Order Code RS22374
February 3, 2006

Data Security: Federal and State Laws

Gina Marie Stevens
Legislative Attorney
American Law Division

Summary

Security breaches involving electronic personal data have come to light largely as a result of the California Security Breach Notification Act, a California notification law that went into effect in 2003. In response, the states and some Members have introduced bills that would require companies to notify persons affected by such security breaches. By December 2005, 35 states had introduced data security legislation and 22 states had enacted data security laws. Numerous data security bills have been introduced in the 109th Congress (S. 115, S. 500, S. 751, S. 768, S. 1216, S. 1326, S. 1332, S. 1408, S. 1594, S. 1789, S. 2169, H.R. 1069, H.R. 1080, H.R. 3140, H.R. 3374, H.R. 3375, H.R. 3397, H.R. 4127). S. 1326, S. 1408, and S. 1789 were reported by Senate committees. This report provides a brief discussion of federal and state data security laws.

The security of personal information and risks to data are paramount concerns addressed in federal and state law, legislation, and regulations. The public disclosure of breaches of customer databases in 2005 heightened interest in the business and regulation of data brokers.[1] Data brokers collect personal information from public and private records and sell this information to public and private sector entities for many purposes, from marketing to law enforcement and homeland security purposes.[2] Recent data security breaches illustrate (1) the risks associated with collecting and disseminating large amounts of electronic personal information, (2) the increased visibility of data security breaches as a result of consumer notice requirements, and (3) the potential risk of harm or injury to consumers from identity theft crimes (e.g., credit card fraud, check fraud, mortgage fraud, health-care fraud, and the evasion of law enforcement). One result of the highly publicized breaches of personal data security has been a new focus on establishing

[1] "In particular, two types of businesses exist in this industry: (1) 'individual reference services providers' (IRSPs), which sell 'profiles' and other reports containing confidential personal information about individuals; and (2) 'marketing list brokers,' which sell lists of names, mailing addresses or electronic mail addresses of individuals, grouped by characteristics, conditions, circumstances, traits, preferences or mode of living." Federal Trade Commission, *Individual Reference Services: A Federal Trade Commission Report to Congress* (Dec. 17, 1997), available at [http://www.ftc.gov/os/1997/12/irs.pdf].

[2] CRS Report RS22137, *Data Brokers: Background and Industry Overview*, by Nathan Brooks.

security standards for safeguarding customer information[3] and imposing security breach notification obligations on entities that own, possess, or license sensitive personal information.

Although no single federal law governs data brokers, other statutes and regulations may be applicable. A review of the laws regulating the use and disclosure of information collected by information brokers appears in CRS Report RL33005, *Information Brokers: Federal and State Laws*, by Angie A. Welborn. In the late 1990s, the Federal Trade Commission (FTC) endorsed self-regulation for the information broker industry as an alternative to comprehensive federal privacy regulation.[4] The FTC also endorsed industry adherence to a set of principles promulgated by the Individual References Service Group (IRSG) to address most of the concerns associated with the increased availability of nonpublic information.[5] Some of the largest information brokers that disclosed data security breaches in 2004 and 2005, such as Axicom and Choicepoint, had signed on to the IRSG principles for the protection of nonpublic information. Nonetheless, Congress chose to regulate the availability of certain types of sensitive information and to establish requirements to protect the confidentiality and integrity of such information.

Federal Data Security Standards. Certain sectors are currently subject to legal obligations to protect sensitive personal information. These obligations were created, in large part, through the enactment of federal privacy legislation in the financial services, health-care, government, and Internet sectors. Federal regulations that support federal privacy laws impose obligations on covered entities, requiring them to implement information security programs that protect personal information.[6]

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires the Secretary of Health and Human Services to issue a rule to implement security standards for health information.[7] The HIPAA Security Standards Rule, which went into effect in April 2005, requires health-care-covered entities to maintain administrative, technical, and physical safeguards to ensure the confidentiality, integrity, and availability of electronic-protected health information; to protect against any reasonably anticipated

---

[3] Consumer data broker ChoicePoint, Inc., which in 2005 acknowledged that the personal financial records of more than 163,000 consumers in its database had been compromised, recently agreed to pay $10 million in civil penalties and $5 million in consumer redress to settle Federal Trade Commission charges that its security and record-handling procedures violated consumers' privacy rights and federal laws. The settlement requires ChoicePoint to implement new procedures to ensure that it provides consumer reports only to legitimate businesses for lawful purposes, to establish and maintain a comprehensive information security program, and to obtain audits by an independent third-party security professional until 2026. *U.S. v. ChoicePoint Inc.* (D. Ct. for the Northern District of Georgia, Atlanta Division), FTC File No. 052-3069 (Jan. 26, 2006), available at [http://www.ftc.gov/opa/2006/01/choicepoint.htm].

[4] CRS Report RL30322, *Online Privacy Protection: Issues and Developments*, by Gina Stevens.

[5] *Individual Reference Services Industry Principles* (Dec. 15, 1997), available at [http://www.ftc.gov/os/1997/12/irsappd.pdf].

[6] Thomas J. Smedinghoff, *The New Law of Information Security: What Companies Need To Do Now*, 22 The Computer & Internet Lawyer 9 (Nov. 2005).

[7] P.L. 104-191, tit. II, subtitle f, § 262, 110 *Stat.* 2025, 42 U.S.C. §§ 1320d *et seq.*; see CRS Report RS21505, *Compliance with the HIPAA Medical Privacy Rule*, by Gina Marie Stevens.

threats or hazards to the security or integrity of such information; and to protect against any unauthorized uses or disclosures of such information.[8] The Children's Online Privacy Protection Act of 1998 (COPPA) requires an owner or operator of a website or online service directed to children, or any operator that collects or maintains personal information from a child, to establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children.[9] The FTC's Safeguards Rule, issued to implement provisions of the Gramm-Leach-Bliley Act of 1999 (GLBA), requires financial institutions to have an information security plan that contains administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of personal consumer information.[10] Interagency guidance issued by the federal banking regulators to implement provisions of the Gramm-Leach-Bliley Act of 1999 requires covered entities to implement information security programs to ensure the security and confidentiality of customer information, protect against anticipated threats or hazards to the security or integrity of such information, and protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.[11] The Federal Information Security Management Act of 2002 requires federal government agencies to provide information security protections for agency information and information systems to provide integrity, confidentiality, and availability.[12]

Under the Federal Trade Commission Act, the Commission is empowered, among other things, to prevent unfair methods of competition and unfair or deceptive acts or practices in or affecting commerce.[13] Using its authority under Section 5, which prohibits unfair or deceptive practices, the Commission has brought a number of cases to enforce the promises in privacy statements, including promises about the security of consumers' personal information. In *BJ's Wholesale Case*, the FTC developed and imposed security procedures pursuant to its jurisdiction over unfair and deceptive trade practices.[14] The settlement requires BJ's to establish and maintain a comprehensive information security program that includes administrative, technical, and physical safeguards. The settlement

---

[8] HIPAA Security Standards for the Protection of Electronic Personal Health Information, 45 C.F.R. Part 164 (Feb. 20, 2003); see CRS Report RL30620, *Health Information Standards, Privacy, and Security: HIPAA's Administrative Simplification Regulations*, by C. Stephen Redhead.

[9] 15 U.S.C. § 6501 *et seq.*, 16 C.F.R. Part 312; see CRS Report RL31408, *Internet Privacy: Overview and Pending Legislation*, by Marcia S. Smith.

[10] Standards for Insuring the Security, Confidentiality, Integrity and Protection of Customer Records and Information, 16 C.F.R. Part 314.

[11] Interagency Guidelines Establishing Standards for Safeguarding Customer Information, 12 C.F.R. Part 30, Appendix B (OCC), 12 C.F.R. Part 208, Appendix D (Federal Reserve System), 12 C.F.R. Part 364, Appendix B (FDIC), and 12 C.F.R. Part 568 (Office of Thrift Supervision); see CRS Report RS20185, *Privacy Protection for Customer Financial Information*, by M. Maureen Murphy.

[12] 44 U.S.C. § 3541 *et seq.*; see CRS Report RL32357, *Computer Security: A Summary of Selected Federal Laws, Executive Orders, and Presidential Directives*, by John Moteff.

[13] 15 U.S.C. §§ 41-58.

[14] *In the Matter of BJ's Wholesale Club, Inc.*, File No. 042 3160 (Sep. 23, 2005), available at [http://www.ftc.gov/os/caselist/0423160/0423160.htm].

also requires BJ's to obtain an audit from a qualified, independent third-party professional that its security program meets the standards of the order and to comply with standard bookkeeping and record-keeping provisions. Similarly, the FTC recently ordered ChoicePoint to establish, implement, and maintain a comprehensive information security program designed to protect the security, confidentiality, and integrity of the personal information it collects from or about consumers. It also required ChoicePoint to obtain, every two years for the next 20 years, an audit from a qualified, independent third-party professional to ensure that its security program meets the standards of the order. ChoicePoint will be subject to standard record-keeping and reporting provisions to allow the FTC to monitor compliance. Finally, the settlement bars future violations of the Fair Credit Reporting Act and the FTC Act.

Federal Data Breach Notification Standards. The imposition of security breach notification obligations on entities that own, possess, or license sensitive personal information is a relatively new phenomenon. As discussed below, California was the first jurisdiction to enact a data breach notification law in 2002. Subsequently, numerous federal and state bills emerged to impose notification requirements on entities that collect sensitive personal information. At the federal level, to date, the only notification requirement that exists is found in guidance issued in March 2005 by the federal banking regulators to interpret the requirements of the GLBA[15] and the Security Guidelines.

The Response Program Guidelines require implementation of a response program to address unauthorized access to or use of customer information maintained by a financial institution or its service provider that could result in substantial harm or inconvenience to any customer, and require disclosure of a data security breach if the covered entity concludes that "misuse of its information about a customer has occurred or is reasonably possible."[16] Pursuant to the guidance, substantial harm or inconvenience is most likely to result from improper access to "sensitive customer information."[17] At a minimum, an institution's response program should contain procedures for (1) assessing the nature and scope of an incident and identifying what customer information systems and types of customer information have been accessed or misused; (2) notifying its

---

[15] Section 501(b) required the Agencies to establish standards for financial institutions relating to administrative, technical, and physical safeguards to (1) ensure the security and confidentiality of customer information, (2) protect against any anticipated threats or hazards to the security or integrity of such information, and (3) protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer. 15 U.S.C. 6801.

[16] Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, Part III of Supplement A to Appendix, at 12 C.F.R. Part 30 (OCC), 12 C.F.R. Part 208 (Federal Reserve System), 12 C.F.R. Part 364 (FDIC), and 12 C.F.R. Part 568 (Office of Thrift Supervision), 70 Fed. Reg. 15736 - 15754 (March 29, 2005).

[17] "Sensitive customer information means 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 access the customer's account, such as user name and password or password and account number." 70 *Fed. Reg.* 15736-15754 (Mar. 29, 2005).

primary federal regulator when the institution becomes aware of an incident involving unauthorized access to or use of sensitive customer information; (3) consistent with the Agencies' Suspicious Activity Report ("SAR") regulations, notifying appropriate law enforcement authorities; (4) taking appropriate steps to contain and control the incident to prevent further unauthorized access to or use of customer information (e.g., by monitoring, freezing, or closing affected accounts and preserving records and other evidence); and (5) notifying customers when warranted. Customer notice may be delayed for an appropriate law enforcement criminal investigation.

State Data Breach Notification Laws. The first data security law was enacted in California in 2002. S.B. 1386, the California Security Breach Notification Act,[18] requires entities to notify customers of security breaches involving their personal information. California requires a state agency, or any person or business that owns or licenses computerized data that includes personal information, to disclose any security breach of data to any resident of the state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. A "breach of the security of the system" is defined by the California law as the "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business." Personal information is defined as the first name or initial and last name of an individual, with one or more of the following: Social Security Number, driver's license number, credit card or debit card number, or a financial account number with information such as PIN numbers, passwords, or authorization codes that could gain access to the account. California provides three exemptions to the notification requirement: for personal information in encrypted form; for criminal investigations by law enforcement; and for breaches that are either immaterial or not "reasonably likely to subject the customers to unauthorized disclosure of personal information." California requires notice be given in the "most expedient time possible and without unreasonable delay," either in writing or by e-mail. If a company can show that the cost of notification will exceed $250,000, that more than 500,000 people are affected, or that an individual's contact information is unknown, notice may be given through media outlets.

Since enactment of the California breach notification law, major data security breaches have been disclosed by several of the nation's largest information brokerage firms, retailers, universities, and federal and state government agencies.[19] The security breaches disclosed in 2005 tended to involve either the creation of fraudulent accounts, stolen laptops or computers, hacking, compromised passwords, insider or employee theft, or lost or misplaced discs or back-up tapes. In response to numerous disclosures of security breaches and public concern, and in the absence of a comprehensive federal data security or data breach notification law, many states have enacted laws requiring consumer notice of security breaches of personal data.[20] The majority of states have introduced or passed bills that would require companies to notify persons affected by

---

[18] Cal. Civ. Code § 1798.82.

[19] See generally CRS Report RL33199, *Personal Data Security Breaches: Context and Incident Summaries*, by Rita Tehan (**Table 1** summarizes selected data security breaches since 2000).

[20] "State Breach Notice Laws Have Similarities, But Significant Differences Require Attention," 89 *Antitrust & Trade Regulation* 176 (Aug. 12, 2005).

security breaches and, in some cases, to implement information security programs to protect the security, confidentiality, and integrity of data.[21]

As of December 2005, 35 states had introduced data security legislation[22] and 22 states had enacted data security laws.[23] The two predominant themes are consumer notification requirements in the event of a data breach and consumer redress. A chart highlighting differences in selected major provisions of the state data breach notification laws was compiled by BNA.[24] Most of the statutes cover private entities and government agencies. The states also impose obligations on service providers to notify the owner or licensor of the data of a breach that occurs. Many of the state laws follow the basic framework of the California breach notification law. The majority of state laws apply to electronic or computerized data only. Notice provisions addressed by the states include description of triggering events, consideration of the level of harm or the risk of misuse that triggers notification, recipients of notification, timing of notice, method of notification, and content of notice. In addition, state laws include exemptions for entities that are regulated under federal privacy laws (e.g., the Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act, or the Interagency Guidelines); expanded definitions of "personal information"; notification requirements to consumer reporting agencies for customers affected by security breaches of personal information; civil penalties for failure to promptly notify customers of a security breach; requirements for the implementation of information security programs; creation of a private right of action to recover actual damages from businesses for failure to notify customers of a security breach in a timely manner; providing consumers the right to place a credit freeze on their credit report; restrictions on the sale and use of social security numbers; and enhanced criminal penalties for identity fraud.

---

[21] Thomas J. Smedinghoff, *Security Breach Notification — Adapting to the Regulatory Framework*, 21 The Review of Banking & Financial Services 115 - 124 (Dec. 2005).

[22] See also *2005 Breach of Information Legislation*, National Conference of State Legislatures at [http://www.ncsl.org/programs/lis/CIP/priv/breach.htm]; see also *50 State Surveys: Financial Services Security Breach Legislation* (West 2005).

[23] Ark. Code Ann. § 4-110-101 *et seq.*, Cal. Civ. Code § 1798.82; 2005 Conn. Acts 148, De. Code Ann. tit. 6, 12B-101 *et seq.*, Fla. Stat. Ann. § 817.5681, Ga. Code Ann. § 10-1-910 *et seq.*, 815 Ill. Comp. Stat. 530/1 *et seq.*, Ind. Code § 1.IC 4-1-10, La. Rev. Stat. Ann. § 51:307 *et seq.*, Me. Rev. Stat. Ann. tit. 10, § 1346 *et seq.*, Minn. Stat. § 325E.61 and § 609.891, Mont. Code Ann. § 30-14-1701 *et seq.*, 2005 Nev. Stat. 465, A.4001, 2005 Leg., 211th Sess. (N.J. 2005), A. 04254, 228th Gen. Assem., Reg. Sess. (N.Y. 2005), N.C. Gen. Stat. § 75-65, N.D. Cent. Code § 51-30-01 *et seq.*, Ohio Rev. Code Ann. § 1349.19 *et seq.*, R.I. Gen. Laws § 11-49.2-1 *et seq.*, 2005 Tenn. Pub. Actd 473, Tex. Bus. & Com. Code Ann. § 48.001 *et seq.*, Wash. Rev. Code § 19.255.010.

[24] "State Breach Notice Laws Have Similarities, But Significant Differences Require Attention," 89 *BNA Analysis & Perspective* 176 (Aug. 12, 2005) (hypertext "Links to Text of State Data Security Breach Consumer Notification Laws" chart included on p. 180).