Legislative Responses to Data Breaches and Information Security Failures

Philip Keitel*

December 2008

Summary: *On July 23, 2008, the Payment Cards Center of the Federal Reserve Bank of Philadelphia hosted a workshop to discuss federal and state legislative responses to data breaches. The workshop addressed several laws and legislative initiatives designed to create greater safeguards for personal consumer information frequently targeted by data thieves and often subject to the failures of information security protocols. Diane Slifer, J.D., M.B.A., who has frequently presented at forums on data security and has represented clients in matters related to data breaches, led the workshop. Slifer examined several highly publicized data breaches and explained how various laws and regulations have been put in place in order to protect and inform consumers whose personal information has been compromised. Additionally, she discussed several legislative initiatives designed to potentially create a more structured and secure environment for private consumer data overall. This paper summarizes Slifer's presentation, the ensuing discussion, and additional Payment Cards Center research. In addition, it offers a brief overview of recent data breaches, a description of various ways that federal and state laws operate, and some thoughts on how effective these laws and regulations have been.*

* Payment Cards Center, Federal Reserve Bank of Philadelphia, Ten Independence Mall, Philadelphia, PA 19106. E-mail: philip.keitel@phil.frb.org. The views expressed here are not necessarily those of this Reserve Bank or of the Federal Reserve System. The contents of this paper and Slifer's presentation at the workshop are intended to be informational in nature and should not be considered legal advice. Individuals, companies, and entities should seek legal counsel when dealing with issues of data security and breaches.

FEDERAL RESERVE BANK OF PHILADELPHIA

Ten Independence Mall, Philadelphia, PA 19106-1574 • (215) 574-7220 • www.philadelphiafed.org/payment-cards-center/

I. Introduction

The increased importance of data in modern consumer finance and the resulting digitization of massive amounts of consumer information have caused a proliferation of data systems that store and transmit sensitive personal information. While the use of such consumer data enables financial institutions to deliver significant benefits to consumers, it also introduces new risks associated with securing the data. In fact, stores of confidential consumer data have attracted the attention of cyber criminals who attack data storage systems for the purpose of gaining large-scale access to consumer financial information in order to commit fraud.[1] Since 2005, over 1,000 data breaches have been reported in the United States.[2] Data storage systems at financial institutions, hospitals, retailers, government agencies, schools, libraries, and local municipalities have all been breached, leaving more than 240 million[3] Americans potentially exposed to subsequent crimes incorporating stolen data.[4] Moreover, attacks of this nature appear to be increasing. By the beginning of September 2008, 449 data breaches had been reported for the year,[5] already passing the total of 446 for all of 2007 and greater proportionally than the two-year data breach total from 2005 and 2006 (estimated at 570 breaches).[6]

Although it is popularly believed that most data breaches are the result of computer hacking, the logistical difficulties inherent in handling personal consumer information contained in data storage

[1] Crimes that commonly incorporate stolen consumer information include payment fraud and identity theft. For more information, see Government Accountability Office, *Data Breaches and Identity Theft Report*, GAO-07-737 (Jun. 4, 2007), p. 5, noting the use of stolen data for account fraud (akin to payment fraud) and new account creation (true identity theft); and Kimberly Kiefer Peretti, U.S. Department of Justice Computer Crime and Intellectual Property Section, "Data Breaches: What the Underground World of 'Carding' Reveals," *Santa Clara Computer and High Technology Journal*, 25 (forthcoming), detailing criminal activities that involve consumer payment card and other confidential data.

[2] See *Data Breaches and Identity Theft Report* [n. 1], p. 4, analyzing evidence of reported data breaches from 2005 and 2006 across a number of varying types of institutions; and Verizon Business Risk Team, "2008 Data Breach Investigations Report," (2008), pp. 5-6, reviewing 500 breaches and concluding that the overall number of data breaches from 2005 through 2007 may be as high as three to four times the number reviewed.

[3] See the Privacy Rights Clearinghouse, "A Chronology of Data Breaches," available at: www.privacyrights.org/ar/ChronDataBreaches.htm, providing a timeline of reported data breaches and a number of records containing personal consumer information that may have been exposed (accessed Sept. 4, 2008).

[4] In February, more than 4.2 million consumers' credit and debit card numbers and expiration dates were exposed as a result of a single data breach at Hannaford Bros. grocery chain. See "Litigation Comes Quickly on Heels of Breach," *Consumer Financial Privacy Bulletin*, a Consumer Financial Services Law Report supplement, April 16, 2008, p. 1.

[5] Identity Theft Resource Center, "Breaches Blast '07 Record; as of August 22, ITRC'S List Surpasses 446 Documented Breaches," PR Newswire, Aug. 25, 2008, p. 1.

[6] See *Data Breaches and Identity Theft Report* [n. 1], p. 4.

systems have resulted in a significant number of data losses. For example, personal consumer data have been misappropriated by employees,[7] obtained by criminals who intended to steal computers—but not necessarily the data located on those machines,[8] exposed through inadvertent error,[9] sold to criminals posing as legitimate businesses,[10] and lost during transport.[11] Moreover, Bank of New York Mellon and credit card issuer GE Money recently disclosed the loss of computer data backup tapes containing thousands of consumers' personal information.[12] As a result of these highly publicized losses and greater attention to losses not related to hacking, industry analysts and policymakers are focusing more on how data are stored, transported, and cared for.

These emergent consumer data security and handling issues and the relatively new criminal phenomena associated with them have been met with a bevy of industry[13] and government responses. In particular, the major payment network companies American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. joined forces in 2006 to create the Payment Card Industry Security Standards Council.[14] Founded to establish and promote "a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures," the council endeavors to create a more structured consumer data environment by designing and communicating standard practices to combat data security shortcomings. One such example is the Payment Card Industry Data Security Standards, or PCI DSS, a

[7] See the syndicated AP article: "Fidelity: Worker Stole Consumer Data," as reported by CBS News, July 3, 2007.
[8] Chris Mondics, "Data Breaches a Concern to Companies," *Philadelphia Inquirer,* Sept. 19, 2008, p. C5. See also Martin Bosworth, "Consumer Data Stolen from TransUnion," ConsumerAffairs.com, Nov. 14, 2005, p. 1; and MSNBC Interactive, "Laptop with GE Employment Data Stolen," MSNBC, Sept. 26, 2006, providing examples of cases in which computers containing confidential consumer information were stolen by individuals with an apparent intent to re-sell those machines.
[9] "Data Breaches a Concern to Companies," [n. 8], p. C5.
[10] See Jeff Leeds, "Bank Sold Credit Card Data to Felon," *Los Angeles Times,* Sept. 11, 1999, p. A-1; Joseph Menn and David Colker, "ChoicePoint CEO Had Denied Any Previous Breach of Database," *Los Angeles Times,* March 3, 2005, p. C1.
[11] Syndicated AP article, "Bank of America Loses Consumer Data," as reported by MSNBC and MSNBC.com, March 1, 2005.
[12] Louis Berner, "'Security' for Sale," *Cards & Payments* 21(4) (April 2008), pp. 22, 24, 26-27; Daniel Wolfe, "Bank of New York Mellon Enlarges Data Loss," *American Banker*, Aug. 29, 2008.
[13] See, for example, Frederick Lowe, "Payments Industry Comes Together to Fight a Common Enemy," *Cards & Payments* (July 2006), pp. 25-28, detailing ways in which the payment industry has responded to data-security issues and fraud.
[14] See www.pcisecuritystandards.org/about/index.shtml (accessed Sept. 9, 2008).

set of protocols that companies handling and storing network-branded payment cards must follow,[15] and that a few states, such as Minnesota and California, are beginning to incorporate into their own legislative initiatives.[16] Around the same time as private payments industry operators formed the council, President George W. Bush recognized "the heavy financial and emotional toll" that crimes involving confidential consumer data —such as identity theft[17]—exact from victims as well as the economic cost of crimes that depend on the unauthorized use of consumers' information. In an effort to stem the tide of these crimes, he established the President's Task Force on Identity Theft.[18] Charged with creating a strategic plan that increases the effectiveness and efficiency of measures taken by the federal government "in the areas of identity theft awareness, prevention, detection, and prosecution,"[19] the task force includes individuals from the Federal Reserve (the Fed), the Federal Trade Commission (FTC), the Federal Deposit Insurance Corporation (FDIC), the Office of the Comptroller of the Currency (OCC), the Office of Thrift Supervision (OTS), the National Credit Union Administration (NCUA), and several other government agencies.[20] In addition to the council and the task force, joint industry and government groups, such as the Anti-Phishing Working Group,[21] and not-for-profit groups, such as the Identity Theft Resource Center,[22] Privacy Rights Clearinghouse,[23] and Electronic Privacy Information Center,[24] are also working to combat crimes related to the theft of confidential consumer data.

Recognizing the importance of emergent government and industry initiatives surrounding the maintenance and handling of confidential consumer information and related crimes, the Payment Cards

---

[15] See n. 14 as well as www.pcisecuritystandards.org/security_standards/pci_dss.shtml.
[16] See Laura Mahoney, "Data Breach Bill Passes California Senate; Business Opponents Eye Governor's Veto Pen," Bureau of National Affairs Inc., *Banking Daily*, Aug. 29, 2008, p. 1; and Jaikumar Vijayan, "'I'll Be Back': Vetoed Data Breach Bill Goes to Schwarzenegger Again," *Computerworld* (Sept. 3, 2008).
[17] For more information on identity theft, see Keith B. Anderson, Erik Durbin, and Michael A. Salinger, "Identity Theft," *Journal of Economic Perspectives* 22(2) (Spring 2008), pp. 171-92.
[18] See www.idtheft.gov/about.html (accessed Sept. 10, 2008).
[19] On April 23, 2007, the task force issued recommendations on a plan for combating identity theft. To view the plan, entitled "Combating Identity Theft: A Strategic Plan," visit: www.idtheft.gov/reports/StrategicPlan.pdf.
[20] See www.idtheft.gov/about.html.
[21] See, for example, www.antiphishing.org/ (accessed Sept. 10, 2008), detailing the aims of a joint law enforcement and industry working group established to combat phishing crimes.
[22] See www.idtheftcenter.org/ (accessed Sept. 10, 2008).
[23] See www.privacyrights.org/index.htm (accessed Sept. 10, 2008).
[24] See http://epic.org/ (accessed Sept. 10, 2008).

Center held a conference in 2006 entitled "Information Security, Data Breaches, and Protecting Cardholder Information: Facing Up to the Challenges."[25] Issues addressed during the conference included industry and regulatory responses to information security concerns and data breaches, the impact of data breaches and identity theft on consumers and businesses, and ways in which consumers can be better protected from harm associated with data breaches. To revisit regulatory and policy-related issues raised during the 2006 conference and to look at how consumer data security concerns are contemplated under various laws, the Payment Cards Center held a workshop on July 23, 2008. The center invited Diane Slifer, who has frequently presented at forums on data security and has represented clients in matters related to data breaches, to lead the workshop's discussion and overview of several key laws, regulations, and legislative initiatives aimed at creating a more secure and structured environment for private consumer data and one designed to help protect consumers whose personal information has been compromised. This paper, based on Slifer's presentation and additional research by the Payment Cards Center, offers an overview of several laws[26]—or types of laws—that have been enacted to address emerging issues related to data breaches and to better safeguard consumers' personal information.[27] This paper also offers insight into responses to these laws.

This paper first looks at federal laws and legislative initiatives discussed during the workshop, including provisions of the Gramm-Leach-Bliley Financial Modernization Act of 1999 and the Fair and Accurate Credit Transactions Act of 2003. Second, it addresses state laws, including state laws concerning the handling of Social Security numbers and state data breach notification laws. Last, it

[25] For more information, see James C. McGrath and Ann Kjos, "Information Security, Data Breaches, and Protecting Cardholder Information: Facing Up to the Challenges," Payment Cards Center Conference Summary, Sept. 13-14, 2006, available at: http://www.philadelphiafed.org/payment-cards-center/events/conferences/2007/C2006SeptInfoSecuritySummary.pdf. payment-cards-center/events/conferences/2007/C2006SeptInfoSecuritySummary.pdf.

[26] Since1999, Congress and a number of state legislatures have enacted laws that address how consumers' personal information is stored, how it is maintained, the ways in which it must be safeguarded, and how it must be disposed of. This paper addresses several of these laws. However, the references to laws and legislative initiatives contained herein are not meant to be an exhaustive list of all federal or state regulations about private consumer information. Rather, this paper summarizes a sampling of related laws and initiatives.

[27] In this context, personal information generally means an individual's name along with his or her Social Security number, account number (including direct deposit accounts, credit card numbers, and debit card numbers) together with passwords or access codes used with those accounts, and/or driver's license/state identification card number that also identifies that consumer. See also n. 41.

concludes with a summary of the regulatory environment, recent findings on the effectiveness of data breach notification laws in preventing subsequent fraud crimes, and thoughts on how consumers can be shielded from harm associated with data breaches and information security failures.

II. Consumer Data Provisions of the Gramm-Leach-Bliley Financial Modernization Act

In 1999, Congress enacted the Gramm-Leach-Bliley Financial Modernization Act, also known simply as the Gramm-Leach-Bliley Act (GLB Act). The underlying intent of the GLB Act was to modernize and enhance competition in the financial services industry by repealing provisions of the Glass-Steagall and Bank Holding Company acts that had prohibited banks from engaging in activities such as affiliating with securities companies or conducting certain insurance-related activities.[28] However, in response to last minute congressional negotiations,[29] consumer privacy provisions were added to the bill.[30] As a result, the GLB Act has three principal provisions that protect consumers'[31] personal financial

[28] See Conference Report on S. 900, Gramm-Leach-Bliley Act, U.S. House of Representatives, *Congressional Record* (Nov, 2, 1999), p. H11256; and Senate Banking Committee Conference Report on the Gramm-Leach-Bliley Bill, (Nov. 1, 1999), available at: http://banking.senate.gov/conf/confrpt.htm (accessed Sept. 11, 2008).

[29] Senate Banking Committee Conference Report on the Gramm-Leach-Bliley bill, at *Title V- Privacy.* Available at: http://banking.senate.gov/conf/fintl5.pdf (accessed Dec. 5, 2008).

[30] Some policy analysts view the enactment of the privacy provisions of the GLB Act as a legislative response to mounting public displeasure with financial institutions' practices concerning consumers' personal information, highly publicized sales of consumer information to disreputable organizations, and growing international awareness of data security concerns (such as the E.U. Data Protection Directive and ensuing E.U.-U.S. agreements). For more information, see, for example, the Electronic Privacy Information Center's history of the Gramm-Leach-Bliley Act, recounting events and conditions leading up to the act's passing, available at: http://epic.org/privacy/glba/ (accessed Sept. 11, 2008).

[31] Under the GLB Act, codified at 15 U.S.C. § 6801 et seq. (2007), only customers of financial institutions are entitled to receive privacy notices automatically, and customers are considered a subset of consumers at large. 15 U.S.C. § 6809(9) defines a "consumer" as "an individual who obtains, from a financial institution, financial products or services which are to be used primarily for personal, family, or household purposes, and also means the legal representative of such an individual." Defining a "customer," under the GLB Act, or, more aptly, defining when a customer relationship is established, is left to the regulatory agencies themselves. 15 U.S.C. § 6809(11) states, "The term 'time of establishing a customer relationship' shall be defined by the regulations prescribed under section 6804 of this title, and shall, in the case of a financial institution engaged in extending credit directly to consumers to finance purchases of goods or services, mean the time of establishing the credit relationship with the consumer." One example comes from 16 C.F.R. § 313.3(h) (2008), which defines "customer" simply as: any consumer "who has a customer relationship with you." A "customer relationship" is defined under 16 C.F.R. § 313.3(i)(1) as "a continuing relationship between a consumer and you under which you provide one or more financial products or services to the consumer that are to be used primarily for personal, family, or household purposes."

information held by financial institutions:[32] (1) the financial privacy rule; (2) the safeguards rule; and (3) the pretexting provision (pretexting is when a person, without authority to do so, attempts to gain access to the personal information of another by creating a false scenario).[33] Generally, the financial privacy rule calls for financial institutions to establish and communicate policies concerning their use of consumers' personal financial information and to afford consumers control over how their information is shared with others; the safeguards rule requires financial institutions to have a security plan in place to protect the confidentiality and integrity of personal consumer information; and the pretexting provision encourages institutions covered by the GLB Act to implement safeguards against pretexting.

More specifically, the financial privacy rule[34] requires financial institutions to provide notices to their customers explaining their privacy practices and the customer's rights. All privacy notices must be updated at the time a financial institution makes changes to its privacy policies, and annually—even if no policy change occurs. Privacy policies must identify in clear, conspicuous, and accurate language what "nonpublic personal information" is collected and disclosed about customers. Privacy notices must also detail how such information is used, how the financial institution protects or safeguards the information, and with whom the information might be shared. Additionally, privacy notices need to inform customers of their right, in many instances, to opt out of having their information shared with third parties and to opt out of having certain information (such as credit report or application information) shared with their financial institution's affiliates.[35]

The financial privacy rule essentially requires financial institutions to notify customers about the protection of their personal information. Noting that industry analysts have raised the concern that most notices merely satisfy the basic legal requirement to explain obligations and rights accurately, workshop participants observed that many notices seem to fall far short when it comes to providing explanations

[32] 15 U.S.C. § 6809(3)(A) defines "financial institution" as "any institution the business of which is engaging in financial activities as described in section 1843(k) of title 12" (12 U.S.C. 1843(k) (2007)).
[33] The FTC defines pretexting as "the use of false pretenses, including fraudulent statements and impersonation, to obtain consumers' personal financial information, such as bank balances." See the FTC's website: www.ftc.gov/privacy/privacyinitiatives/pretexting.html (accessed Aug. 19, 2008).
[34] Codified at 15 U.S.C. § 6801(a) et seq.
[35] The right to opt out of information sharing between affiliates exists under the Fair Credit Reporting Act.

that are meaningful to the reader. This is a sentiment echoed by consumers, state attorneys general, and privacy advocates—all of whom have expressed their concern over the complexity of privacy notices and the ability of consumers to understand the terms they contain,[36] and some of whom have raised the issue of consumer desensitization to mailed notices and alerts.[37] Responding to these concerns, regulators have provided updated guidance on how institutions might structure simpler and more comprehensible notices.[38]

Under the safeguards rule,[39] financial institutions[40] must develop written security plans detailing how they will protect the confidentiality and integrity of personal consumer information.[41] Plans may be tailored to the organization's size and complexity, the activities the organization undertakes, and the type of information handled, but they must take into consideration all areas of an organization's operations,

[36] See, for example, Joanna Glasner, "Survey: Opt-Out Is a Cop Out," *Wired* (May 7, 2002), discussing responses to consumer privacy protections created under the Gramm-Leach-Bliley Act; and testimony of Edmund Mierzwinski, consumer program director of the U.S. Public Interest Research Group, before the Senate Committee on Banking, Housing and Urban Affairs Oversight Hearing on Financial Privacy and the Gramm-Leach-Bliley Financial Services Modernization Act, available at: www.privacyrights.org/ar/USPirg-GLB0902.htm, detailing concerns surrounding consumers' ability to understand privacy policy notices.

[37] Testimony of Edmund Mierzwinski [n. 36], at section (2).

[38] Materials to educate consumers on the financial privacy rule are available from www.ftc.gov/privacy/privacyinitiatives/financial_rule_con.html (accessed Aug. 17, 2008).

[39] Codified at 15 U.S.C. § 6801(b).

[40] The term "financial institution" encompasses a broad range of businesses. In fact, the safeguards rule has been extended by the Federal Trade Commission implementing regulations to "any financial institution that is handling 'consumer information'… [and] a wide range of entities, including: nondepository lenders; consumer reporting agencies; debt collectors; data processors; courier services; retailers that extend credit by issuing credit cards to consumers; personal property or real estate appraisers; check-cashing businesses; mortgage brokers, and any other entity that meets this definition." See "Federal Trade Commission Standards for Safeguarding Customer Information," Final Rule of the Federal Trade Commission, 67 *Fed. Reg*. 36484-94 [codified at 16 C.F.R. Part 314]. See also "Interagency Guidelines Establishing Standards for Safeguarding Customer information and Rescission of Year 2000 Standards for Safety and Soundness," Final Rule of the Office of the Comptroller of the Currency, Office of Thrift Supervision, Federal Reserve System, and Federal Deposit Insurance Corporation Final Rule, 66 *Fed. Reg*. 8616-41, implementing the safeguards rule of the GLB Act.

[41] The terms "personal information" or "personally identifiable information," as used by the FTC, "mean individually identifiable information from or about an individual consumer including, but not limited to: (a) a first and last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information; (d) a telephone number; (e) a Social Security number; (f) credit or debit card information, including card number, expiration date, and security code; (g) a persistent identifier, such as a customer number held in a "cookie" or processor serial number, that is combined with other available data that identifies an individual consumer; and (h) information that is combined with any of (a) through (g) …" In the Matter of Life is Good Inc. and Life is Good Retail Inc., Agreement Containing Consent Order of the FTC, File No. 072 3046, Jan. 17, 2008, p. 3, number 1.

including accounting for areas such as employee management and training, information systems management, and system failure planning.

Workshop participants explained that developing an appropriate written information security program to safeguard personal consumer information requires institutions to take a number of steps. These steps include: (1) designating an employee or employees to coordinate safeguards; (2) identifying and assessing risks (while evaluating the effectiveness of current safeguards for controlling the risks); (3) designing and implementing written policies and procedures to manage risks;[42] (4) developing a response plan; (5) evaluating and adjusting the program as needed; and (6) carefully considering the services provided by third parties. Participants also noted that financial institutions, which under implementing regulations include a broad range of businesses,[43] must have information security plans in place and cannot represent to consumers that their information is protected if in fact it is not—or is not to the degree represented.[44] Overall, responses have been positive to the safeguard rule's implementing regulations and to actions related to the safeguard rule.[45] Consumer[46] and business[47] representatives have expressed approval for what they view as a step in the right direction, indicating that both parties recognize the importance of comprehensive data safeguards in today's technological environment.

Last, provisions of the Gramm-Leach-Bliley Act seek to safeguard against pretexting by requiring financial institutions to protect consumers' information and by making it a crime for an individual to attempt to fraudulently access another's confidential information. As previously mentioned,

[42] See pp. 12-14, noting that the FACT Act requires financial institutions covered under the GLB Act to incorporate rules about disposing of consumer data into written information security program practices required by the GLB Act.
[43] See n. 40.
[44] For more information on enforcement actions related to the safeguards rule, see "FTC Enforces Gramm-Leach-Bliley Act's Safeguards Rule Against Mortgage Companies," Federal Trade Commission Press Release, Nov. 16, 2004, pp. 1-2.
[45] See John Schwartz, "Settling with F.T.C., Microsoft Agrees to Privacy Safeguards," *New York Times,* Aug. 9, 2002.
[46] See, for example, the letter from Calvin R. Ashley, on behalf of numerous individuals, to the secretary of the Federal Trade Commission, dated Oct. 9, 2000, expressing support for the safeguards rule, available at: www.ftc.gov/os/comments/glbcommentextension/ashley.htm.
[47] See, for example, the Oct. 15, 2001, letter from Ken Brandt, managing director of Tiger Testing, to the secretary of the Federal Trade Commission, characterizing the safeguards rule as "a move in the right direction: toward increased systems and privacy safeguards" available at: www.ftc.gov/privacy/glbact/safeguard/tiger.htm.

pretexting is when a person, without authority to do so, attempts to gain access to the personal information of another by creating a false scenario. Examples of pretexting include impersonating the true account holder on the phone, by mail, or by e-mail, or using a fictitious website or e-mail that directs or solicits an individual to enter his or her personal information into fields that are captured (a practice commonly known as "phishing").[48] Moreover, evidence gathered on the prevalence and nature of phishing attacks indicates that this form of pretexting is a growing and evolving threat.[49] To defend against pretexting, section 501 of the GLB Act requires financial institutions to "protect the security and confidentiality of [their] customers' nonpublic personal information"[50] and to put safeguards in place to "to protect against unauthorized access to or use of [consumers'] records or information that could result in substantial harm or inconvenience to any customer."[51] Additionally, section 521 of the GLB Act makes it a crime for an individual to obtain consumer information by false pretenses or to solicit another to obtain consumer information from a financial institution under false pretenses.[52] Together, these provisions form the collective pretexting protections. Because pretexting is often a prelude to subsequent criminal offenses, such as payment fraud or identity theft,[53] forcing financial institutions to create policies that recognize and seek to mitigate the effects of pretexting is a major focus of regulatory and law enforcement agencies.[54] Currently, regulatory agencies and financial institutions are taking steps to educate consumers on how to identify such pretexting attempts, and technology providers are working to develop mechanisms to block unauthorized web-based phishing attacks.

---

[48] For examples of cases of pretexting, see *Federal Trade Comm'n v. Hill*, Civ. Action No. H03-5537 (SD Tex. Dec. 3, 2003); press release, "FTC Charges Telemarketing Network with Selling Bogus Advance-Fee Credit Card Packages," Federal Trade Commission, Jan. 17, 2003; and press release, "Justice Department Halts Identity Theft Scam," Federal Trade Commission, March 22, 2004.

[49] Anti-Phishing Working Group, "Phishing Activity Trends Report, Q1/2008," (Jan.–March 2008), pp. 2-4, available at: www.antiphishing.org/reports/apwg_report_Q1_2008.pdf.

[50] Codified at 15 U.S.C. § 6801(a) (2007).

[51] Codified at 15 U.S.C. § 6801(b)(3) (2007).

[52] Codified at 15 U.S.C. §§ 6821(a) & (b) (2007); and made a criminal offense under 15 U.S.C. § 6823 (2007).

[53] For more information on crimes frequently committed in connection with pretexting, see "Pretexting: Your Personal Information Revealed," FTC Facts for Consumers (Feb. 2006), available at: www.ftc.gov.

[54] See "Prepared Statement by the Federal Trade Commission Before the U.S. House of Representatives Committee on Energy and Commerce on 'Combating Pretexting: H.R. 936, Prevention of Fraudulent Access to Phone Records'," March 9, 2007, pp. 5-7, available at: www.ftc.gov/os/testimony/P065409CommissionTestimonyReCombatingPretextingandHR936House.pdf (accessed Dec. 5, 2008).

III. Data Disposal, Receipt Truncation, and Red Flag Requirements of the Fair and Accurate Credit Transactions Act

Also discussed during the workshop were consumer data protection and identity theft prevention rules contained in the Fair and Accurate Credit Transactions Act (FACT Act) of 2003,[55] including a provision that addresses the disposal of personal consumer information[56]– which was designed to prevent criminals from obtaining complete credit and debit card information from transaction records,[57] and a set of provisions that require businesses to take particular actions to prevent identity theft when certain events commonly associated with fraud take place.[58] Under section 216 of the FACT Act, also known as the FACT Act data disposal section, federal banking agencies must "issue final regulations requiring any person that maintains or otherwise possesses consumer information, or any compilation of consumer information, derived from consumer reports for a business purpose to properly dispose of any such information or compilation."[59] The Fed, FTC, FDIC, OCC, and OTS have each enacted consumer data disposal protocols under section 216.[60] Under section 113 of the FACT Act, also known as the receipt truncation provision, "no person that accepts credit cards or debit cards for the transaction of business [and electronically prints receipts] shall print more than the last 5 digits of the card number or the expiration date upon any receipt provided to the cardholder at the point of the sale or transaction."[61] Under section 114 of the FACT Act, also known as the FACT Act red flag provisions, federal banking agencies must establish and maintain guidelines designed to prevent identity theft, prescribe regulations

[55] The Fair and Accurate Credit Transactions Act of 2003, Public Law 108-159, Dec. 3, 2003, codified at 15 U.S.C. § 1681 et seq. (2007). For a chart that juxtaposes sections of the FACT Act with corresponding sections of the Fair Credit Reporting Act, go to: www.bankersonline.com/tools/facta_chart_updated.pdf.
[56] Codified at 15 U.S.C. § 1681w.
[57] Codified at 15 U.S.C. § 1681c(g).
[58] Codified at 15 U.S.C. §§ 1681m(e) & 1681c(h).
[59] Codified at 15 U.S.C. § 1681w(a)(1).
[60] See "Proper Disposal of Consumer Information Under the Fair and Accurate Credit Transactions Act of 2003," Final Rule of the Office of the Comptroller of the Currency, Federal Reserve System, Federal Deposit Insurance Corporation, and Office of Thrift Supervision, 69 *Fed. Reg*., pp. 77610-21, available at: www.federalreserve.gov/boarddocs/press/bcreg/2004/20041221/attachment.pdf (accessed Aug. 20, 2008) [effective July 1, 2005]; and "Disposal of Consumer Report Information and Records," Federal Trade Commission Final Rule, 69 *Fed. Reg.,* pp. 68690-01 (codified at 16 C.F.R. § 682) [effective June 1, 2005], implementing the FACT Act's data disposal requirements.
[61] Codified at 15 U.S.C. § 1681c(g).

that require financial institutions and creditors to establish policies and procedures implementing those guidelines, and "prescribe regulations applicable to card issuers to ensure" that address changes received contemporaneously with requests for new cards are screened.[62] Under section 315 of the FACT Act, also known as the address discrepancy section (and which accompanies the red flag rules in subsequent rulemaking), the federal banking agencies must "prescribe regulations providing guidance regarding reasonable policies and procedures that a user of a consumer report should employ when such user has received a notice" that there is an address discrepancy between an address reported and one already in a consumer credit report.[63] The Fed, FTC, FDIC, OCC, OTS, and NCUA enacted red flag and address discrepancy rules that went into effect November 1, 2008.[64]

Noting that section 216 of the FACT Act "is designed to protect a consumer against the risks associated with unauthorized access to information about the consumer," "such as fraud and related crimes including identity theft,"[65] the OCC, Fed, FDIC, and OTS (collectively referred to as the agencies) have implemented the FACT Act's data disposal requirements by amending the Interagency Guidelines Establishing Standards for Safeguarding Customer Information to include consumer data disposal guidelines.[66] Under the amended guidelines, now called the Interagency Guidelines Establishing Standards for Information Security,[67] and supplemental information, institutions regulated by the agencies are "expect[ed]" or "generally require[d]" "to adopt procedures and controls to properly dispose of 'consumer information' and 'customer information,'"[68] and to "develop, implement, and maintain [such

[62] Codified at 15 U.S.C. §§ 1681m(e)(1)(A), (B) & (C).
[63] Codified at 15 U.S.C. § 1681c(h)(2)(A).
[64] "Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003," Final Rule of the Office of the Comptroller of the Currency, Federal Reserve System, Federal Deposit Insurance Corp., Office of Thrift Supervision, National Credit Union Administration, and Federal Trade Commission, 72 *Fed. Reg*., pp. 63718-75, available at: www.ftc.gov/os/fedreg/2007/november/071109redflags.pdf (accessed Sept. 12, 2008) [effective Nov. 1, 2008].
[65] *"*Proper Disposal of Consumer Information Under the Fair and Accurate Credit Transactions Act of 2003," Final Rule, Supplementary Information, p. 3, and 69 *Fed. Reg*., p. 77610.
[66] 69 *Fed. Reg*., pp. 77610-21.
[67] 69 *Fed. Reg*., p. 77610.
[68] *"*Proper Disposal of Consumer Information Under the Fair and Accurate Credit Transactions Act of 2003," [n. 65] Final Rule, Supplementary Information, p. 11.

procedures and controls], as part of [their] existing information security program[s]."[69] Indeed, criminal use of consumer information that has been disposed of for the purpose of stealing consumer identities has been well established.[70] Moreover, the use of disposed of information in phishing attacks—where fraudsters use already obtained information to attempt to gain other information that can then be used to commit fraud—is also well documented.[71] For these reasons, Subpart I of the guidelines requires covered institutions to "properly dispose of any consumer information" that is in their possession.[72] The guidelines define "consumer information" as "any record about an individual, whether in paper, electronic, or other form, that is a consumer report or derived from a consumer report and that is maintained or otherwise possessed by or on behalf of the [covered institution] for a business purpose," including any "compilation of such records,"[73] and require that all consumer information be disposed of "in accordance with the Interagency Guidelines Establishing Information Security Standards," and that consumer information be disposed of pursuant to information security programs implemented by covered institutions.[74] In accordance with these rules and guidelines, the agencies advise that "an institution's information security program should ensure that paper records containing either customer or consumer information should be rendered unreadable as indicated by the institution's risk assessment, such as by shredding or other means."[75] Moreover, the agencies advocate that "[i]nstitutions … should recognize that computer-based records present unique disposal problems," such that "additional disposal techniques should be applied to

[69] 69 *Fed. Reg.*, p. 77610.
[70] See, for example, Alexia Elejalde-Ruiz, "Identity Crisis; as Society Gets More High-Tech, So Do the Thieves of Personal Information," *Chicago Tribune*, Aug. 18, 2008, RedEye, p. 6 (noting that 20 percent of reported identity thefts involve a nontechnological method of obtaining confidential consumer victim information, such as dumpster diving); and Frank Abagnale, "If You Make It Easy, Someone Will Steal from You," *Richmond Times-Dispatch*, Aug. 3, 2008, p. E4 (identifying "traditional" methods of perpetrating identity theft and advising consumers to shred credit card statements, bank statements, and credit card offers).
[71] See, for example, "Credit Card Inquiry May Be from Thief," *Allentown Morning Call*, Aug. 21, 2008, p. B3 (detailing a phishing attack in which the perpetrator used information obtained from dumpster diving or a low-tech means of information theft to perpetuate fraud on consumers by impersonating their credit card company so as to obtain sufficient information to commit identity theft).
[72] 69 *Fed. Reg.*, pp, 77616-21, Subpart I.
[73] 69 *Fed. Reg.*, pp. 77616-21, definitions of "consumer information," and provisions entitled "Disposal of consumer information."
[74] 66 *Fed. Reg.*, pp. 8632-41.
[75] "Proper Disposal of Consumer Information Under the Fair and Accurate Credit Transactions Act of 2003," [n. 65] Final Rule, p. 11.

sensitive electronic data" and the disposal of "[r]esidual data [that] frequently remains on media after erasure" is ensured.[76]

Making sure that organizations properly dispose of consumers' information is of interest to both federal and state policymakers intent on protecting consumers. To ensure that state regulators are not unduly inhibited by the legislation, a provision of the FACT Act's consumer data disposal requirements states that the act "does not annul, alter, affect, or exempt any person subject to the [act] from complying with the laws of any State" and notes that state laws will be unaffected by the act unless they are found to be inconsistent with federal legislation.[77] In fact, several states now provide consumers with added protection against identity theft through laws that stipulate further requirements for disposing of consumer records[78] or create identity theft resolution programs designed to assist victims and prevent further damage in the aftermath of identity theft.[79] The point was raised during the workshop that issues related to the disposal of consumer records are likely to continue to be a popular topic among state legislatures as legislators seek to prevent low-tech forms of data taking, such as dumpster diving, and related fraud. Dumpster diving, delving into the trash for confidential consumer information, is recognized as a "top tactic"[80] of identity thieves and is linked to as much as 20 percent of all identity theft cases.[81] As noted earlier,[82] in order to help prevent precisely this sort of access to consumer information, a provision of the

[76] See n. 75.
[77] Sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003, codified at 15 U.S.C. §§ 1681m(e)(1)(A), (B) & (C), and § 1681c(h), respectively.
[78] Hawaii, Indiana, and Texas, for example, have all enacted laws that govern the disposal or destruction of consumer records.
[79] For more information on one such program in Nevada, see Jean Mitchell, "State Offers Help with Identity Theft Consequences," *Reno Gazette-Journal*, Aug. 22, 2008, p. 14.
[80] Phil Mulkins, "Take Steps to Thwart Identity Thieves," *Tulsa World*, Aug. 27, 2008, p. E4. See also Christopher Conkey, "Politics & Economics: Identity Thieves, Methods More Diverse That Believed, Study Finds," *Wall Street Journal*, Oct. 20, 2007, p. A5, detailing a study finding that approximately half of all identity thefts perpetrated between 2000 and 2007 made use of the Internet or other technological means, and that the remaining half were low tech.
[81] See "Identity Crisis; as Society Gets More High-Tech, So Do the Thieves of Personal Information," [n. 70].
[82] See pp. 11-12, herein.

FACT Act,[83] in effect for all businesses since 2006, requires credit and debit card information to be shortened by merchants who print receipts.[84]

A separate set of provisions of the FACT Act requires covered institutions to develop procedures that help identify actions or tactics commonly used by identity thieves.[85] As part of red flag and address discrepancy regulations that implement the FACT Act, released in October of 2007,[86] financial institutions[87] must develop and "implement a written Program to detect, prevent and mitigate identity theft in connection with the opening of an account or an existing account."[88] While such programs are to "be tailored to an entity's size, complexity and [the] nature of its operations," organizations covered under the rules must "[i]dentify relevant Red Flags for [incorporation] into the Program" as well as "[d]etect Red Flags that have been incorporated into the Program; [r]espond appropriately to any Red Flags that are detected to prevent and mitigate identity theft; and [e]nsure the Program is updated periodically, to reflect changes in risks to customers or to the safety and soundness of the financial institution or creditor from identity theft."[89] A "red flag" is defined as "a pattern, practice or specific activity that indicates the possible existence of identity theft."[90] The rules enumerate some 26 red flags and include, for example, the provision by a person of suspicious-looking documents or information, the receipt of a notice from a consumer credit reporting agency that an individual's file is frozen or that there is a discrepant address on

[83] Codified at 15 U.S.C. § 1681c(g).
[84] Noting that fraudsters and identity thieves frequently look for consumer card information printed on sales receipts, and characterizing receipts with full credit or debit card numbers and expiration dates as a "golden ticket" for identity thieves, the FTC has issued guidance to businesses to help them understand the importance of printing receipts containing truncated information; see "FTC Business Alert, Slip Showing?," *FTC Business Alert Bulletin* (May 2007), p. 1.
[85] Codified at 15 U.S.C. §§ 1681m(e) & 1681c(h).
[86] See press release, "Agencies Issue Final Rules on Identity Theft Red Flags and Notices of Address Discrepancy," Board of Governors of the Federal Reserve, Oct. 31, 2007.
[87] For more information on who must comply with these rules see Federal Trade Commission, "New 'Red Flag' Requirements for Financial Institutions and Creditors Will Help Fight Identity Theft," *FTC Business Alert Bulletin* (June 2008), pp. 1-2.
[88] See "Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003," Final Rule, at Subparts J [n. 64].
[89] See "Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003," Final Rule, pp. 63719-20 [n. 64].
[90] See "Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003," Final Rule, p. 63723 [n. 64].

file, or, the use of a newly applied for line of credit for expenditures commonly associated with fraud.[91] Under the address discrepancy portion of the regulations, financial institutions that receive notice from consumer reporting agencies that there is a difference between the address they have provided and the consumer's addresses on file with the agency must take steps to verify that the "consumer report relates to the consumer about whom [the information has been] requested."[92] Such verification steps, which must establish a reasonable belief that the consumer is who he or she purports to be, include comparing the address with previously held information, obtaining corroborative information from third-party sources, and contacting the consumer to confirm.

Overall, the red flag and address discrepancy rules, which went into effect on November 1, 2008, have met with a mixed response. While state agencies, such as New York state's Consumer Protection Board, and credit reporting agencies have expressed support for the rules, characterizing them as "a positive step forward,"[93] many organizations have conveyed concern. Canadian banks with both American and Canadian customers have noted that they will be forced either to differentiate between their customers, implementing some sort of earmarking system, or to simply "extend blanket coverage" as a result of U.S. regulation.[94] Moreover, and reflecting the challenges that many nonbanks covered under the act face, the National Automobile Dealers Association (NADA) has opposed the rules. The NADA has argued that many dealers will be unable to meet the onerous burden of detecting fraud and identity theft, and that recognizing activities that indicate fraud is simply beyond the many dealers' or dealerships' abilities.[95] And while some American banks have also expressed displeasure with the rules— for

[91] See "Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003," Final Rule, at Supplement A to Appendix J [n. 64].
[92] See "Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003," Final Rule, at Subpart I [n. 64].
[93] Press release, "Identity Theft Red Flag Rules Help Banks and Credit Card Companies Protect Consumers' Identities," New York State Consumer Protection Board, available at: www.consumer.state.ny.us/id_theft_red_flag_rules.htm (accessed Sept. 19, 2008); Inc.com, "Experian to Support Red Flag Rules," *New York Times*, at nytimes.com, April 22, 2008.
[94] Kathleen Lau, "U.S. 'Red Flag' Rules Could Affect Canadian Banks," *ComputerWorld Canada*, Aug. 19, 2008.
[95] Steve Finlay, "Red-Flag Rules Worry Dealers," *Ward's Dealer Business News*, wardsauto.com, Dec. 1, 2007; Steve Santiago, "New Red Flag Rules to Stem ID Theft," bankrate.com article, as reported by Yahoo Finance News, May 27, 2008, at "Who opposes the rules?"

example, the Illinois Bankers Association called them "excessive and overly burdensome"[96]—most domestic financial institutions have simply communicated apprehension that compliance, training, and ongoing implementation will require a considerable expenditure of resources.[97] Indeed, a recent survey of 300 financial institutions found that almost half will "either barely meet or will miss the [November 1 red flag and address discrepancy rule] deadline."[98] Nonetheless, and despite these concerns, many banks have praised regulators for taking into consideration that not all financial institutions are alike and for providing flexibility surrounding the creation of fraud detection programs under the rules.[99] In the end, many technology security experts view these rules as necessary in today's digital environment. Danny Shaw, a risk management expert with the technology auditing firm of Jefferson Wells, notes that financial institutions simply "need to look at this as part of their normal best practice."[100] Moreover, Heather Grover, a director of product management for Experian, believes "that many [financial institutions] will eventually come around when they see the benefits of protecting their customers, as well as a decrease in fraud losses."[101]

IV. State Laws About Social Security Numbers

When the federal government established a system of assigning Social Security numbers to Americans in 1936, its primary purpose was to create a system whereby workers' wages could be tracked and eligibility for retirement benefits could be determined.[102] At the time, the role that Social Security numbers would come to play for today's consumers and their eventual (and resulting) popularity among

[96] "New Red Flag Rules to Stem ID Theft" [n. 95], quoting an Illinois Bankers Association position letter to the FDIC.
[97] Steve Garmhausen, "The Tricky Business of Identity Theft Compliance," *American Banker,* April 8, 2008.
[98] See "U.S. 'Red Flag' Rules Could Affect Canadian Banks" [n. 94], citing a BankInfoSecurity survey of financial institutions on their readiness to implement red flag and address discrepancy rules.
[99] Joe Adler, "FACT Act Rules Have Some Give," *American Banker,* Oct. 17, 2007.
[100] "U.S. 'Red Flag' Rules Could Affect Canadian Banks" [n. 94].
[101] "New Red Flag Rules to Stem ID Theft" [n. 95], reporting remarks made by Heather Grover.
[102] California Office of Privacy Protection, *Recommended Practices on Protecting the Confidentiality of Social Security Numbers* (April 2008), p. 5.

data thieves was unforeseeable.[103] Indeed, Social Security numbers have become a favorite target for cyber criminals, a "crown jewel"[104] of consumers' personal information, a "magic key" for identity thieves.[105] The Government Accountability Office has noted that Social Security numbers "are a key piece of information used to create false identities for financial misuse or assume another individual's identity," and that "[m]ost often, identity thieves use Social Security numbers belonging to real people."[106] Nonetheless, and despite widespread recognition that fraudsters often make use of others' Social Security numbers, on the Internet the numbers are frequently available for purchase,[107] are posted inadvertently,[108]are available as a result of court proceedings,[109] or are readable on imaged documents made available by the government.[110]

Seeking to reduce the sale, availability of, and the resulting fraudulent use of Social Security numbers,[111] more than 42 states have, since 2005,[112] enacted some form of law that regulates the use of, or

[103] For a report detailing the importance of Social Security numbers to identity thieves and vulnerabilities generated by the widespread use of Social Security numbers today, see Government Accountability Office, *Social Security Numbers: Federal Actions Could Further Decrease Availability in Public Records, Though Other Vulnerabilities Remain*, GAO-07-752 (June 2007), available at: http://www.gao.gov/new.items/d07752.pdf.
[104] Heather Mark, "Personal Security Authentication," *Transactions World Magazine* (July 2008), p. 1.
[105] Daniel Solove, prepared testimony and statement of Daniel J. Solove, Associate Professor of Law, George Washington University Law School, Before the U.S. House of Representatives Committee on Energy & Commerce Hearing on Securing Consumers' Data: Options Following a Data Breach, May 11, 2005, p. 5.
[106] *Social Security Numbers: Federal Actions Could Decrease Availability in Public Records,* [n. 103] p. 14.
[107] See Jonathan Krim, "Net Aids Access to Sensitive ID Data, Social Security Numbers Are Widely Available," *Washington Post*, April 4, 2005, p. A01.
[108] See Bill Hendrick, "Insurance Records of 71,000 Ga. Families Made Public," *Atlanta Journal-Constitution,* April 8, 2008.
[109] See Glenn Hagele, "Whistleblower's Social Security Number Published; Court Orders Internet Data Blocked," Reuters /PRNewswire article, Dec. 12, 2007, noting that an individual's Social Security number was recently found posted to various websites after it was obtained from court documents and posted to the Internet as the result of a retaliatory action; and *Greidinger v. Davis*, 988 F.2d 1344 (4th Cir. 1993), addressing whether a voter could be compelled to disclose his or her Social Security number, which would then be published in public voting rolls.
[110] See Damon Darlin, "Think Your Social Security Number Is Secure? Think Again," *New York Times*, at nytimes.com, Feb. 24, 2007, and Government Accountability Office, *Social Security Numbers: Federal and State Laws Restrict Use of SSNs, Yet Gaps Remain*, GAO-05-1016T, p. 7 (Sept. 2005).
[111] For example, the preamble to Georgia Senate Bill 475 states that the legislation's purpose is "[t]o amend various provisions of the Official Code of Georgia Annotated as they relate to identity fraud and the collection and dissemination of personal identifying and financial information on individuals and businesses so as to protect such information from being utilized in an unlawful manner; to amend Title 16 of the Official Code of Georgia Annotated, relating to crimes and offenses, so as to change provisions relating to definitions, financial identity fraud, and racketeer influenced and corrupt organizations."
[112] For a survey of enacted state laws concerning Social Security numbers by year, visit the National Conference of State Legislatures' website at www.ncsl.org. The site's search function will yield results on these laws (visited and searched Aug. 20, 2008).

mandates a particular method for protecting, Social Security numbers.[113] However, the range of these laws is broad. Similar to the safeguards rule of the GLB Act, a number of state laws require written confidentiality policies designed to protect Social Security numbers; other state laws require that interorganizational access to Social Security numbers be limited to authorized personnel only; and still other state laws create requirements for disposing of documents containing Social Security numbers similar to the FACT Act's requirements for disposing of personal consumer information. Despite this range, the most common types of state legislation concerning Social Security numbers come in the form of laws that: (1) prohibit companies from printing the numbers on identification cards or other materials; (2) restrict the intentional communication of Social Security numbers, whether by mail or public posting; or (3) require that Social Security numbers be truncated, erased, or otherwise modified.[114] Arizona law, for example, prohibits the printing of Social Security numbers on identification cards and the intentional disclosure of the numbers to the general public and sets standards for the transmission of Social Security numbers over the Internet.[115] Meanwhile, Colorado and Georgia laws set special disposal requirements for Social Security numbers.[116] Georgia law requires Social Security numbers contained on paper records to be shredded and that they be completely erased when contained on electronic records, or to otherwise be "modifie[d]" so as to be "unreadable."[117] However, some states have taken a more comprehensive approach.

California law provides an illustration of how comprehensive state legislation can operate. Generally recognized as the first state to enact privacy protections for Social Security numbers, California phased in Civil Code sections 1798.85 through 1798.89 from 2001 to 2005.[118] Under section 1798.5, "a person or entity" (including businesses and other organizations) may not: (1) publicly post or display a

[113] For more information on these laws, see "Social Security Number Protection Legislation for States," ConsumersUnion.org, available at: www.consumersunion.org/pub/core_financial_services/004801.html (accessed Sept. 15, 2008).
[114] "Social Security Number Protection Legislation for States" [n. 113], providing groupings of various types of state laws concerning Social Security numbers.
[115] See Arizona House Bill 2429 (46th Legislature, First Regular Session, 2003).
[116] See Colorado House Bill 06-1156 (signed into law, March 2006), and Georgia Senate Bill 475 (2002).
[117] Georgia Senate Bill 475 (2002).
[118] Cal. Civ. Code §§ 1798.85 & 1798.89 (2002); phased in under § 1798.85(d); available at: www.leginfo.ca.gov/calaw.html.

Social Security number in any way; (2) print a Social Security number on any card required to access products or services; (3) require an individual to transmit his or her Social Security number over the Internet unless the connection is secure and the number is encrypted; (4) require an individual to use his or her Social Security number alone to access a website; (5) print a Social Security number on mailed materials in many circumstances; or (6) encode or embed Social Security numbers in cards or documents as a way of avoiding having to remove Social Security numbers under the regulation.[119] Additionally, and to further address emerging issues concerning Social Security numbers, California's legislators created the Office of Privacy Protection.[120] The office is generally charged with "mak[ing] recommendations to organizations for privacy policies and practices that promote and protect the interests of California consumers."[121] Along with researching and identifying consumer privacy issues, the office provides a continually updated set of recommended practices for handling Social Security numbers in a manner tending to maintain confidentiality and in a fashion that complies with the state's laws.[122]

While state laws concerning Social Security numbers have generally sought to create a more structured and secure environment for personal consumer information, issues remain. First, the role that state Social Security number legislation plays is complicated by the fact that businesses have created their own rules about how these numbers ought to be handled. While state laws have some underlying influence over how businesses handle Social Security numbers, federal government interviews of employees at banks, securities firms, telecommunication firms, and tax preparation firms regarding how Social Security numbers are shared with third-party vendors indicate that companies rely primarily on complex commercial contracts and recognized industry practices when deciding what to do.[123] Second, the Government Accountability Office (GAO) has noted that although state laws about Social Security numbers provide "some consistency" in their protection of consumers' information, these laws vary

[119] Cal. Civ. Code § 1798.85(a).
[120] Cal. Gov. Code § 11549.5(a) (2000).
[121] Cal. Gov. Code §§ 11549.5(b) & (c).
[122] See California Office of Privacy Protection, "Recommended Practices on Protecting the Confidentiality of Social Security Numbers" (April 2008), available at: www.privacy.ca.gov.
[123] See Government Accountability Office, *Social Security Numbers: Stronger Protections Needed When Contractors Have Access to SSNs*, GAO-06-238, Jan. 2006, pp. 2-7.

widely. The GAO also found that inconsistency among the intentions of legislatures—particularly between intending to prevent identity theft and intending to increase privacy protections—remains a significant concern that must be addressed.[124] Echoing this notion—that policymakers' understanding of the relationship between failures in information security and fraud is varied—payments industry feedback provided during past conferences sponsored by the Payment Cards Center indicates that confusion abounds in the payments industry concerning the links that connect data breaches, identity theft, and fraud.[125] Indeed, the importance of establishing a common understanding of the differences between failures of privacy protections and fraud is made more prominent by recent research on data breaches and related financial crimes that indicates there is, perhaps, less of a link between data breaches and crimes related to personal consumer information than previously believed. Although the number of data breaches is increasing dramatically,[126] some observers report that the incidence of identity theft is decreasing. One recent study notes that in 2007, 8.1 million Americans suffered identity theft, half a million fewer than the previous year, with related losses dropping 12 percent.[127] A 2007 report by the GAO that looked at the connection between data breaches and subsequent crimes found that of the "24 largest breaches that appeared in the news media from January 2000 through June 2005," three of them seem "to have resulted in fraud on existing accounts, and [one] breach appear[s] to have resulted in the unauthorized creation of new accounts,"[128] a weaker connection than many analysts previously supposed.

V. State Laws About Data Security Breach Notification

The last type of legislation discussed during the workshop was state laws related to notifying consumers about data security breaches or, simply, data breach notification laws. Approximately 39 states

[124] *Social Security Numbers: Federal Actions Could Decrease Availability in Public Records,* [n. 103], p. 19.
[125] See, for example, "Information Security, Data Breaches, and Protecting Cardholder Information," [n. 26], pp.10-21, detailing uncertainties over the interrelatedness between data breaches, poor information security, and identity theft.
[126] Identity Theft Resource Center, "Breaches Blast '07 Record; As of August 22, ITRC's List Surpasses 446 Documented Breaches," PR Newswire, Aug. 25, 2008, p. 1.
[127] Javelin Strategy & Research, "2007 Identity Fraud Survey Report—Consumer Version; How Consumers Can Protect Themselves" (Feb. 2007), p. 1.
[128] *Data Breaches and Identity Theft Report* [n. 1], pp. 5-6.

presently possess a data breach notification law, and 48 states, all but New Mexico and South Dakota, have such a law on their books or have a data breach notification bill pending before their legislature.[129] As was discussed during the workshop, these laws generally require notification of consumers, state agencies, or other parties when unencrypted personal information held in some fashion by an organization is acquired or accessed by an unauthorized person. However, state data breach notification laws differ widely. Statutes diverge over whether they cover both computerized and paper data thefts, what is considered personal information, the manner of notification required, whether they require state agencies to be notified, whether they require credit reporting agencies to be notified, and what types of events trigger notification requirements. A number of states require notification only when there is an identifiable risk of harm to a consumer, while others require notification when information is reasonably believed to have been accessed by an unauthorized party in a manner constituting a breach.

Although state laws about data security breach notification differ, one example of such a law is California's Database Breach Notification Security Act (CDBNSA). California, one of the first states to establish a data security breach notification requirement, enacted the CDBNSA in 2002, with the law going into effect July 1, 2003.[130] Under the CDBNSA, the "owner" or "licens[or]" of personal consumer data must disclose any breach to "any resident of California whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person" once a breach has occurred.[131] The law defines a "breach of the security of [a] system" as an "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information."[132] Personal information is defined as "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 the data elements are not encrypted: (1) Social Security number; (2) driver's license number or California identification card number; (3)

[129] See Donald Aplin, "Data Breaches; Washington House OKs Retailer Liability Bill; Similar Bills Introduced in Alabama, Iowa," Bureau of National Affairs Inc., *Banking Daily* (Feb. 2008), p. 1.
[130] Jeffrey Rawitz, "Security Breach Notification Requirements: Guidelines and Securities Law Considerations," Jones Day Publications (March 2006), p. 1.
[131] Cal. Civ. Code § 1798.29(a) (2002).
[132] Cal. Civ. Code § 1798.29(d).

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; (4) medical information; and (5) health insurance information."[133] It was noted during the workshop that establishing whether notification requirements have been triggered, and drafting a notification is often more complicated than one might imagine. To provide ongoing assistance with this, California offers continually updated guidance on the precise notification requirements essential to the state's mandated data breach reporting process.[134]

Looking further at differences between states' laws, workshop participants pointed out that many states have special or unique requirements when it comes to data breach notification. New York and Maine, for example, require that their attorneys general be notified when a breach has occurred, and New Jersey requires that its state police be notified. Such divergent requirements, it was observed, often make compliance with these laws a difficult task for businesses. Indeed, this issue and, more broadly, businesses' ability to understand what constitutes a breach under states' laws and then to practically establish that a data security breach has occurred (or that the type of data breach that has occurred requires reporting) is receiving national attention as a result of the current prosecution of 11 criminals responsible for stealing consumers' information from several large companies' databases.[135] As the Justice Department has revealed in this case, nine major retailers' systems were ultimately breached in a prolonged attack, and despite the seeming operation of applicable state data breach notification laws, only four retailers—TJX, BJ's Wholesale Club, DSW, and Dave and Buster's—appear to have notified consumers.[136] Two other retailers, Boston Market and Forever 21, initially reported that they "never told customers because they never confirmed data were stolen from them."[137] Moreover, Forever 21 officials

[133] Cal. Civ. Code § 1798.29(e).
[134] See, for example, www.oispp.ca.gov/government/incident.asp#Inci_Othr_Res (accessed Aug. 25, 2008), outlining the steps that must be taken in the wake of a breach.
[135] Jon Swartz, "11 Charged in TJX Identity Theft; Huge Computer Data Breach Hits Nine Major U.S. Retailers," *USA Today*, Aug. 6, 2008, p. B1.
[136] Joseph Pereira, Jennifer Levitz, and Jeremy Singer-Vine, "Some Stores Quiet Over Card Breach—Consumers Not Told About Alleged Theft of Consumer Data," *Wall Street Journal*, Aug. 11, 2008, p. B1.
[137] Id.

have subsequently stated that they have not notified consumers whose information was accessed because the stolen information did not include customer names and addresses and because "they do not believe any of the stolen [information] was used fraudulently."[138] Three more retailers—OfficeMax, Barnes and Noble, and Sports Authority—appear to have remained silent about whether they have made disclosures; the *Wall Street Journal* reported that "computer searches of their Securities and Exchange Commission filings, Web sites, press releases and news archives [concerning these companies] turned up no evidence of such disclosures."[139] These types of challenges—challenges concerning the implementation of data breach notification laws (particularly, the absence of a common understanding among payment industry participants and merchants as to what specific events trigger reporting requirements or constitute risks that must be reported)—were recognized by conference participants during a 2006 Payment Cards Center conference.[140] Those participants noted that confusion about what was required under different types of data breach notification laws "need[ed] to be resolved [in order for] the [legal] framework [to be] effective, intelligible, and viable for organizations that act nationally and internationally."

The final issues addressed during the workshop surrounded the impact that state data breach notification laws have on consumers, including how consumers respond in the wake of a data breach or suspected breach. Workshop participants noted that while many notices satisfy the basic legal requirements to explain obligations and rights accurately, notices, at times, may appear to fall short when providing explanations that are meaningful to their readers. To help resolve this problem and deal with difficult issues surrounding data breach notices, government agencies, consumer advocacy groups, and state regulators all make resources available to businesses to help craft clearer notices—notices that are capable of providing consumers with useful information in language that consumers are likely to understand.[141] Looking beyond whether consumers understand the data breach notices they receive, one

[138] Bethany Clough, "Forever 21 Breach Hits Fresno Store," *Fresno Bee*, Sept. 24, 2008.
[139] "Some Stores Quiet Over Card Breach" [n. 136], p. B1.
[140] See "Information Security, Data Breaches, and Protecting Cardholder Information" [n. 25], p. 20, discussing challenges in implementing data breach laws.
[141] Sample notices, notice content, and other resources are provided by the Federal Trade Commission, not-for-profit anti-fraud groups, and many state agencies. See, for example, www.ftc.gov/bcp/edu/microsites/idtheft/business/data-

workshop attendee noted that consumers often behave in ways that are difficult to predict. This phenomenon was recently addressed during a 2008 Payment Cards Center conference on fraud, when payments industry experts noted that there appears to be a significant disparity between what consumers say they will do after receiving a data breach notification and what they actually do.[142] Although consumers frequently report that they will stop shopping at a merchant deemed responsible for a data breach leading to the compromise of their personal information, conference participants noted that in many cases these same merchants report increased sales levels after a publicized breach. Additional awareness of discrepancies between what consumers do and say, the effects of state data breach notification laws, and the connections between data breaches and identity theft generally[143] is being generated by a recent Carnegie Mellon University study that analyzes data from the FTC in an attempt to measure the "impact of data breach disclosure laws on identity theft over the years 2002 to 2006." [144] Using "state and year fixed effect regression analysis to empirically estimate the impact of data breach laws," the study finds *"no statistically significant"* evidence that data breach notification laws reduce identity theft, "even after considering income, urbanization, strictness of law and interstate commerce."[145] While the authors of the Carnegie Mellon study admit that there may be some issues with the underlying methodology used in the study,[146] and payments industry data security analysts have noted that it is

---

breach.html (accessed Nov. 24, 2008). See also n. 134, referencing an informational website made available by California regulators.

[142] Susan Herbst-Murphy, "Maintaining a Safe Environment for Payment Cards: Examining Evolving Threats Posed by Fraud," Payment Cards Center Conference Summary (April 23-24, 2008) [forthcoming].

[143] See Robert McMillan, "Researchers Say Notification Laws Not Lowering Theft," IDG News Service, June 4, 2008, quoting payments information security expert Avivah Litan, who notes that "thieves are just getting better and there's more fraud," and that "[i]f you talk to the largest banks, they will tell you that fraud has really increased in the past 18 months." See also Paul Damiano, "Online Security, Great Expectations, Banks Are Challenged to Meet Consumers' Expectations for Online Security," *Bank Systems and Technology* (June 2008), p. 14, discussing evolving challenges faced by banks in combating attacks on their information systems; and "Information Security Data Breaches, and Protecting Cardholder Information: Facing Up to the Challenges," [n. 25], pp. 14-19.

[144] Sasha Romanosky, Rahul Telang, and Alessandro Acquisti, "Do Data Breach Disclosure Laws Reduce Identity Theft?" abstract from the Seventh Workshop on the Economics of Information Security (2008), p. 1 [the full study is forthcoming].

[145] See "Do Data Breach Disclosure Laws Reduce Identity Theft?" [n. 144], p. 3 (emphasis added).

[146] See "Do Data Breach Disclosure Laws Reduce Identity Theft?" [n. 144], pp. 12-15.

difficult to draw conclusions from the study because the underlying data (reports submitted by consumers to the FTC) are often incomplete,[147] they note that the FTC remains the only source for this kind of data.

Summing up the state data breach notification law portion of the workshop, attendees acknowledged that while the potential for consistent data breach regulations or standards has been well recognized by payments industry participants,[148] recent research suggests that more work is needed to better determine what kinds of initiatives might be most effective in preventing fraud and protecting consumers. However, they recognized that any organization that possesses or handles consumers' personal information needs to be prepared for an attack on its data security systems. Workshop participants noted that irrespective of nuances in states' data breach notification laws, it simply makes sense to be prepared for a breach in today's technological environment—one where wireless devices abound, remote access is commonplace, and the services of third-party consultants and vendors are necessary.[149]

VI. Conclusion

For more than a decade federal and state legislators have sought to create a more structured and secure environment for private consumer data and to help protect consumers whose personal information has been compromised; however, challenges and issues remain. These include forming a better understanding of the links that connect data breaches, identity theft, and fraud; establishing more universally understood data breach notification requirements for businesses (or even a commonly recognized definition for data breaches); overcoming obstacles related to consumers (such as ensuring that consumers understand breach, opt-out, or policy notices they receive and avoiding consumer

[147] See "Researchers Say Notification Laws Not Lowering ID Theft" [n. 143], p. 1.
[148] "Information Security, Data Breaches, and Protecting Cardholder Information: Facing Up to the Challenges" [n. 25], pp. 19-20, detailing conference participants' recognition of the potential of a common standard setting surrounding data breach definitions and notification requirements.
[149] "Data Breaches a Concern to Companies" [n. 8], pp. C1 & C5.

desensitization to these types of information);[150] and creating solutions that are flexible enough to adjust to changes in technology and fraudsters' tactics. Pointing to today's technological environment, one in which wireless devices and remote access are commonplace, workshop participants noted that attacks on data security systems can and will be staged in new and unanticipated ways—something that must be anticipated by policymakers and industry participants alike. Participants also drew attention to the fact that the problem extends well beyond criminal attacks on computer systems, noting that leaked data also originates from the actions of organizations' own employees, whether negligent or intentional. Furthermore, participants also suggested that increasing reliance on third-party data processors, data storage suppliers, and other third-party data service providers will create additional challenges to safeguarding consumers' financial information as massive files containing such information change hands more frequently and come into contact with more individuals. The workshop concluded with participants encouraging the Payment Cards Center to continue promoting critical dialogue and research on these issues as an important contribution to the industry's (and policymakers') efforts to develop effective solutions.

[150] "Researchers Say Notification Laws Not Lowering ID Theft" [n. 143], p. 1, noting that "[m]any consumers simply ignore breach notification letters" because they have been desensitized to receiving them.