notify If:	Party to Whom Disclosure is Required	Substantive Requirement For Level Of Security?	Private Right Of Action For Violations Of The Statute?
North Dakota N.D. CENT. CODE § 51-30-01, *et seq.*	• Any person that conducts business	Acquisition		• Affected Individuals • Owner or licensee of information		• Yes; Attorney General may enforce, but remedies from state's "Unlawful Sales or Advertising" laws are also available. These remedies include private party claims
Ohio OHIO REV. CODE ANN. §§ 1347.12, 1349.19	• State agencies • Business entities	"Accessed and acquired" *if* "material risk of identity theft or other fraud to the resident"	No material risk of identity theft or other fraud to the resident	• Affected Individuals • Owner or licensee of information • Credit Reporting Agencies, if greater than 1,000 persons affected		• No. Attorney General has exclusive right to bring actions
Pennsylvania S.B. 712 (signed into law Dec. 22, 2005, Act No. 94) 73 PA. CONS. STAT. § 2302 *et seq.* Effective June 22, 2006	• Any entity	"Accessed and acquired," and causing or reasonably believes will cause injury		• Affected Individuals • Owner or licensee of information • Credit Reporting Agencies, if greater than 1,000 persons affected		• No. Attorney General has exclusive right to bring actions
Rhode Island R.I. GEN. LAWS § 11-49.2-1 *et seq.*	• Any state agency or person • Does not include HIPAA agencies	Breaches that pose a significant risk of identity theft	Breach has not and will not likely result in a significant risk of identity theft	• Affected state residents • Owner or licensee of information	Reasonable security procedures and practices	• Yes, violator subject to a fine of not more than $100 per occurrence up to $25,000

Jurisdiction	Entities Covered	Trigger For Notification	But Entities Do Not Have To Notify If:	Party to Whom Disclosure is Required	Substantive Requirement For Level Of Security?	Private Right Of Action For Violations Of The Statute?
Tennessee TENN. CODE ANN. § 47-18-2107	• Persons • Businesses • State agencies • Excludes persons subject to Gramm-Leach-Bliley Act	Acquisition		• Affected Individuals • Owner or licensee of information • Credit Reporting Agencies, if greater than 1,000 persons affected		• Yes; excludes actions brought by customers of state agencies
Texas TEX. BUS. & COM. CODE ANN. § 48.103	• Any person that conducts business	Acquisition		• Affected Individuals • Owner or licensee of information • Credit Reporting Agencies, if greater than 10,000 persons affected	Reasonable procedures to protect information AND Destruction of records no longer to be retained	• Yes. Harmed individual can obtain equitable relief. Attorney General can obtain civil penalties and other reasonable costs
Utah S.B. 69 (signed into law March 20, 2006, Session Law Chapter 343) UTAH CODE ANN. § 13-44-101 *et seq.* Effective January 1, 2007	• Any person that conducts business or maintains computerized data	Misuse of personal information for identity theft or fraud has or is reasonably likely to occur	Misuse of personal information for identity theft or fraud is not reasonably likely to occur	• Affected Individuals • Owner or licensee of information	Reasonable procedures to protect information AND Destruction of records no longer to be retained	• No; provides for Attorney General enforcement; Attorney General may seek injunctive relief or levy fines

Jurisdiction	Entities Covered	Trigger For Notification	But Entities Do Not Have To Notify If:	Party to Whom Disclosure is Required	Substantive Requirement For Level Of Security?	Private Right Of Action For Violations Of The Statute?
Vermont S. 284 (signed into law May 18, 2006, Act 162) VT. STAT. ANN. tit. 9, § 2430 *et seq.* Effective January 1, 2007	• Any data collector	Acquisition or access	Data collector establishes that misuse is not reasonably possible and provides notice of that determination and an explanation to the AG or to the department of banking, insurance, securities, and health care administration, as applicable	• Affected Individuals • Owner or licensee of information • Credit Reporting Agencies, if greater than 1,000 persons affected		• No; provides the department of banking, insurance, securities, and health care administration with exclusive enforcement power over entities registered with that department • The state Attorney General and state attorney have exclusive enforcement authority with respect to all other entities
Washington WASH. REV. CODE § 19.255.010	• Any person or business	Acquisition	Not required to disclose a technical breach of the security system that does not seem reasonably likely to subject customers to a risk of criminal activity	• Affected Individuals • Owner or licensee of information		• Yes; civil damages permitted
Wisconsin S.B. 164 (signed into law March 16, 2006, Act 138) WIS. STAT. § 895.507 Effective March 31, 2006	• Entity (person, other than an individual, but including state agencies) • Exempts persons subject to Gramm-Leach-Bliley Act	Acquired and there is a material risk of identity theft or fraud to the subject	No material risk of identity theft or fraud to the subject	• Affected Individuals • Owner or licensee of information • Credit Reporting Agencies, if greater than 1,000 persons affected		• Possibly; "Failure to comply with this section is not negligence or a breach of any duty, but may be evidence of negligence or a breach of a legal duty"

The above chart outlines security breach notification laws that apply to private sector entities. Oklahoma's breach notification law applies only to state agencies (Indiana's breach notification laws formerly only applied to state agencies as well but now include private sector entities as well). Oklahoma's breach notification law is listed below.

State	Entities Covered	Trigger For Notification	But Entities Do Not Have To Notify If:	Party to Whom Disclosure is Required	Substantive Requirement For Level Of Security?	Private Right Of Action For Violations Of The Statute?
Oklahoma Okla. Stat., tit. 74, § 3113.1	• State agencies	Acquisition		• Affected Individuals • Owner or licensee of information		• Does not specify