Volume 10 | Issue 1 Article 14

2006

Data Security and Data Breach Notification for Financial Institutions

Sean C. Honeywill

Data Security and Data Breach Notification for Financial Institutions

I. INTRODUCTION

With more than 45 million customer accounts compromised in less than eight months, the year of 2005 may come to be known as the year of the data breach.[1] Data losses at well known financial institutions, such as Bank of America, Citigroup, and Wachovia, as well as at data broker companies and third-party service providers, have caused the media, consumers, and the government alike to hone in on data protection measures.[2] The year started with ChoicePoint, a company that compiles consumer data for resale, reporting that thieves posing as legitimate customers had purchased the addresses, social security numbers, and credit reports of around 145,000 consumers.[3] Bank of America then reported losing backup tapes containing the personal account information of 1.2 million federal employees.[4] Next, DSW Shoe Warehouse reported that hackers stole credit and debit card, checking account, and driver's license numbers from a database for 108 of the chain's 175 stores, affecting 1.4 million customers.[5]

Various entities, ranging from LexisNexis, Ameritrade, Time Warner, and MCI reported data compromises next.[6] In May, Bank of

---

1. *See, e.g.,* Michael Dumiak, *Absent the Fort Knox Effect*, FIN. IT SECURITY, Sept. 2005, at 22. For a list of data breaches in 2005, see *A Chronology of Data Breaches Since the ChoicePoint Incident*, PRIVACY RIGHTS CLEARINGHOUSE, http://www.privacyrights.org/ar/ChronDataBreaches.htm (last visited Jan. 12, 2006) (summarizing data breaches beginning with the ChoicePoint incident in Feb. 2005).

2. Dumiak, *supra* note 1, at 23.

3. *Id.*

4. *Id.* Ironically, one of the consumers whose personal information was lost when Bank of America's backup tapes disappeared was Pat Leahy, Democrat-Vermont, a congressman who is leading the debate on whether more regulation of data brokers is needed and whose name is on a proposed breach notification bill. *See* Michael Sisk, *It Fell off the Truck*, FIN. IT SECURITY, Sept. 2005, at 12.

5. Steven Gray, *DSW Shoe Says Theft of Data Involved 1.4 Million Credit Cards*, WALL ST. J., Apr. 19, 2005, at B8.

6. *Without a Trace*, WALL ST. J. ONLINE, June 17, 2005 (subscription required; on file with author).

America and Wachovia reported that former employees had allegedly sold the data of 108,000 former and current customers to a third-party who then sold the information to collection agencies.[7] Citigroup then joined the data breach disclosure party in June when it reported that United Parcel Service had lost computer data tapes on 3.9 million customers while in transit to a credit bureau.[8] Two weeks later, Mastercard International topped everyone, disclosing that the credit card data of 40 million consumers had been compromised by an unidentified hacker at third-party credit processor CardSystems, which moves information for Visa, Mastercard, and American Express.[9]

The consequences of the misuse of such confidential customer information on consumers and the public are numerous - financial and criminal identity theft, family stress, public embarrassment, terrorism, and even murder.[10] In 2004 alone, 9.3 million Americans were the victims of identity theft.[11] And in terms of monetary harm, identity theft annually costs consumers $5 billion, and businesses and financial institutions $48 billion.[12] While the accidental loss of computer backup tapes was the major source of compromised data disclosures for financial institutions, the spill-over effect caused by the uproar from breaches at data brokers and third-parties is being felt by the financial industry, both in compliance costs and reputation damage.[13]

---

7. *Id.*

8. *See* Mitchell Pacelle, *UPS Loses Citigroup Customer Data*, WALL ST. J., June 7, 2005, at A3.

9. Dumiak, *supra* note 1, at 23.

10. *See Oversight Hearing on Data Security, Data Breach Notices, Privacy & Identity Theft Before the S. Comm. on Banking, Housing and Urban Affairs*, 109th Cong. 5 (2005) [hereinafter Testimony of Consumer & Privacy Groups] (testimony of Consumer and Privacy Groups on Security Breaches and Privacy), *available at* http://www.Consumersunion.org/pdf/IDTheft-Test0905.pdf. In one case, a man purchased a woman's work address online and then tracked her down and killed her. *See Hearing on Identity Theft & Data Broker Services Before the S. Comm. on Commerce, Science, & Transportation*, 109th Cong. (2005) (testimony of Mari J. Frank, Esq.), *available at* http://commerce.senate.gov/hearings/testimony.cfm?id=1491&wit_id=4254; *see also* IDENTITY THEFT RESOURCE CENTER, IDENTITY THEFT: THE AFTERMATH 2004 (2005), *available at* http://www.idtheftcenter.org/aftermath2004.pdf (studying the impact of identity theft on victims).

11. Bob Sullivan, *Study: 9.3 Million ID Theft Victims Last Year*, MSNBC, Jan. 26, 2005, http://msnbc.msn.com/id/6866768/.

12. FED. TRADE COMM'N, IDENTITY THEFT SURVEY REPORT 7 (2003), *available at* http://www.ftc.gov/os/2003/09/synovatereport.pdf.

13. *See, e.g.*, Dionne Searcey, *In 2003, California Passed its Security Breach Notice Law. Its Effect has Extended Well Beyond the State.*, WALL ST. J., July 18, 2005, at R6.

An issue that came to the forefront in 2005 is that data brokers,[14] companies that collect personal information from public and private records and then sell the information to both government and private entities, fall outside the scope of most current federal privacy regulations, including the Fair Credit Reporting Act[15] (FCRA) (applicable to consumer reporting agencies) and the Gramm-Leach-Bliley Act[16] (GLBA) (applicable to financial institutions).[17] And while some business entities had a legal duty to safeguard customer data, such as financial institutions under the GLBA, none had a legal duty to disclose data security breaches to consumers whose information may have been affected unless a state law mandated such.[18] Over twenty-one state legislatures passed data breach disclosure notification laws in 2005 as a response, causing a patchwork regulatory environment with which financial institutions, along with third-parties and data brokers, must comply.[19]

In Part II, this note explores the newfound focus on security measures being taken by financial institutions, and considers possible further innovations.[20] Part III concentrates on current federal and state

14. For a discussion of the data broker industry, see NATHAN BROOKS, DATA BROKERS: BACKGROUND & INDUSTRY OVERVIEW (2005), *available at* http://www.opencrs.com/rpts/RS22137_20050505.pdf. *See also* Daniel J. Solove & Chris Jay Hoofnagle, *A Model Regime of Privacy Protection (Version 2.0)*, (Geo. Wash. U. Law School Pub. Law Research Paper No. 132, 2005; Geo. Wash. U. Legal Studies Research Paper No. 132, 2005), at 5-10, *available at* http://ssrn.com/abstract=699701.

15. 15 U.S.C. § 1681 (2000). The FCRA defines a "consumer reporting agency" as an entity that regularly engages in "assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties." 15 U.S.C. § 1681a. It is possible, therefore, for a data broker to be subject to the requirements of the FCRA, but only to the extent they are providing "consumer reports." *See Hearing on Protecting Consumers' Data: Policy Issues Raised by ChoicePoint Before the Subcomm. On Commerce, Trade, and Consumer Protection of the H. Comm. on Energy and Commerce*, 109th Cong. 7-8 (2005) [hereinafter FTC ChoicePoint Testimony] (statement of the Fed. Trade Comm'n), *available at* http://www.consumer.gov/idtheft/pdf/ftc_03.15.05.pdf. For an overview of the FCRA and its application to data brokers, see *id.* at 6-10.

16. 15 U.S.C. §§ 6801-6827 (2000). To the extent that data brokers fall within the definition of "financial institutions" under the GLBA, they would be subject to the Act. FTC ChoicePoint Testimony, *supra* note 15, at 11; *see also* discussion *infra* Part III.A and accompanying notes.

17. *House & Senate Hold Hearings on Identity Theft & Data Protection Legislation*, PRIVACY LAW ALERT (Collier Shannon Scott, PLLC, Wash., D.C.), May 12, 2005, at 1, *available at* http://www.colliershannon.com/documents/IdentityTheftHearing.pdf.

18. *See, e.g.*, Searcey, *supra* note 13; *see also* discussion *infra* Part III.

19. *See, e.g.*, Searcey, *supra* note 13.

20. *See infra* notes 24-106 and accompanying text.

data security and breach disclosure legislation, as well as regulatory guidance affecting financial institutions.[21] Part IV examines possible aspects of a new federal data breach disclosure law, and the arguments for and against such features.[22] Part V concludes, summarizing the best case scenario for financial institutions regarding federal intervention in the data breach disclosure arena.[23]

II. THE BANKING INDUSTRY RESPONSE TO DATA BREACHES

Securing customers' data is not a one time problem with a single solution.[24] Because today's technology will be obsolete tomorrow, any security program must be flexible enough to adapt to change.[25] And while technical data protection methods have come to the forefront of discussions, other more traditional areas of security cannot be ignored.[26] This section examines three key components of data security in the current banking environment – information technology (IT), human resources, and consumer education.

A. Emerging Importance of Information Technology

Bank executives cannot ignore the IT department.[27] Media coverage of security mishaps harms a bank's brand image, which in turn

---

21. *See infra* notes 107-66 and accompanying text.

22. *See infra* notes 167-252 and accompanying text.

23. *See infra* notes 253-68 and accompanying text.

24. *See, e.g.*, Daniel Wolfe, *Wanted: Ways to Protect Online Data After the Login*, AM. BANKER, July 26, 2005, at 5A, *available at* 2005 WLNR 12091327.

25. The Federal Trade Commission has noted that "security is more a process than a state." *See* FED. TRADE COMM'N ADVISORY COMM., FINAL REPORT OF THE FTC ADVISORY COMMITTEE ON ONLINE ACCESS AND SECURITY 19 (2000), *available at* http://www.ftc.gov/acoas/papers/acoasfinal1.pdf.

26. *See* Susan Marks, *Data Security is an HR and an IT Issue*, AM. BANKER, Aug. 19, 2005, at 10, *available at* 2005 WLNR 13389233.

27. *See* Michael Grebb, *Changing of the Guard*, U.S. BANKER, July 1, 2005, at 40, *available at* 2005 WLNR 10363425. Financial institutions are hesitant to discuss what they do to monitor compromised accounts, likely to prevent giving people interested in committing fraud more information with which to work. *See* Robin Sidel & Mitchell Pacelle, *Credit-Card Breach Tests Banking Industry's Defenses*, WALL ST. J., June 21, 2005, at C1. However, this strategy can backfire because consumers feel more secure the more they know about how their personal information is being protected. *Id.*

lowers consumer confidence and use of the bank's products.[28] Before the days of data breach notification legislation, most banks would have a projected budget for financial loss due to breaches, and as long as that budget number was not exceeded, protecting data was not an issue.[29] But now, with the possibility of major harm to reputation, customer trust levels, and stock prices, executives take IT seriously.[30]

Financial institutions today focus much more on data security than in the past when data protection was handled solely by the IT department.[31] Now, it is not uncommon for executives from multiple areas to come together to discuss IT issues and how to better protect data.[32] As a result, the IT department is receiving more respect and a bigger budget.[33] For example, Wachovia has formed a Security and Identity Protection Committee, which includes executives from a cross-section of Wachovia's lines of business.[34] Another element of this greater focus on IT is that security vendors deal with higher-level executives rather than just those in the IT department.[35] By acknowledging that data security is an integral aspect of the whole financial institution, banks are taking a much needed step to better protect customer information.[36]

In terms of the actual technology being used, firewall software works hand in hand with the customer authentication process, and is standard security for a bank's online systems.[37] A firewall blocks unauthorized interactive access with a bank's network from individuals

28. *See, e.g.*, Press Release, Elec. Data Sys. Corp., Consumers Insist Financial Institutions Remain Vigilant In Protecting Their Privacy (Sept. 19, 2005), *available at* http://www.eds.com/news/news.aspx?news_id=2596 (indicating that thirty percent of consumers would close all accounts and move to another financial institution if their personal information was compromised).

29. Jeffrey Rothfeder, *Pressure Increases, But CIO's Still Struggle to Stop Identity Theft*, CIO INSIGHT, Sept. 9, 2005, http://www.cioinsight.com/article2/0,1540,1855955,00.asp.

30. *See* Grebb, *supra* note 27.

31. *Id.*

32. *Id.*

33. *Id.* Putting money into IT security can more than pay for itself in the money saved from fraud losses. *See* John Engen, *Intelligence Turned Inward*, FIN. IT SECURITY, Sept. 2005, at 18.

34. *See* Grebb, *supra* note 27.

35. *Id.*

36. *Id.*

37. *See* Michael Sisk, *Fixes on the Fly*, FIN. IT SECURITY, Sept. 2005, at 28.

or other networks.[38] To get beyond a firewall, one must provide some type of access right, which typically consists of the username and password combination.[39] Securing customer access rights is critical due to the fact that phishing, pharming, malware, and other compromise techniques are becoming prevalent in the financial industry.[40] This raises serious concerns because hackers in turn use such information to gain access to customers' online accounts, which contain more sensitive data and can thus perpetrate greater fraud.[41]

In October 2005, U.S. regulators ordered banks to improve security measures to reliably authenticate customers accessing internet services, giving them until the end of 2006 to implement such methods.[42] The "Federal Financial Institutions Examination Council – an umbrella group of [federal banking] regulators – said that the use of single-factor authentication, such as user name and password, [is] inadequate for safeguarding against account fraud and identity theft . . . [and] banks should [instead rely on] dual-factor authentication."[43] Dual authentication allows the user to be sure that the website is legitimate and not set up as part of a scam, and permits the bank to authenticate the customer's identity.[44]

---

38. *See* Wolfe, *supra* note 24. For a layman's description of a firewall, see http://www.firsttennessee.com/index.cfm?Fuseaction=Potpourri.ViewContent&Item=OnlineSecurity (last visited Jan. 12, 2006) (likening the firewall access process to that of a safety deposit box).

39. *See* Wolfe, *supra* note 24.

40. *See* FED. FINANCIAL INSTITUTIONS EXAMINATION COUNCIL, AUTHENTICATION IN AN INTERNET BANKING ENVIRONMENT 4 (2005), *available at* http://www.ffiec.gov/pdf/authentication_guidance.pdf. Pharming is similar in nature to e-mail phishing, and seeks to obtain personal information by directing users to fake web sites where their information is then gathered on legitimate looking forms for the purpose of committing fraud. *Id.* at n.7. Malware is short for malicious software, such as software designed to capture and forward private information such as ID's, passwords, account numbers, and access codes. *Id.* at n.8. *See generally* AARON EMIGH, IDENTITY THEFT TECH. COUNCIL, ONLINE IDENTITY THEFT: PHISHING TECHNOLOGY, CHOKEPOINTS AND COUNTERMEASURES (2005), *available at* http://www.antiphishing.org/Phishing-dhs-report.pdf (detailing the technologies being used by online identity thieves and the possible tools that can be used to reduce financial losses from such attacks).

41. *See* FED. FINANCIAL INSTITUTIONS EXAMINATION COUNCIL, *supra* note 40.

42. *Id.*; *see also* Steven Marlin, *Feds Order Banks to Strengthen Online Authentication*, BANK SYSTEMS & TECH. ONLINE, Oct. 18, 2005, http://www.banktech.com/showArticle.jhtml;jsessionid=JNYKCGMTXSELYQSNDBECKHSCJUMEKJVN?articleID=172302371.

43. Marlin, *supra* note 42.

44. *See, e.g.*, *id.*

As the name suggests, dual factor authentication adds a second security method, usually something the account user has in his/her possession, to the standard practice of requiring a username and password to log into a secure website.[45] The additional layer of security typically takes the form of a security token, a device that can attach to a key chain and displays different numerical digits every minute.[46] "Users simply [add] the number [to] the end of their [login] passwords when signing in to their accounts to gain access. The device foils perpetrators who manage to steal passwords and IDs because the sign-in process cannot be completed without the numbers generated by the security token."[47]

Bank of America was the first large financial institution to adopt such technology in May 2005 with SiteKey.[48] Uniquely, SiteKey provides two factor authentication without requiring the customer to carry any kind of security token by instead using the customer's personal computer (PC) as the second-factor hardware device.[49] SiteKey requires customers to "pick an image, write a brief phrase, and select three challenging questions."[50] The customer and the bank can then pass this information back and forth to confirm each other's identity.[51] If the customer attempts to login from another PC, the system will seek answers to the three challenging questions before

45. Press Release, PassMark Security, PassMark Delivers the Internet's First Two-Factor, No Hardware Authentication System (Feb. 3, 2005), *available at* http://news.thomasnet.com/fullstory/460273.

46. Jim Middlemiss, *CIO Challenge: Two-Factor Authentication*, WALL ST. & TECH., Apr. 27, 2005, http://www.wallstreetandtech.com/showArticle.jhtml?articleID=161600915.

47. *Id.*

48. Press Release, Bank Of Am., Bank of America Announces Industry-Leading Security Feature for its 13.2 Million Online Banking Customers to Help Prevent Fraud and Identity Theft (May 26, 2005), *available at* http://www.bankofamerica.com/newsroom/press/press.cfm?PressID=press.20050526.03.htm. Stanford Federal Credit Union of Palo Alto, Cal., was the first to utilize the SiteKey technology. *See* Wolfe, *supra* note 24.

49. Press Release, PassMark Security, *supra* note 45.

50. Press Release, Bank Of Am., *supra* note 48.

51. *Id.* The SiteKey approach still relies on the storage of each customer's unique identifier on the merchant's database. *See* Trevor Zion Bauknight, *PassMark's SiteKey – Answering the Wrong Question*, CAFE ID, http://www.cafeid.com/art-sitekey.shtml (last visited Jan. 12, 2006). Compromise of this data would leave the consumer just as vulnerable as they would be if their username and password were obtained. *Id.* Further, even though the PassMark system is better at securing customer information than the login/password authentication scheme, it is still possible that a consumer could lose or reveal their "secret question" answers to a hacker. *Id.*

allowing access to the online account.[52] In October 2005, Wachovia announced plans to pilot a similar dual certification system, with the hope of launching the service for its 3 million online customers in 2006.[53]

Taking dual certification technology one step further, SiteKey developer PassMark Security Inc. has developed a new system that will monitor customers after they have passed the login test, and alert the bank if suspicious activity occurs after login.[54] The technology also allows banks to monitor their employees' habits by checking for changes in network settings and tracking if any employee is abusing his/her data access rights.[55] This type of technology not only lessens the possible harm if a security breach occurs by allowing the bank to discover the breach faster, but also helps banks create audit trails in real time, alleviating bank employees from having to dig through logs and manually perform such tasks.[56] The emergence of such software reflects the financial industry's concern that hackers that steal

52. Lindsay Clarke, *Bank of America to Use Two-Factor System to Beat Phishers*, COMPUTER WKLY., May 27, 2005, http://www.computerweekly.com/Articles/2005/05/27/210196/BankofAmericatousetwo-factorsystemtobeatphishers.htm.

53. Will Boye, *Wachovia to Pilot Test Online Security Feature*, CHARLOTTE BUS. J., Sept. 30, 2005, http://www.bizjournals.com/charlotte/stories/2005/10/03/newscolumn3.html?from_rss=1. While the dual authentication systems are currently the leading standard in the industry, a three factor system would be even safer. *See* Wolfe, *supra* note 24. However, a three factor system would require a finger scan or iris scan, something that most home computers currently do not have the capability to read. *Id.* For a more in depth discussion of fingerprint and eye scanning technology and banks, see James Hannah, *Privacy Concerns, Expense Keep Biometrics Out of U.S. ATMs*, Oct. 13, 2005, http://www.securityinfowatch.com/online/Financial/Privacy-Concerns—Expense-Keep-Biometrics-Out-of-U.S.-ATMs/5933SIW339.

54. *See* Wolfe, *supra* note 24.

55. Daniel Wolfe, *War on Fraud Focusing on the Insider Front*, AM. BANKER, Mar. 31, 2005, at 17, *available at* 2005 WLNR 5379835; *see also* discussion *infra* Part II.B.

56. *See* Sisk, *supra* note 37, at 29. First Citizens Bank, based in Raleigh, NC., uses Covelight Solutions' Percept for its online business banking application to help identify suspicious activity. *Id.* Software maker Corillian Corp. launched its Intelligent Authentication package on October 25, 2005, which tracks the behavior of online-banking customers and builds histories of their habits, such as the computers the customer uses and the normal time of day and geographic location from which the customer logs in from. Riva Richmond, *Banks Seek Better Online-Security Tools*, WALL ST. J., Dec. 1, 2005, at B4. "Corillian . . . has sold the technology to three credit unions and says it is in talks with three of the top-ten U.S. banks." *Id.* On November 8, 2005, software maker Entrust Inc. unveiled a new version of its IdentityGuard product that offers a menu of user-verification methods banks can choose to secure transactions they deem risky, which Miami-based Commercebank NA employs. *Id.*

consumers' account information could hurt online banking, which is valued by banks as a low cost way of doing business.[57]

Another method to increase online security involves encrypting as much as possible behind firewalls.[58] Encryption software "automatically encodes and decodes . . . information [marked sensitive and confidential on financial institutions' servers and databases] as it moves among different PCs on the network, thus rendering the files unreadable to hackers."[59] For example, when a customer types in a username and password on a bank's online banking webpage, that information will be encrypted before being sent over the internet to the bank's network.[60] While using encryption technology on communications between a customer's PC and the bank is standard practice in the industry, encrypting all information is not, because while encryption itself is easy, the keys to read the data can be very difficult to manage.[61]

Recent data breaches have exposed this point and turned the focus of encryption efforts to another area of stored customer data.[62] Most companies copy computer data onto backup tapes for storage with third-party vendors in the event of a disaster.[63] However, only six percent of financial service companies encrypt all backup tapes, primarily due to the high cost and technical difficulties of doing so.[64] But with many of the reported data breaches involving lost unencrypted

57. Richmond, *supra* note 56.

58. Matthew de Paula, *California Law Holds Firms Responsible for Breaches*, U.S. BANKER, Apr. 1, 2005, at 11, *available at* 2005 WLNR 5104784.

59. Jeffrey Rothfeder, *Recipe for Foolproof Encryption*, CIO INSIGHTS, Sept. 5, 2005, http://www.cioinsight.com/article2/0,1540,1855963,00.asp. The top three U.S. credit reporting companies recently announced they would adopt a single encryption standard to better protect the huge amounts of sensitive electronic data they receive everyday from data furnishers, including banks. *Credit Reference Agencies Agree on Encryption Standard*, CARDLINE, Oct. 7, 2005, *available at* 2005 WLNR 16292028. This shows how important protecting customer data has become in light of security breaches, as the three companies are traditionally rivals competing for business. James B. Kelleher, *Credit Cos to Adopt One Data Protection Standard*, REUTERS, Sept. 22, 2005, http://findarticles.com/p/articles/mi_zdpcm/is_200509/ai_n15614818.

60. *See* Rothfeder, *supra* note 59.

61. *See* Sisk, *supra* note 37, at 29. Burt Kaliski, vice president of research and chief scientist at RSA Laboratories, predicts that within ten years, all sensitive data will be encrypted as managing data becomes easier due to technology advances. *Id.*

62. *See, e.g.*, Jon Swartz, *Data Losses Push Businesses to Encrypt Backup Tapes*, USA TODAY, June 13, 2005, at B1, *available at* 2005 WLNR 9341385.

63. *Id.*

64. *Id.*

backup tapes, financial institutions are taking the necessary measures to prevent similar occurrences in the future.[65] Bank of America and Citigroup, for instance, are eliminating backup tapes where possible and transitioning to computer-to-computer data transfers.[66] They are also testing encryption for any backup tapes that will still be used.[67]

B. Human Component of Data Security

All available security and encryption efforts do little good if employees with the encryption codes or with daily access to customer personal information are careless, or worse yet, commit fraudulent or criminal activities.[68] Thus, human resources are just as critical a part of the data security solution as technical resources.[69] In fact, insiders – employees, third-parties under contract, and others – are the major source of fraud-related losses for banks.[70] The number of thefts by insiders has risen in recent years, with the incurring ease that technology provides for moving information.[71] Insiders are involved in an estimated seventy percent of security incidents,[72] which result in average damages when committed against a large company of $2.7 million, compared to only $57,000 in average damages when an outsider commits the breach.[73] For example, in New Jersey, branch managers and other employees at Bank of America, Wachovia, and

65. *Id.* Encryption of customer information can add another benefit for financial institutions – if encrypted data is stolen, the institution is not required to report it under California's breach notification act and many of the other state breach notification laws, thus leading to speculation that Bank of America's lost backup tapes were in fact not encrypted. *See, e.g.*, Clint Boulton, *Bank Data Leak Jump-Starts Encryption Talk*, INTERNET NEWS, Mar. 2, 2005, www.internetnews.com/ent-news/article.php/3486786.

66. *See* Isabelle Lindenmayer, *Amro Unit: Loan Data Tapes Lost*, AM. BANKER, Dec. 19, 2005, at 1, *available at* 2005 WLNR 20863883.

67. *Id.*

68. *See* Michele Heller, *Competing Data Security Bills Near Introduction*, AM. BANKER, June 9, 2005, at 1, *available at* 2005 WLNR 9505863.

69. *See* Marks, *supra* note 26.

70. *See* Holly Sraeel, *Want to Make a CEO Wince? Talk About Fraud*, US BANKER, July 2005, at 8, *available at* 2005 WLNR 10363407.

71. Wolfe, *supra* note 55. Additionally, there is more demand for consumer information today on the black market, making it easier to profit from such acts than in the past when one had to have their own methods for using the stolen data in place. Isabelle Lindenmayer, *FBI Report Underscores Insider Data-Theft*, AM. BANKER, Nov. 29, 2005, at 10, *available at* 2005 WLNR 19563075.

72. *Stats, The Industry Snapshot*, FIN. IT SECURITY, Sept. 2005, at 8.

73. *Id.*

Commerce Bank were alleged to have assisted an outsider in stealing private information from 500,000 customer bank accounts, selling it to bill collectors for a reported profit for the insiders of $10 per affected account.[74]

Even honest employees with the best of intentions can severely hurt a bank.[75] One study found that ninety-five percent of all data loss incidents were unintentional and usually the result of careless or untrained employees.[76] Thus, simple security measures such as proper training can be especially important for employees who might not otherwise understand the risks stemming from certain actions.[77] Additionally, many bank employees must handle customer information in the normal course of business.[78] To lessen the risk of misuse of data in these normal situations, banks are required to conduct background checks on all employees who will have access to customers' personal information, and are prohibited by federal law from employing persons who have been convicted of certain crimes.[79]

To further protect data, financial institutions are also setting up stricter access protocols to limit the ability of employees and outsiders from obtaining sensitive customer information.[80] E*Trade Financial, for example, is setting up protocols "to heavily restrict what customer data is available to customer-service representatives."[81] Along the same lines, some banks are establishing protocols to make customer

74. Tom Costello, *Massive Bank Security Breach Uncovered in N.J.*, MSNBC, Apr. 28, 2005, http://www.msnbc.msn.com/id/7670774.

75. *See* VONTU, INC., DATA SECURITY TRENDS 2004, at 2 (2004), *available at* http://www.vontu.com/uploadedFiles/global/VontuDataSecurityTrends2004.pdf.

76. *Id.* The human resource component includes destroying confidential information properly. *See* Todd Davenport, *Breaches, Credibility, and Agencies. With Data Security 'the New BSA,' Banks Need to Adapt*, AM. BANKER, July 28, 2005, at 1, *available at* 2005 WLNR 12220143. For example, a customer found intact loan files in a dumpster outside a First Horizon Home Loan office in Fairfax, VA., which employees should have shredded. *Id.* In April 2005, Wells Fargo alerted a small number of customers that their personal information may have gone astray "due to an envelope stuffing error." *See* David Lazarus, *Wells Fargo's Snafu in Stuffing Envelopes*, S.F. CHRON., May 8, 2005, at E1, *available at* http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2005/05/08/BUGP7CKKEB1.DTL&feed=rss.business; *see also infra* notes 118-19 and accompanying text.

77. *See* Grebb, *supra* note 27.

78. *See, e.g.*, Kelly Shermach, *Technology Can't Fix Trust Breach*, CRM BUYER, June 6, 2005, http://www.crmbuyer.com/story/43721.html.

79. *See* 12 C.F.R. pt. 30 App. B, pt. III.C.1.e (2005); *see also* 12 U.S.C. § 1829 (2000).

80. *See* Grebb, *supra* note 27.

81. *Id.*

information less usable (and thus less valuable), such as a recent Wachovia initiative to end the use of social security numbers for customer authentication.[82] Such measures have the additional benefit of reducing the chance of having to report a breach, since eliminating data means less exposure to criminals attempting to breach a financial institution's network.[83] To test such protocols, outside security experts are hired to attempt unauthorized attacks to assess the vulnerability of a bank's data protection measures.[84]

Banks also look beyond their own physical perimeters to scrutinize the data protection measures of third-party marketing companies that receive data from the banks to assist in selling products to the customers.[85] The GLBA provides that, in certain circumstances, if information is going to be shared with non-affiliates of the financial institution, the customer must be notified of this sharing and given an opportunity to "opt out."[86] As a result, nine of the top fifteen U.S banks have adopted privacy policies that prohibit sharing customer information with third-parties, and thus do not have to provide the "opt out" procedure.[87] This is important because often third-parties are less careful about protecting confidential information than the financial institution.[88] For instance, in June 2005 hackers stole forty-million MasterCard and Visa accounts from CardSystems Solutions Inc., a

82. *Id.*

83. *See* Michele Heller & Isabelle Lindenmayer, *Call to Make Stolen Data Less Usable*, AM. BANKER, Aug. 1, 2005, at 1, *available at* 2005 WLNR 12344688.

84. *See* Grebb, *supra* note 27.

85. *Id.*

86. 15 U.S.C. § 6802(b) (2000).

87. de Paula, *supra* note 58. There is still an exception, however, that allows even institutions that have adopted a privacy policy that prohibits sharing of customer information (and therefore have no "opt out" procedure in place) to give out customer information to nonaffiliated third parties "to perform services for" the financial institution or to jointly market products to the institution's customers. 15 U.S.C. § 6802(b)(2). The GLBA does, however, provide limits on the reuse of such information and on sharing account numbers for marketing information. 15 U.S.C. § 6802(c) & (d). Additionally, there does have to be disclosure of the joint marketing exception in the company's privacy notice. 15 U.S.C. § 6803; *see also* discussion *infra* notes 119-21 and accompanying text.

88. Rothfeder, *supra* note 59. For the third time in 2005, Bank of America reported losing confidential customer information, when a laptop containing information was stolen from a third-party "service provider" on August 29, 2005. *See* Martin H. Bosworth, *Bank of America Loses Customer Data Again*, CONSUMERAFFAIRS.COM, Oct. 12, 2005, http://www.consumeraffairs.com/news04/2005/bofa_laptop.html.

third-party that processed credit transactions between merchants and banks.[89]

Despite the above, studies on the security initiatives of financial institutions continue to show that training and awareness of employees falls well behind technical solutions and compliance for methods of combating data security breaches.[90] While some banks do realize the importance that humans play in data security, others must accept the fact that even though human capital may be more costly than automated machines, to ignore the human component of security will result in a greater expense to both the consumer and bank in the long run.[91]

C. *Consumer Education*

Yet another aspect that is critical to the success of a bank's security program is educating consumers about the actual risks of identity theft, especially in the online environment.[92] Most identity theft occurs offline from the interception of paper documents, although the perception among consumers is that online transactions pose a greater risk of identity theft.[93] Banks should counteract these misconceptions so they will not lose online banking customers and profits, as face to face human interaction is far more expensive than automated computer transactions.[94] "For example, a bill sent electronically costs about half of what a bill costs when sent through regular mail."[95]

---

89. Rothfeder, *supra* note 59. Visa and Mastercard both require companies they deal with to encrypt data transmissions, but CardSystems ignored the rule, something that is not uncommon. *Id.*

90. *See* Ciaran Buckley, *Internal Security Attacks Affecting Banks*, ELECTRICNEWS.NET, June 22, 2005, http://www.electricnews.net/news.html?code=9614655.

91. *See* Grebb, *supra* note 27.

92. Nowadays, when people think of identity theft, they usually think of computers. *See* Davenport, *supra* note 76. However, a January 2005 study conducted by Javelin Strategy and Research found that in known identity theft cases, the information was obtained online in only 11.6% of the cases. *Id.*

93. *Id.*

94. Press Release, Gartner, Gartner Survey Shows Frequent Data Security Lapses and Increased Cyber Attacks Damage Consumer Trust in Online Commerce (June 23, 2005), *available at* http://www.gartner.com/press_releases/asset_129754_11.html.

95. *Id.* Studies show the misconception is taking hold. A Gartner survey of 5,000 U.S. adults found that seventy-three percent regularly logged on to banking accounts and sixty-three percent paid bills online. *Id.* However, thirty percent of those that bank online reported that recent data attacks have influenced their online banking activities, with over three-quarters of this group logging on less frequently, and nearly fourteen percent ceasing online bill payment altogether. *Id.* This decline in consumer online banking shows a failure

Consumers should be aware that banks do not call or email customers and ask them for their personal information.[96] And to encourage online account use, banks should better promote the fact that they do not hold customers liable for any unauthorized use of the customer's account.[97] For instance, both Bank of America and Wachovia guarantee full reimbursement for any unauthorized activity if notified within sixty days of the date the unauthorized activity shows up on a customer's bank statement.[98] Furthermore, studies show that those who bank online are able to catch unauthorized activity quicker, thus leading to less financial harm than those who bank by traditional methods.[99] If consumers were aware that identity theft is less likely to occur online than offline, and that they would not be liable for unauthorized access to their online accounts, both the bank and customer would benefit.[100] Banks also need to highlight new security features, such as dual authentication, and convince customers that any inconvenience presented by the new technology is offset by the greater protection provided.[101] From a marketing perspective, a bank can use

---

of banks to educate consumers that online banking is more secure than traditional paper methods. Daniel Wolfe, *Fear of Data Theft Hurting Site Traffic, Surveys Find*, AM. BANKER, June 28, 2005, at 9, *available at* 2005 WLNR 10436975.

96. Isabelle Lindenmayer, *Data Breaches Remaking Organizations, Processes*, AM. BANKER, Sept. 27, 2005, at 1, *available at* 2005 WLNR 15943452. According to a report by Javelin Strategy and Research, Bank of America Corp., Citigroup Inc., E-Trade Bank, Washington Mutual Inc., and Wells Fargo & Co. are the top five banking companies in regards to protecting and educating their online customers about identity fraud. Isabelle Lindenmayer, *Security Watch*, AM. BANKER, Jan. 6, 2006, at 5, *available at* 2006 WLNR 671797.

97. *See* Isabelle Lindenmayer, *Data Breaches Remaking Organizations, Processes*, AM. BANKER, Sept. 27, 2005, at 1, *available at* 2005 WLNR 15943452.

98. Bank of Am. Corp., http://www.bankofamerica.com/onlinebanking/index.cfm?template=security (last visited Jan. 12, 2006) (discussing the bank's "$0 Liability Guarantee"); Wachovia Corp., www.wachovia.com/customerprotection/0,,7650_7657,00.htm (last visited Jan. 12, 2006) (discussing the bank's "Online Services Guarantee"). The sixty day time-frame is even longer than provided by law for forged or stolen checks pursuant to U.C.C. § 4-406 (amended 2002) and N.C. GEN. STAT. § 25-4-406 (2005), which allow the customer an amount of time not exceeding thirty days after receiving a statement to report unauthorized activity.

99. *See* Holly Sraeel, *Tackling ID Theft: Will the Real Jane Doe Stand Up?*, US BANKER, Mar. 1, 2005, at 8, *available at* 2005 WLNR 3098725.

100. *See id.*

101. *See, e.g.*, Larry Ponemon, *Trust in Online Banking: Hard to Earn, Easy to Lose*, COMPUTERWORLD, Apr. 26, 2005, http://www.computerworld.com/securitytopics/security/story/0,10801,101341,00.html (noting that more than seventy-one percent of the respondents to the 2005 Privacy Trust Survey for Online Banking conducted by Ponemon Institute cited convenience as their top reason for banking online). While new security

such security to show how much it values privacy and possibly gain market share along with customer trust.[102]

While recent breaches are creating some misconceptions about the security of online banking, at least they are helping to educate the public.[103] This education by default should shed light on areas where banks have no control, such as how important it is for consumers to have virus software and firewalls installed on their personal computers.[104] In turn, the potential for online fraud will decrease as both banks and personal computer systems become more secure.[105] Ensuring 100% data security is an ideal financial institutions can only strive for, but those that integrate technology, human resources, and consumer education will be in the best position to avoid costly breaches.[106]

III. FEDERAL AND STATE LEGISLATION REGULATING SECURITY BREACH NOTIFICATION

Even with the best security measures, data breaches still can occur.[107] Thus, banks should also devote resources towards developing a breach notification policy that complies with applicable laws and regulations, and is as customer-friendly as possible.[108]

---

features are more secure, they are also more cumbersome (albeit only marginally so) to maneuver than traditional security methods, such as single authentication. *See* Wolfe, *supra* note 24.

102. *See, e.g.*, John Engen, *Intelligence Turned Inward*, FIN. IT SECURITY, Sept. 2005, at 18.

103. *See* Holly Sraeel, *Secure Times? Define Secure.*, FIN. IT SECURITY, Sept. 2005, at 6.

104. *See* Wolfe, *supra* note 24.

105. *Id.*

106. *See* Marks, *supra* note 26.

107. *See Hearing on Protecting our Nation's Cyberspace Before the Subcomm. On Tech., Info. Policy, Intergovermental Relations, and the Census of the H. Comm. on Gov't Reform*, 109th Cong. 5 (2004) (statement of the Fed. Trade Comm'n), *available at* http://www.ftc.gov/os/2004/04/042104cybersecuritytestimony.pdf.

108. *See Data Breaches Bad for Business*, CONSUMERAFFAIRS.COM, Sept. 27, 2005, http://www.consumeraffairs.com/news04/2005/data_breaches_business.html (explaining that companies need to clearly communicate what effect the security breach will have on customers' personal information, and those that do not are four times more likely to experience customer turnover as a result). *See generally* Tracy Mayor, *Breach Brigade: When Bad Things Happen to Your Enterprise, You'll Need a Team and a Process in Place to Help You Survive the Hot Glare of Media Scrutiny*, CSO MAGAZINE, Feb. 2004, http://www.csoonline.com/read/020104/response.html?action=print.

A. *Federal Data Security for Financial Institutions: Gramm-Leach-Bliley Act*

The purpose of the GLBA[109] was to reform and modernize the banking industry by creating financial entities authorized to conduct various financial activities within the same holding company, including banking, securities brokering, and insurance, and to control how financial institutions handled the nonpublic personal information of customers.[110] Title V of the GLBA states that "each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information."[111] To promote this obligation, the GLBA directed the agencies responsible for enforcement of the GLBA to establish appropriate standards and rules for financial institutions to adhere to.[112]

The federal banking regulatory agencies and the Federal Trade Commission (FTC) implemented comparable regulations for entities under their jurisdictions, including the Interagency Guidelines Establishing Information Security Standards[113] (Security Guidelines)

---

109. 15 U.S.C. §§ 6801-6827 (2000), *available at* http://www.steptoe.com/publications/PI6434.pdf.

110. *See, e.g.*, 67 Fed. Reg. 36,484 (May 23, 2002), *available at* http://www.ftc.gov/os/2002/05/67fr36585.pdf (discussing the history of the GLBA in 'preamble Section A: Background'). Under the GLBA, a "financial institution" is defined as an entity that engages in one or more of the specific activities listed in the Bank Holding Company Act and its implementing regulations. *See* 15 U.S.C. § 6809(3). These activities include traditional banking, extending credit, brokering loans, financial advising, and credit reporting. *See* 12 U.S.C. § 1843(k) (2000).

111. 15 U.S.C. § 6801(a).

112. *See* 15 U.S.C. §§ 6801(b), 6805(b)(2). The agencies responsible for establishing the standards were: The National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), the Board of Governors of the Federal Reserve System (Board), the Federal Deposit Insurance Corporation (FDIC), the Office of Thrift Supervision (OTS), the Secretary of the Treasury (Treasury), the Securities and Exchange Commission (SEC), and the Federal Trade Commission (FTC). *See* 15 U.S.C. § 6804. The purpose of the standards was "to insure the security and confidentiality of customer records and information, to protect against any anticipated threats or hazards to the security or integrity of such records, and to protect against unauthorized access to or use of such records or information which would result in substantial harm or inconvenience to any customer." 15 U.S.C. § 6801(b)(1)-(3).

113. 12 C.F.R. pt. 30, App. B (2005) (OCC); 12 C.F.R. pt. 208, App. D-2 and pt. 225, App. F (Board); 12 C.F.R. pt. 364, App. B (FDIC); 12 C.F.R. pt. 570, App. B (OTS). For a copy of the Federal Register Notice that contains the final Security Guidelines, see http://www.steptoe.com/publications/PI9188.pdf.

and Safeguards Rule,[114] respectively. The standards stipulate that financial institutions must design and implement written security programs to protect the nonpublic personal information of customers.[115] A key aspect of the regulations is flexibility, which allows institutions to decide how best to protect customer information within a certain outlined framework.[116] At the end of 2004, the federal banking agencies amended the Security Guidelines to include requiring financial institutions to develop appropriate measures to dispose of consumer information derived from consumer reports, implementing section 216 of the Fair and Accurate Credit Transactions Act of 2003[117] (FACT Act).[118]

In addition, financial institutions are prohibited by the GLBA from disclosing nonpublic personal information to non-affiliated third parties without first providing consumers with notice and the opportunity to opt out of such disclosure.[119] The GLBA provides, however, "a number of statutory exceptions under which disclosure is permitted without specific notice to the consumer . . . includ[ing] consumer reporting (pursuant to the FCRA), fraud prevention, law enforcement and regulatory or self-regulatory purposes, compliance

114. 16 C.F.R. pt. 314 (2005). For a copy of the Federal Register Notice that contains the final Safeguards Rule, see http://www.ftc.gov/os/2002/05/67fr36585.pdf. The Securities and Exchange Commission also adopted a final safeguards rule as part of its Privacy of Consumer Financial Information Final Rule. *See* 17 C.F.R. pt. 248 (2005).

115. *See, e.g.*, 12 C.F.R. pt. 30, App. B. To the extent that a data broker falls within the definition of "financial institution" under the GLBA, it must maintain such security measures for customer information. *See* FTC ChoicePoint Testimony, *supra* note 15, at 14.

116. *See, e.g.*, FED. TRADE COMM'N, FINANCIAL INSTITUTIONS AND CUSTOMER DATA: COMPLYING WITH THE SAFEGUARDS RULE (2002), http://www.ftc.gov/bcp/conline/pubs/buspubs/safeguards.pdf (explaining how regulated entities can comply with the Safeguards Rule).

117. 15 U.S.C.A. § 1681w (2005). Section 216 of the FACT Act is designed to protect consumers against the risks associated with identity theft and fraud. Letter from Fed. Deposit Ins. Corp. to FDIC-Supervised Banks (Commercial and Savings) (Feb. 2, 2005), *available at* http://www.fdic.gov/news/news/financial/2005/fil705.pdf.

118. *See* 69 Fed. Reg. 77,610 (Dec. 28, 2004) (to be codified at 12 C.F.R pt. 30, App. B (OCC); 12 C.F.R. pt. 208, App. D-2 and pt. 225, App. F (Board); 12 C.F.R. pt. 364, App. B (FDIC); 12 C.F.R. pt. 570, App. B (OTS)), *available at* http://www.fdic.gov/regulations/laws/federal/04jointfact.pdf. The amended Security Guidelines took effect July 1, 2005. *Id.*

119. FTC ChoicePoint Testimony, *supra* note 15, at 11; 15 U.S.C. § 6802; *see also* BUREAU OF CONSUMER PROT. DIV. OF FIN. PRACTICES, FED. TRADE COMM'N, THE GRAMM-LEACH-BLILEY ACT PRIVACY OF CONSUMER FINANCIAL INFORMATION, http://www.ftc.gov/privacy/glbact/glboutline.pdf (last visited Jan. 12, 2006) (explaining the privacy provisions of the GLBA).

with judicial process, and public safety investigations."[120] "Entities that receive information under . . . [a GLBA exception] are subject to . . . reuse and redisclosure restrictions . . . even if those entities are not themselves financial institutions."[121]

Service providers of financial institutions are not specifically monitored by the agencies responsible for enforcing the GLBA.[122] However, the agencies direct financial institutions to oversee their service providers by taking appropriate steps to ensure the service providers are capable of protecting customer information and by requiring the service providers, by contract, to implement and maintain safeguards that satisfy the objectives of the GLBA.[123]

While the GLBA addresses financial institutions' duties to protect customer information, the Act contained no specific mandates concerning a duty to notify customers whose nonpublic personal information was compromised.[124] Nor did the standards implemented by the agencies directly address the issue.[125] And while the GLBA preempts state laws that are inconsistent with its provisions, state legislation that provides greater protection than the GLBA is not considered to be inconsistent.[126] This opened the door for states to pass their own breach notification laws, such as was done in California.[127]

120. FTC ChoicePoint Testimony, *supra* note 15, at 11 (citing 15 U.S.C. § 6802(e)).

121. FTC ChoicePoint Testimony, *supra* note 15, at 11 (citing 16 C.F.R. § 313.11(a)). Data brokers may receive some of their information from credit reporting agencies, such as credit header data that includes a consumers name, address, and social security number. FTC ChoicePoint Testimony, *supra* note 15, at 12. "Because credit header data is typically derived from information originally provided by financial institutions, data brokers who receive this information are limited by the GLBA's reuse and redisclosure provision." *Id.*

122. *See, e.g.*, 12 C.F.R. pt. 30, App. B (2005).

123. *Id.* Even though monitoring service providers is the primary responsibility of the financial institution, regulators do have authority to examine them. *See* Michele Heller, *Agencies: No New Bank-Data Laws*, AM. BANKER, May 19, 2005, at 4, *available at* 2005 WLNR 8288917; *see also* Damian Paletta & Michele Heller, *Lenders Demand Closer Scruitiny of Data Processors*, AM. BANKER, June 24, 2005, at 3, *available at* 2005 WLNR 10306989 (calling for regulators to better scrutinize the third-party processors that banks use).

124. *See* 15 U.S.C. §§ 6801-6827 (2000).

125. *See, e.g.*, 12 C.F.R. pt. 30, App. B (2005).

126. *See* 15 U.S.C. § 6807.

127. *See* CAL. CIV. CODE § 1798.82 (West 2005), *available at* http://www.privacy.ca.gov/code/cc1798.291798.82.htm#two.

B. State Breach Notification Legislation

On July 1, 2003, California Senate Bill 1386 (SB 1386) became the first breach notification law in the country.[128] California's law applies to any person or business that conducts business in California and that owns or licenses computerized data that includes personal information.[129] As defined by the California law:

> "personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or data elements are not encrypted: (1) Social Security number. (2) Driver's license number or California Identification Card number. (3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.[130]

"Personal Information" does not include publicly available information, such as government records.[131]

The California law calls for disclosure of any breach of the unencrypted personal information of any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.[132] Notice of the breach has

---

128. CAL. CIV. CODE § 1798.82. For a more in depth discussion of the history of California SB 1386, see generally Timothy H. Skinner, *California's Database Breach Notification Secuirty Act: The First State Notification Law is Not Yet a Suitable Template for National Identity Theft Legislation*, 10 RICH. J.L. & TECH. 1, 12-19 (2003).

129. CAL. CIV. CODE § 1798.82.

130. *Id.*

131. *Id.*

132. *Id.* Under guidance issued by the California Office of Privacy Protection, a variety of factors can be considered in determining whether information has been "acquired," including (1) indications that protected data is in the physical possession and control of an unauthorized person (such as a lost or stolen computer or other device); (2) indications that protected data has been downloaded or copied; or (3) indications that protected data has been used by an unauthorized person, such as to open new accounts. CAL. OFFICE OF PRIVACY PROT., CAL. DEP'T OF CONSUMER AFFAIRS, RECOMMENDED PRACTICES ON NOTIFICATION OF SECURITY BREACH INVOLVING PERSONAL INFORMATION 11 (2003), *available at* http://www.privacy.ca.gov/recommendations/secbreach.pdf.

to be made without unreasonable delay in the most expedient way, but may be withheld if the notice would impede a criminal investigation or if measures are necessary to restore the integrity of the data system before the breach is made public.[133] Acceptable methods of providing the notice include written notice and electronic notice.[134] However, if the cost of providing the notice exceeds $250,000 or the number of people to be notified exceeds 500,000, substitute notice consisting of email, a posting on the businesses' website, and notification of major statewide media will suffice.[135]

California's law has been credited as the reason companies that suffered security breaches in 2005 notified affected customers, thus propelling the issue into the national spotlight.[136] In fact, data brokers admitted in testimony before Congress that prior to SB 1386, they simply did not inform consumers of breaches and the resulting possibility of identity theft.[137] But with the onslaught of attention being given to disclosures of data breaches pursuant to SB 1386 in 2005, other states began to take action.[138] Through the first seven months of 2005, thirty-five states had breach notification legislation pending, and as of December 2005, breach notification legislation had been enacted in twenty-two states.[139] Effective dates ranged from March 21, 2005 (Arkansas),[140] to July 1, 2006 (Indiana).[141]

---

133. CAL. CIV. CODE § 1798.82.

134. *Id.*

135. *Id.*

136. *See, e.g.*, Pacelle, *supra* note 8. No other state enacted breach notification legislation during 2004, and California SB 1386 seemed to slip under the radar. *See, e.g.*, Searcey, *supra* note 13.

137. *See Senate Vote on Data Brokers Likely This Week*, CONSUMERAFFAIRS.COM, Sept. 26, 2005, http://www.consumeraffairs.com/news04/2005/senate_data_privacy.html.

138. *See, e.g.*, Searcey, *supra* note 13. Before any other state could enact breach notice legislation, state attorney generals forced ChoicePoint and other data compromised companies to honor California's notice requirements nationwide. *See, e.g., 2005 Breach of Information Legislation*, NAT'L CONF. STATE LEGISLATURES, http://www.ncsl.org/programs/lis/CIP/priv/breach.htm (last visited Jan. 12, 2006) (describing how, at first, ChoicePoint only notified California residents of the breach).

139. *See* GAIL HILLEBRAND, CONSUMERS UNION U.S., INC., NOTICE OF SECURITY BREACH STATE LAWS, http://www.consumersunion.org/campaigns/financialprivacynow/learn.html (last visited Jan. 12, 2006) (follow "States with Notice of Security Breach Laws" hyperlink) (summarizing state breach laws enacted as of Nov. 30, 2005). For a brief comparison of how each state's breach notification law compares to CA SB 1386, see http://www.perkinscoie.com/content/ren/updates/privacy/010306.htm (last visited Jan. 12, 2006); *see also 2005 Breach of Information Legislation, supra* note 138.

140. ARK. CODE ANN. § 4-110-105 (2005), *available at* http://www.arkleg.state.ar.

While these new state laws generally follow the California framework, there are differences. Some states, such as Louisiana and Arkansas, allow for a risk assessment analysis, and will not require notice if after an investigation it is determined that there is "no reasonable likelihood" of harm to customers.[142] Others apply to a narrower grouping of entities than California's, such as Indiana's, which only applies to government agencies.[143] However, some cover more ground than SB 1386, such as New York's and North Carolina's (NC), which direct notification for both unencrypted and encrypted personal information, if the encryption key is also breached.[144] A corollary to the NC law is that financial institutions subject to and in compliance with the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice[145] are deemed to be in compliance with NC's law.[146] Illinois' law, unlike California's and most other states, will allow no delay in telling consumers about a breach even when such notice may impede a criminal investigation.[147] Various state breach notification laws also call for civil and criminal penalties if notice is not timely, and also for recovery of damages by individuals in a civil action against businesses in violation of the disclosure requirements.[148] In addition to data breach notification, several of the state laws address other related issues, such as NC's, which gives consumers the right to freeze their credit reports

---

us/ftproot/bills/2005/public/SB1167.pdf.

141. IND. CODE ANN. § 4-1-11-1 (West 2005), *available at* http://www.in.gov/legislative/ic/code/title4/ar1/ch11.pdf.

142. LA. REV. STAT. ANN. § 51:3074.G (2005), *available at* http://www.legis.state.la.us/billdata/streamdocument.asp?did=320093; ARK. CODE ANN. § 4-110-105(d).

143. IND. CODE ANN. § 4-1-11-5 (West 2005).

144. N.Y GEN. BUS. LAW § 899-aa.1(b) (McKinney 2005), *available at* http://assembly.state.ny.us/leg/?bn=A04254&sh=t; N.C. GEN. STAT. § 75-61(14) (2005), *available at* http://www.ncga.state.nc.us/Sessions/2005/Bills/Senate/PDF/S1048v6.pdf.

145. 70 Fed. Reg. 15,736 (Mar. 29, 2005) (to be codified at 12 C.F.R pt. 30, Supplement A to App. B (OCC); 12 C.F.R. pt. 208, Supplement A to App. D-2 and pt. 225, Supplement A to App. F (Board); 12 C.F.R. pt. 364, Supplement A to App. B (FDIC); 12 C.F.R. pt. 570, Supplement A to App. B (OTS)), *available at* http://www.steptoe.com/publications/PI9187.pdf; *see also* discussion *infra* part III.C.

146. *See* N.C. GEN. STAT. § 75-65(h). Various other states exempt financial institutions in compliance with the Guidance as well. *See, e.g.*, LA. REV. STAT. ANN. § 51:3076.

147. 815 ILL. COMP. STAT. ANN. 530/10 (LexisNexis 2005), *available at* http://www.ilga.gov/legislation/publicacts/94/PDF/094-0036.pdf.

148. *See, e.g.*, FLA. STAT. § 817.5681 (2005) (timely); LA. REV. STAT. ANN. § 51:3075 (2005) (recover damages).

and restricts the use of social security numbers.[149] While the differences are mostly minor as compared to California's law, the implications of having to comply with fifty different state laws could be huge for financial institutions, especially ones operating in multiple states (this would include nationally chartered or state chartered banks).[150]

C. *Interagency Guidance on Response Programs Guidelines*

Presumably as a result of the onslaught of security breaches being disclosed to the public as a result of California's breach notification bill, the federal banking agencies issued the Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice (Guidance)[151] to clarify the responsibilities of financial institutions in dealing with breach notification. The Guidance, which became effective on March 29, 2005, is an interpretation of both section 501(b) of the GLBA and the Security Guidelines adopted by the agencies at the direction of the GLBA.[152] The Guidance provides specific mandates for financial

149. *See* N.C. GEN. STAT. §§ 75-62 to 63. For a summary of states with security freeze legislation, see http://www.pirg.org/consumer/credit/statelaws.htm (last visited Jan. 12, 2006).

150. *See, e.g.*, Mitchell Pacelle and Christopher Conkey, *Card Issuers Take Swipe at Rules. Federal, State Legislators Propose Bills on Reporting Data Thefts; Financial Firms Want Control*, WALL ST. J., June 23, 2005, at C1.

151. 70 Fed. Reg. 15,736 (Mar. 29, 2005) (to be codified at 12 C.F.R pt. 30, Supplement A to App. B (2005) (OCC); 12 C.F.R. pt. 208, Supplement A to App. D-2 and pt. 225, Supplement A to App. F (Board); 12 C.F.R. pt. 364, Supplement A to App. B (FDIC); 12 C.F.R. pt. 570, Supplement A to App. B (OTS)), *available at* http://www.steptoe.com /publications/PI9187.pdf. Federal bank and thrift regulators released a compliance guide in December 2005 summarizing existing rules on safeguarding customer data, including the Guidance, to assist financial institutions. Press Release, Fed. Deposit Ins. Corp., Interagency Guidelines Establishing Information Security Standards Small-Entity Compliance Guide (Dec. 14, 2005) *available at* http://www.fdic.gov/news/news/press /2005/pr12705a.html.

152. *See* 70 Fed. Reg. at 15,736. The Guidance became effective immediately instead of being phased in because the agencies contended that the Guidance was nothing more than an elaboration of preexisting requirements. *Id.* at 15,748. In fact, the agencies published a 'proposed Guidance' in the Federal Register on August 12, 2003, which noted that financial institutions' information security programs were expected to include a breach response program. *Id.* at 15,737. For a copy of the Federal Register Notice containing the proposed Guidance, see http://www.ots.treas.gov/docs/7/73195.pdf. Due to the immediate effective date of the final Guidance, "when evaluating the adequacy of a national bank's information security program," the agencies "will take into account the good faith efforts made by each bank to develop a response program that is consistent with the guidance, together with all other relevant circumstances." OFFICE OF THE COMPTROLLER OF THE CURRENCY, OCC BULL.

institutions on notification to customers whose sensitive information is breached.[153]

The Guidance, like the Security Guidelines, allows financial institutions flexibility in designing a response program tailored to the institutions' business as long as certain minimum guidelines are met.[154] These minimum guidelines include: assessing the nature and scope of an incident, and identifying what customer information systems and types of customer information have been accessed or misused; notifying the institution's primary federal regulator as soon as possible when the institution becomes aware of an incident involving unauthorized access to or use of sensitive customer information; notifying appropriate law enforcement authorities consistent with suspicious activity report regulations; taking appropriate steps to contain and control the incident to prevent further unauthorized access to or use of customer information, for example, by monitoring, freezing, or closing affected accounts, while preserving records and other evidence; and notifying customers when warranted.[155]

In addition, the Guidance mandates that the standard for providing notice for incidents of "unauthorized access to sensitive customer information" is when the information has been or is reasonably likely to be misused.[156]

Sensitive customer information is defined to mean:

> a customer's name, address, or telephone number, in conjunction with the customer's social security number, driver's license number, account number, credit or debit card number, or a personal identification number or password that would permit access to the customer's account. Sensitive customer information also includes any combination of components of customer information that would allow someone to log onto or

---

NO. 2005-13, RESPONSE PROGRAMS FOR UNAUTHORIZED ACCESS TO CUSTOMER INFORMATION AND CUSTOMER NOTICE: FINAL GUIDANCE (2005), *available at* http://www.occ.gov/ftp/bulletin/2005-13.doc.

153. 70 Fed. Reg. at 15,751.

154. *Id.*

155. *Id.* at 15,752.

156. *Id.* at 15,736.

> access the customer's account, such as user name and password or password and account number.[157]

The notice should be given in a "clear and conspicuous manner" and delivered "in any manner designed to ensure that a customer can reasonably be expected to receive it."[158] Similar to most state breach notification laws, notice can be delayed if a law enforcement agency determines it will interfere with a criminal investigation.[159]

However, there is no exception for encrypted information like in California's breach notification law.[160] Dealing with service providers, the Guidance states that a financial institution's contracts with its service providers should mandate the service providers take appropriate measures to address incidents of unauthorized access to the financial institution's customer information.[161] This includes notification to the institution as soon as possible to allow implementation of the institution's response program.[162] Thus, as with the Security Guidelines, monitoring service providers is left primarily to the financial institutions.[163]

It is important to note that as an interpretation of the GLBA, the Guidance only preempts state laws that are inconsistent with the GLBA, and as previously mentioned, state laws are not inconsistent if they offer more protection than the GLBA.[164] Arguably, the Guidance sets forth the broadest data breach coverage to date, as it does not contain a blanket exemption for encrypted information breaches and applies on a national level to financial institutions.[165] Some critics have argued, however, that by granting financial institutions more flexibility in deciding whether to report a breach, it is less desirable than legislation like SB 1386, which forgoes any type of risk assessment analysis and

---

157. *Id.*

158. *Id.* at 15,752-53.

159. 70 Fed. Reg. at 15,752.

160. *Id.* at 15,745.

161. *Id.* at 15,752.

162. *Id.* The Guidance allows a financial institution to authorize or contract with its service provider to notify the institution's customers or regulator on its behalf. *Id.*

163. *See supra* notes 122-23 and accompanying text.

164. 70 Fed. Reg. at 15,738. Bank regulators expressly refused to preempt state data breach notification laws with the Guidance. *Id.*

165. *See, e.g.*, Mark Rasch, *Cleaning Up Disclosure*, SECURITY FOCUS, Apr. 11, 2005, http://www.securityfocus.com/columnists/316.

mandates reporting any breach when a consumer's unencrypted personal information is acquired.[166]

IV. CONGRESSIONAL RESPONSE TO RECENT BREACHES

With the onslaught of media attention being given to data security breaches in 2005, and with as many as 50 million constituents whose personal information had been compromised due to the breaches, congressional action was inevitable.[167] Twenty bills on data breaches or identity theft were pending in Congress during June alone.[168] By October 2005, six congressional committees were considering legislation to establish national standards on data security.[169] At first, financial institutions, as well as other businesses, were adamantly opposed to any federal mandates in the area.[170] But as word of more breaches spread, and as states started to enact inconsistent breach disclosure legislation setting up a patchwork regulatory scheme for the institutions to follow, sentiment turned towards favoring federal preemptive legislation.[171] While many of the bills introduced share strong bipartisan support, there are still many challenges to enactment of a federal breach disclosure law.[172]

Almost every proposed federal bill addresses the self-regulated nature of the data broker industry and the need for change.[173] Additionally, any national data protection law will deal with the following issues: preemption, exemptions, scope of data protection programs, notice triggers, and penalties.[174] What remains to be seen is who will win the debate on what shape and form these factors should possess, with industries supporting basic notification standards that

166. *See, e.g.*, Hannah Bergman, *Federal Bills Could Weaken Data Security, Activists Say*, AM. BANKER, Mar. 30, 2005, at 2, *available at* 2005 WLNR 5312072.

167. *See, e.g.*, Pacelle & Conkey, *supra* note 150.

168. *See, e.g.*, *id.*

169. *See, e.g.*, Michele Heller, *Debate Starts on Legislative Response*, AM. BANKER, Oct. 11, 2005, at 1, *available at* 2005 WLNR 16817872.

170. *Id.*

171. *Id.*

172. *Id.*

173. *See, e.g.*, Testimony of Consumer and Privacy Groups, *supra* note 10, at 8.

174. *See, e.g.*, Heller, *supra* note 169.

allow for discretion and consumer advocates supporting stricter standards that contain no risk analysis.[175]

A. Preemption

A federal law that preempts the inconsistent patchwork of state laws in the area of breach disclosure is critical to financial institutions.[176] State and consumer advocates, however, have lobbied against such preemption.[177] The federal proposals call for differing levels of preemption. Some bills would totally preempt state laws that cover data security, breach notification, identity theft, and other consumer-privacy issues.[178] Other bills, however, while preempting state privacy laws in the areas of data security and breach disclosure, would allow states to continue to legislate in other areas of data protection as long as the state laws were not inconsistent with the federal law, in a manner similar to the GLBA.[179]

The benefit to financial institutions of a federal bill that totally preempts state laws in the area of monitoring security programs and breach disclosures is clear - not having to comply with fifty different state laws.[180] This would save both time - as only one uniform standard will need to be consulted - and money, as complying with one law is cheaper than having to comply with fifty.[181] As businesses pass costs onto consumers, this in turn should provide consumers with cheaper

175. *See, e.g.*, Pacelle & Conkey, *supra* note 150.

176. *See, e.g.*, Bank Lawyer's Blog, http://www.banklawyersblog.com/ (Aug. 11, 2005, 5:33 PM). Though a preemption rule the OCC issued in January 2005 has shielded national banks from many state privacy laws, the OCC has not said whether it applies to state data security and breach notification laws. Michele Heller, *In Focus: Federal Effort Stalled, Firms Prep for State Laws on Data*, AM. BANKER ONLINE, Nov. 21, 2005 (subscription required; on file with author). Parties on both sides of the issue agree that the comptroller may have the ability to preempt such state privacy protections, and all that is needed is the right case to prove it in court. Ethan Zindler, *Preemption Issue May Turn on Conflict in 2 Federal Laws*, AM. BANKER, Dec. 19, 2005, at 4, *available at* 2005 WLNR 20863891.

177. *See, e.g.*, Pacelle & Conkey, *supra* note 150.

178. *See* Heller, *supra* note 176.

179. *Id.* This view supports that any federal law should be a floor that state legislatures can raise with their own laws, instead of a ceiling that prevents further state legislation, similar to the GLBA's treatment of privacy protection. *See, e.g.*, Testimony of Consumer and Privacy Groups, *supra* note 10, at 4.

180. *See, e.g.*, Bank Lawyer's Blog, *supra* note 176.

181. *Id.*

services.[182] However, a law that only partially preempts state laws could create a burdensome and inconsistent regulatory framework, especially if the remaining states enact their own data security laws containing unique features, such as credit freezes.[183] Moreover, customers in different states would receive different levels of protection.[184] Finally, if compliance becomes too costly, financial institutions may stop offering certain services, an outcome that should be avoided.[185]

B. Exemption

What entities are exempted from any federal disclosure law is another important question for financial institutions.[186] Financial institutions already regulated in this area by the GLBA security and notification requirements have made a strong case that they should be exempt from any additional federal law in this area.[187] All of the federal proposals contain an exemption from any data protection measures for GLBA-covered entities, as the GLBA already requires such data safeguards.[188] And some of the federal proposals provide a breach notification exemption for GLBA covered entities.[189] Under such a proposal, financial institutions would thus be subject to the GLBA's data protection standards along with the data breach notification requirements of the Guidance.[190] Proponents of an exemption of GLBA

182. *See, e.g.*, Heller, *supra* note 169.

183. *Id.* While a uniform standard for notice would be a positive step, a federal bill that also allows for different and tougher state privacy laws in other areas of data security is hard to justify from the perspective of financial institutions. *Id.* However, legislators may see this as the only way to get a bill passed without creating an uproar from consumer friendly groups. *Id.*

184. *Id.* The more likely scenario, however, is that banks would follow the strictest standards of the various state laws, thus giving consumers the same level of protection – although likely offering more protection than any one state contemplated. Heller, *supra* note 176.

185. *See* Searcey, *supra* note 13.

186. *See, e.g.*, Heller, *supra* note 169.

187. *Id.*

188. *See, e.g.*, Kirk J. Nahra, *Federal Security Breach Legislation Progresses (but Slowly)*, PRIVACY IN FOCUS, (Wiley Rein & Feilding LLP, Wash., D.C.), Nov. 2005, at 4, *available at* http://www.wrf.com/docs/newsletter_issues/394.pdf.

189. *See* Identity Theft Protection Act, S. 1408, 109th Cong. § 5(g) (2005), *available at* http://www.govtrack.us/data/us/bills.text/109/s1408.pdf.

190. *See, e.g.*, Heller, *supra* note 169.

covered institutions from any new federal law's notification requirement point to the fact that the Guidance is a fair disclosure law and all that is needed to prove that fact is time.[191] As previously discussed, opponents argue that such a proposal gives financial institutions too much discretion, and the Guidance is a weaker regulatory scheme than the current superior state law framework.[192]

If not exempted from federal breach disclosure legislation, financial institutions could be in a position of having to comply with dual compliance obligations, subject to state oversight along with GLBA regulator oversight.[193] While some in the industry claim this to be an "untenable position," having to comply with one national standard and the GLBA seems a more manageable framework than compliance with fifty state laws and the GLBA.[194] And being that data breach disclosures by financial institutions are now addressed by the Guidance - which is not law nor regulation – it is likely that the Guidance could be easily modified or eliminated in response to a federal data breach disclosure bill to alleviate any burden of dual compliance.[195] Yet breach disclosure is just one aspect of the federal proposals, and other issues not addressed by the GLBA, such as civil penalties for violations of security standards, would create additional burdens not present to financial institutions under only GLBA regulation.[196]

Another possible aspect of exemption is that certain types of breached data could be excluded from the notification requirement, such as encrypted files.[197] Opponents of this approach argue that encrypted files should not be exempted due to weaknesses in encryption technologies.[198] Yet an exemption on data that is encrypted, as long as the encryption codes are not also compromised, would no doubt strongly encourage all regulated entities to adopt encryption

191. *See, e.g.*, Eugene A. Ludwig, *Don't Let Security Fears Stifle Innovation*, AM. BANKER, Sept. 23, 2005, at 10, *available at* 2005 WLNR 15364229.

192. *See, e.g.*, Testimony of Consumer and Privacy Groups, *supra* note 10, at 8.

193. *See, e.g.*, Heller, *supra* note 169.

194. *Id.*

195. *See* Rob Garver, *Is it Time to Start Issuing Guidelines on the Guidelines?*, AM. BANKER, May 3, 2005, at 6A, *available at* 2005 WLNR 7276418.

196. *See, e.g.*, Heller, *supra* note 169.

197. *See* Testimony of Consumer and Privacy Groups, *supra* note 10, at 8.

198. *Id.*; *see also supra* notes 58-67 and accompanying text.

technologies and facilitate technological advances in the field to reduce liability in case of a data breach.[199]

C. *Scope of Data Security Programs*

While financial institutions may be exempted from coverage of a federal data security bill, data brokers will not.[200] Early federal proposals were focused almost entirely on the data broker industry.[201] More recent proposals, however, apply to all businesses that maintain sensitive personal consumer data.[202] Still, a focal point of each proposed bill is to require written security programs for data brokers.[203] Because financial institutions are already required by the GLBA to maintain data protection programs, and all the proposed bills mirror the GLBA requirements, any federal mandate in this area will not impose any additional burdens on financial institutions.[204]

However, the effect of such legislation will have a huge impact on the financial industry. This is because by creating a national standard for non-financial institutions to adhere to, the security of sensitive customer personal information across all industries will be brought up to the level that exists in the financial services industry, a much needed improvement over the current regulatory scheme.[205]

Another possible benefit to financial institutions is if third-party service providers are regulated along with data brokers, which will be the case if the bill covers all entities that maintain sensitive consumer information, as most proposals do.[206] "If vendors are mandated by federal law to meet essentially the same data protection and [breach notification] standards as . . . bank[s] . . . , this would remove . . . the bargaining power" some vendors hold over less sophisticated and

199. *See, e.g.*, Heller, *supra* note 68.

200. *See, e.g.*, Christopher Conkey, *Identity-Theft Bills Stall in Congress*, WALL ST. J., Nov. 26, 2005, at A4.

201. *See, e.g.*, Nahra, *supra* note 188.

202. *Id.*

203. *Id.*

204. *Id.*; *see also supra* notes 109-27 and accompanying text.

205. *See* Ludwig, *supra* note 191.

206. *See* Testimony of Consumer and Privacy Groups, *supra* note 10, at 3 (calling for the extension of the GLBA's Safeguards rule to third party processors); *see also* Michele Heller, *Postponing Battle, Panel OKs Data Bill*, AM. BANKER ONLINE, Nov. 18, 2005 (subscription required; on file with author).

smaller banks to negotiate less than full compliance with GLBA standards.[207] Additionally, third-party service providers will be held accountable and monitored for compliance on a continuous basis by federal regulators, instead of solely by banks overseeing their contracts with the vendors per the GLBA.[208] This shift of liability can only help banks whose images have taken a hit due to the loss of data by third-parties.[209] It may also help shift financial liability, as banks are currently left to sue service providers who allow customer data to be accessed by unauthorized individuals in order to gain restitution.[210] A financial institution would still, however, likely take a reputation hit for selecting a third-party who was subject to a data breach.[211]

D. Notice Triggers

The most debated aspect of the federal bills, outside of federal preemption, is when a breached entity must provide notice to those whose data was breached.[212] At least one federal proposal would just extend the bank security Guidance framework to other businesses.[213] Another bill would require notification if the breached information included a person's name along with any two of the following details:

---

207. Bank Lawyer's Blog, http://www.banklawyersblog.com/ (Jul. 28, 2005, 7:30 AM). "Except to the extent that state law imposes . . . similar requirement[s] [for data protection, such as in California,] . . . vendors have room to 'maneuver' in the course of contract negotiations . . . ." *Id.* Some vendors use this bargaining power to negotiate less than full protection for banks in this area, as well as shifting the cost of compliance with the GLBA onto the bank. *Id.*

208. *Id.*; *see supra* notes 122-23, 161-63 and accompanying text.

209. *See, e.g.*, Michele Heller, *13 Breach Bills (Only 1 Tackles Liability Issue)*, AM. BANKER, Aug. 5, 2005, at 1, *available at* 2005 WLNR 12643713. Critics argue that banks should be held liable for the failures of third parties to protect data. *See, e.g.*, Testimony of Consumer and Privacy Groups, *supra* note 10, at 2.

210. *See, e.g.*, Heller, *supra* note 209. "Service providers generally are not household names, so when a breach occurs that puts card accounts at risk, the bank that issued the card has to notify affected customers and reissue the card." *Id.* Along with shouldering the cost of notifying the breached cardholders, banks often take a reputation hit as well, as customers view the bank as the responsible party. *Id.* Companies argue that notification and replacing debit and credit cards is expensive, costing as much as $15 per affected customer just to reissue a card, and those responsible for any data breach should cover such costs. Conkey, *supra* note 200.

211. Heller, *supra* note 209.

212. *See, e.g.*, Heller, *supra* note 169.

213. *Id.* Notably, this proposal comes from the House Financial Services Committee. *Id.*

address, phone number, or birth date.[214] Additionally, customers would have to be notified of a breach if it involved their name and an account access code or password.[215] Critics of these farthest reaching notification measures argue that none of this information is generally considered sensitive, either alone or when combined together.[216]

Each proposal does, however, provide more leeway than SB 1386 in deciding whether or not to report a breach.[217] For example, even the most far-reaching proposal states that a business can avoid notification of customers if a risk assessment conducted in consultation with Federal law enforcement authorities concludes that there is no significant risk of harm to individuals whose sensitive personally identifiable information was at issue in the breach.[218] Another proposal sets the notice trigger at a "reasonable risk of identity theft" to one or more individuals, using a preponderance of the evidence standard to see if such theft is foreseeable.[219]

If every single breach, no matter what risk of harm involved, had to be reported, consumers might start ignoring the notices, especially if the compromised information is never actually used by thieves.[220] On top of this, regulators could possibly feel the same effect, and not react appropriately when a serious breach occurred.[221] Moreover, requiring notification for every breach, no matter how minimal, could carry with it great expense.[222] This cost would

214. *Id.*; Personal Data Privacy and Security Act of 2005, S. 1789, 109th Cong. § 3 (2005), *available at* http://www.govtrack.us/data/us/bills.text/109/s1789.pdf. The Personal Data Privacy and Security Act of 2005 is co-sponsored by Senators Arlen Specter, Patrick Leahy, Dianne Feinstein, and Russell Feingold. *Id.*

215. *See, e.g.*, Heller, *supra* note 169.

216. *Id.*

217. *See, e.g.*, Bergman, *supra* note 167.

218. *See* S. 1789.

219. *See* Identity Theft Protection Act, S. 1408, 109th Cong. § 3(c) (2005), *available at* http://www.govtrack.us/data/us/bills.text/109/s1408.pdf.

220. *See* Searcey, *supra* note 13.

221. *See, e.g.*, Michael Sisk, *Careful What You Wish For*, FIN. IT SECURITY, Sept. 2005, at 11 (describing how when bank regulators demanded more rigorous reporting of suspicious activity reports (SARs), regulators could not identify the SARs that might actually be an indicator of wrongdoing because of the volume received).

222. *See Hearing on Data Breaches and Identity Theft Before the S. Comm. on Commerce, Science, and Transportation*, 109th Cong. 10 (2005) [hereinafter FTC June 2005 Testimony] (statement of the Fed. Trade Comm'n), *available at* http://www.ftc.gov/os/2005/06/050616databreaches.pdf. For example, a customer may respond to a security breach notification by canceling credit cards, contacting credit bureaus to place fraud alerts on their files, or by obtaining a new driver's license. *Id.* Each of these actions can be time

ultimately be passed onto the consumer in the shape of less or more expensive services.[223] Adding to this, some fear that onerous notice requirements will stifle and impede the advances being made in data protection technology.[224]

Notification proponents argue that customers have a right to know whenever their sensitive information is acquired by an unauthorized person.[225] They contend that breached entities have no way of knowing how stolen information will be used, and also have a conflicting interest to not report a breach to avoid reputation harm.[226] Moreover, if every breach must be reported, companies will put more money into data security measures.[227] By this logic, the number of breaches will be reduced as a result of stronger security encouraged by a strict notification standard.[228]

Another factor that could affect how much harm a breach causes is the timeliness of notice.[229] Prompt notification of data breaches to customers and law enforcement officials can help mitigate any damage caused by identity theft or other fraud.[230] Language in proposed bills ranges from requiring notice "in the most expedient manner practicable, but not later than 45 days"[231] after discovery of a breach, to "without unreasonable delay following the discovery of"[232] a security breach. Like SB 1386 and the Guidance, all the proposed federal bills also allow for a delay of notice if law enforcement determines that such notice would impede an investigation or if steps are necessary to restore the integrity of the data system.[233]

---

consuming and costly, both for the consumer and business involved. *Id.*

223. *See* Searcey, *supra* note 13.

224. *See* Michele Heller, *Flurry of Action in Congress on Data Security*, AM. BANKER, July 21, 2005, at 6, *available at* 2005 WLNR 11796382.

225. *See, e.g.*, Testimony of Consumer and Privacy Groups, *supra* note 10, at 9.

226. *Id.* at 10.

227. *Id.*

228. *Id.*

229. *See* FTC June 2005 Testimony, *supra* note 222, at 10.

230. *Id.*

231. Identity Theft Protection Act, S. 1408, 109th Cong. § 3(e) (2005), *available at* http://www.govtrack.us/data/us/bills.text/109/s1408.pdf.

232. Personal Data Privacy and Security Act of 2005, S. 1789, 109th Cong. § 321(c) (2005), *available at* http://www.govtrack.us/data/us/bills.text/109/s1789.pdf.

233. *See, e.g.*, S. 1408, § 3(e)(2).

E. *Penalties and Other Issues*

The majority of federal proposals also contain some kind of monetary penalty for failing to report a breach within the specified time frame. The amounts are significant, ranging from "$1,000 per day per individual whose sensitive personally identifiable information was, or is reasonably believed to have been, accessed or acquired" up to $11 million "in the aggregate for all such individuals [related to one breach]."[234] In addition, businesses or individuals that intentionally or willfully violate the notice requirements could be subject to additional monetary punishment or up to five years imprisonment.[235] Critics argue that the civil penalties should have a limit, because "'[i]f violations are not discovered for a long period of time, the uncapped [monetary] penalties may be excessive . . . [as compared to the actual harm] incurred.'"[236] Most of the proposals do, however, bar individuals from suing for damages, but some would allow states to bring suits.[237]

Various other issues, including giving consumers the right to correct inaccurate information data brokers hold on them, restricting the use of social security numbers, and allowing consumers to freeze their credit reports, could be addressed by a federal data security law.[238] Allowing consumers the right to correct inaccurate information data brokers hold on them would extend similar requirements already imposed on credit reporting agencies under the Fair Credit Reporting Act,[239] financial institutions under the GLBA,[240] and health care providers under the Health Insurance Portability and Accountability Act.[241]

Dealing with social security numbers, one proposal would bar businesses from requiring a consumer's social security number "unless there is a specific use . . . for which no other identifier can be reasonably used."[242] It would also ban the sale, purchase, and display of

234. S. 1789, § 327; S. 1408, § 5(e).
235. *See* S. 1789, § 102.
236. *See* Heller, *supra* note 169.
237. *See* Heller, *supra* note 209.
238. *See, e.g.*, Heller, *supra* note 169.
239. *See* 15 U.S.C. §1681g (2000).
240. *See* 15 U.S.C. § 6802 (2000).
241. *See* 42 U.S.C. §§ 1320d to 1320d-8 (2000).
242. *See* Identity Theft Protection Act, S. 1408, 109th Cong. § 8 (2005), *available at*

social security numbers to the general public.[243] Proponents of such a measure note that restricting the use of social security numbers is perhaps the core issue of data security – making customer information less valuable to thieves.[244] While data security is important, proponents note that if criminals could not create value from the data, they would not try to steal it.[245] But businesses oppose such a measure, saying that "[w]ithout the ability to use Social Security numbers as personal identifiers and fraud prevention tools, the granting of credit and the provision of other financial services would become riskier . . . [,] more expensive[,] and inconvenient for customers."[246]

Following the states lead, a federal data security bill may also allow consumers to block access to their credit reports.[247] Such a tool effectively prevents criminals from opening up new lines of credit under false identities, as creditors are unlikely to extend credit to those that they cannot check credit reports or scores on.[248] Financial institutions contend that the time requirements imposed by such freezes create unnecessary costs for all consumers, slows down the flow of information (and therefore business), and that freezing credit reports should be limited to previous victims of identity theft.[249] Proponents argue that such credit freezes would "prevent identity thieves from achieving their ultimate goal – opening up new credit accounts to accumulate debt in the consumer's name" – and should be available for all consumers.[250] If modeled after New Jersey's security freeze law,[251]

---

http://www.govtrack.us/data/us/bills.text/109/s1408.pdf.

243. *Id.* § 8(d). The "Personal Data Privacy and Security Act of 2005" (originally S. 1332) included a proposal to limit the buying and selling of social security numbers, but was amended to remove such language in order to get more Senate Judiciary Committee members to support the bill. *See* Alexei Alexis, *Senate Judiciary Committee Chairman Considers Moving Narrow ID Theft Bill*, E-COMMERCE LAW DAILY, Sept. 30, 2005, http://subscript.bna.com/SAMPLES/ecd.nsf/0/cd70a8e2679382968525708b007fb1c1?OpenDocument.

244. *See* Heller & Lindenmayer, *supra* note 83.

245. *Id.*

246. *See* FTC June 2005 Testimony, *supra* note 222, at 13. Various policy and practical concerns are raised by the fact that social security numbers are in the public records of many cities and counties. *Id.* at 15.

247. Heller, *supra* note 176; *see also supra* note 149 and accompanying text.

248. *See, e.g.*, Testimony of Consumer and Privacy Groups, *supra* note 10, at 11-12.

249. *Id.*

250. *Id.* at 11.

251. N.J. STAT. ANN. § 56:11-46 (West 2005), *available at* http://www.njleg.state.nj.us/2004/Bills/A3500/4001_I1.PDF.

which is the farthest reaching in the country, a federal credit freeze provision would allow individuals to freeze their credit reports and would require credit agencies to allow consumers to instantly unthaw such a freeze within fifteen minutes of notice to do so.[252]

V. CONCLUSION

For financial institutions that are already regulated by the GLBA, any extension of GLBA-like data safeguard standards to the rest of corporate America means having to worry less about customer data getting lost or stolen after it gets to third parties.[253] In addition, if a federal breach disclosure law is enacted that does not exempt financial institutions already covered by the GLBA and Guidance mandates, the regulatory landscape for financial institutions will become more burdensome as states continue to pass their own data security laws.[254] Such a regulatory environment could result in companies focusing more on compliance than security, and stifle the wave of innovations the industry responded to data security breaches with in 2005.[255] As previously discussed, any federal proposal that preempts the maze of state breach disclosure laws developing would be a welcome sign for banks.[256] In contrast, a federal bill with inadequate preemption measures will be of little value to financial institutions.[257]

Financial institutions also need a specific standard to follow in terms of when to notify.[258] A vague standard could lead to over-notification in fear of penalties, and would be both expensive and could numb consumers and regulators alike when a serious data breach occurs.[259] In a best case scenario, a federal bill would limit notification to data breaches that threaten a "significant risk" of identity theft.[260] In addition, financial institutions would best be served by a federal bill that

252. Testimony of Consumer and Privacy Groups, *supra* note 10, at 12.

253. *See* Michael Grebb, *Congress Jumps Into Privacy Debate*, FIN. IT SECURITY, Sept. 2005, at 15.

254. Heller, *supra* note 176.

255. *See* Ludwig, *supra* note 191.

256. *Id.*

257. Heller, *supra* note 206.

258. *See, e.g.*, Conkey, *supra* note 200.

259. *See, e.g.*, Pacelle & Conkey, *supra* note 150.

260. *See, e.g.*, Conkey, *supra* note 200.

did not empower consumers to freeze their credit reports, as such a measure would slow down electronic commerce.[261]

"Congress will not pass data-security legislation until . . . March [2006] at the earliest - by which time [twenty-one] state laws, many conflicting, will be in effect."[262] Due to the differences between the state laws, the longer Congress waits, the more difficult compliance will be.[263] The net effect, however, will probably result in financial institutions following the strictest state standards nationwide and doing more than any one state contemplated.[264]

Financial institutions would be wise to learn from the lesson learned in 2005 – no matter how secure customer information seems, there is still a good chance a data breach may occur.[265] Additionally, even if the financial institution was not directly responsible for the breach, it will likely suffer reputation harm if the breach is not handled swiftly and properly after discovery.[266] Financial institutions should thus continue to develop the mindset that security is a total organization focus, instead of just one department.[267] Those that embrace this mindset will not only be able to better protect sensitive customer information, but will also gain a reputation for such with the ever increasing importance being placed on data protection by consumers.[268]

SEAN C. HONEYWILL

261. *Id.*

262. Heller, *supra* note 176.

263. *Id.*

264. *Id.*

265. *See Hearing on Protecting our Nation's Cyberspace Before the Subcomm. On Tech., Info. Policy, Intergovermental Relations, and the Census of the H. Comm. on Gov't Reform*, 109th Cong. 5 (2004) (statement of the Fed. Trade Comm'n), *available at* http://www.ftc.gov/os/2004/04/042104cybersecuritytestimony.pdf.

266. *See Data Breaches Bad for Business*, *supra* note 108.

267. *See* Grebb, *supra* note 27.

268. *Id.*