UNC SCHOOL OF LAW

NORTH CAROLINA BANKING INSTITUTE

Volume 10 | Issue 1 Article 6

2006

Notice Requirements: Common Themes and Differences in the Regulatory and Legislative Responses to Data Security Breaches

Satish M. Kini

James T. Shreve

NOTICE REQUIREMENTS: COMMON THEMES AND DIFFERENCES IN THE REGULATORY AND LEGISLATIVE RESPONSES TO DATA SECURITY BREACHES

SATISH M. KINI
JAMES T. SHREVE*

I. INTRODUCTION

The year 2005 saw a wave of publicity about data security breaches involving personal information from millions of consumers. Not surprisingly, the news set off alarm bells with consumers, who worried about possible identity theft and compromises to personal privacy. The news also prompted new federal banking guidance and spurred frenetic legislative activity on both the state and federal level.

The year started with reports of a large-scale data loss at ChoicePoint, one of the country's largest data brokers. In February 2005, ChoicePoint – which compiles and sells information about consumers, such as information available from mortgage, real estate and government records – revealed that it had sold addresses, names, social security numbers, and other information concerning 126,000 individuals to thieves posing as legitimate businesses. ChoicePoint initially announced its data breach in compliance with a 2002 California law requiring notice to its citizens of such incidents.[1] Nineteen other states' attorneys general then submitted a joint letter to ChoicePoint demanding that the company also give notice to affected consumers in their states, and ChoicePoint agreed to notify affected persons nationwide

The widespread publicity surrounding the ChoicePoint fiasco was followed with front-page news of other data breaches. Indeed, hardly a month passed without yet another high-profile incident. Institution after institution reported problems ranging from the hacking

* Messrs. Kini and Shreve are attorneys in the Washington, D.C. office of Goodwin | Procter LLP.

1. CAL. CIV. CODE §§ 1798.29, 1798.80-1798.84 (2005).

of computer systems to inappropriate use of information by insiders to the loss of laptops and unencrypted computer back-up tapes. Data breaches occurred at banks and other financial services firms, such as Bank of America, Citigroup, ABN AMRO, and MasterCard; at data brokers other than ChoicePoint, such as LexisNexis; at retailers, such as DSW Shoe Warehouse; and at colleges and universities, such as Harvard, MIT, and the University of California.

The data breach at ChoicePoint and the other breaches that followed prompted swift regulatory and legislative reactions. The new rules and laws set forth the actions the covered institutions must take following data security breaches, generally requiring firms to notify customers and potentially affected customers when breaches occur so that these persons may take appropriate steps to protect themselves. For example, in March 2005, the federal bank regulatory agencies (the Office of the Comptroller of the Currency; the Federal Reserve Board; the Office of Thrift Supervision; and the Federal Deposit Insurance Corporation) issued joint guidance requiring banks to develop data breach incidence response programs, a key element of which was customer notice.[2]

In addition, by the end of 2005, twenty-two states and New York City passed laws requiring notice to customers in the event of a security breach. These state bills are generally modeled on the pre-existing California law. Congress also focused on the issue, prompted by an interest in protecting consumers at the federal level and an interest in ensuring a uniform federal standard (rather than a patchwork of state requirements). As of this writing, approximately twenty bills are under consideration in Congress.

This Article examines the bank regulatory guidance, state notice laws, and federal notice legislation responsive to ChoicePoint and other data breaches. Part II reviews the federal bank regulatory guidance. The Article then examines some of the common themes of the various

2. *See* Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 Fed. Reg. 15,736 (Mar. 29, 2005). The bank regulatory guidance had been proposed prior to the news of data breaches. *See* Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 68 Fed. Reg. 47,954 (Aug. 28, 2003). The bank regulators noted that the release of their guidance was not a direct response to ChoicePoint and other high-profile breach incidents, although many suspected differently, given the timing of the guidance.

state data breach notice laws. Although these laws have some significant differences, they also share many common approaches; indeed, on certain elements there is broad agreement. We review these commonalities and differences in Part III of the Article. Part IV of the Article focuses on pending federal data breach notice legislation.

II. FEDERAL BANK REGULATORY GUIDANCE ON DATA BREACHES AND NOTICES

On March 29, 2005, the federal bank regulatory agencies issued guidance, entitled *Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice* (the "Interagency Guidance"), that requires banks, thrifts, and certain other entities (collectively, "banks") to implement response programs to address security breaches that involve customer information.[3]

A. Background and Legal Authority

The Interagency Guidance interprets section 501(b) of the Gramm-Leach-Bliley Act ("GLB Act")[4] and supplements data security guidelines ("Security Guidelines") previously issued by the federal bank regulatory agencies under that statutory section governing administrative, technical, and physical safeguards to customer information.[5] In brief, the Security Guidelines required banks to adopt comprehensive, risk-based information security programs designed to ensure the confidentiality of customer information, to protect against anticipated threats to such information, and to protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to customers.[6]

---

3. The Interagency Guidance generally applies to banks and thrifts, and their subsidiaries; the U.S. branches, agencies, and commercial lending companies of non-U.S. banks; and bank holding companies and certain affiliates of such holding companies, other than broker-dealers, investment advisers, and insurance companies. *See* 70 Fed. Reg. at 15,738 n.6.

4. 15 U.S.C. § 6801 (2000).

5. *See, e.g.*, 12 C.F.R. pt. 30, App. B (2005). The Federal Trade Commission and the Securities and Exchange Commission both issued similar information safeguards requirements that apply to non-bank financial institutions. *See* 16 C.F.R. pt. 314 (FTC) (2005); 17 C.F.R. pt. 248 (2005) (SEC).

6. 12 C.F.R. pt. 30, App. B (2005).

B. *Response Programs*

The Interagency Guidance recognized that – despite the existence of robust security programs, as commanded by the Security Guidelines – breach incidents may and do still occur. As a result, the Interagency Guidance called on banks to develop risk-based response programs that address how they would react to data security breaches.

Specifically, the Interagency Guidance describes the necessary elements of an incident response program, which must include (1) an assessment of the nature and scope of the incident; (2) prompt notice of an incident to the bank's primary federal regulator; (3) notice to the appropriate law enforcement authorities; (4) steps to contain and control the incident, such as by monitoring, freezing or closing compromised accounts, while preserving records and other evidence; and (5) notifying customers "when warranted."[7]

C. *Regulator Notice*

The Interagency Guidance requirement of notice to an institution's federal bank regulator is designed to provide that regulator with "early warning" and to permit that regulator to assess the effectiveness of the bank's response program.[8] Notice is required "as soon as possible" when a bank becomes aware of a data breach that involves access to or use of "sensitive customer information."[9]

Sensitive customer information is defined to include a customer's name, address, or phone number in conjunction with that customer's social security number, driver's license number, account number, credit or debit card number, or password or other similar numbers. Sensitive customer information also includes any combination of components of customer information that would permit someone to log on to or otherwise access a customer's account.[10]

---

7. 70 Fed. Reg. at 15,752.
8. *Id.* at 15,741.
9. *Id.*
10. *Id.*

D. *Customer Notice*

Much of the detail in the Interagency Guidance focuses on the customer notice, including when and to whom the notice should be given, the specific content of the notice, and the manner in which it should be delivered. In general, customer notice is mandated by the Interagency Guidance "as soon as possible" if a bank determines that "misuse of its information about a customer has occurred or is reasonably possible."[11]

The bank regulatory agencies, by this formulation, attempted to strike a balance and to provide a reasonable threshold for customer notification. Under this standard, a bank may determine that a data security breach has occurred but that such breach is unlikely to result in the misuse of its customers' sensitive information and, on that basis, decide that no notice is needed.[12] In addition, the Interagency Guidance makes clear that a bank that suffers a breach may notify only affected customers – i.e., those individuals for whom the bank determines a misuse of their information has occurred or is reasonably possible. If it is not possible to isolate some subset of bank customers as likely to be affected, a bank must notify all its customers.[13]

Customer notice must be "clear and conspicuous."[14] The Interagency Guidance sets forth certain elements required in a customer notice; among them, the notice must describe the data breach in general terms, the type of information that was subject to access, and what the bank has done to protect customer information from further unauthorized access. The notice also should include a contact phone number at the bank and counsel customer vigilance.[15] The Interagency Guidance also notes certain additional optional elements that may be included in a notice, including: a recommendation that a customer

---

11. *Id.* at 15,752.

12. The Interagency Guidance does not permit a bank to forgo customer notice to avoid embarrassment or inconvenience to the bank where it has determined that misuse of its information about a customer has occurred or is reasonably possible. Customer notice may be delayed, however, where a law enforcement agency has made written request for a delay to avoid compromising a criminal investigation.

13. 70 Fed. Reg. at 15,752.

14. *Id.* at 15,753. The Interagency Guidance notes that "clear and conspicuous" notice to customers can reduce a bank's legal risk, contribute to good customer relations, and enable customers to protect themselves against identity theft.

15. *Id.*

review account statements; a description of fraud alerts and an explanation of how a customer may place such an alert in the customer's consumer reports; and an explanation of how a customer may obtain a free credit report.[16]

E. Preemption

An important question – particularly given the many state laws that have been enacted on data breach notices – is whether the Interagency Guidance preempts state laws that also require customer notice. The federal bank regulatory agencies were asked this direct question and were urged in the rulemaking process to include an express preemption in the Interagency Guidance; however, they declined to do so.[17]

The federal regulators, instead, noted that the scope of preemption was decided by Congress and set forth in the GLB Act. That federal law preempts state law "inconsistent" with the GLB Act's privacy protections, but only to the extent of such inconsistency. The GLB Act also makes clear that state laws are not preempted to the extent that they offer greater privacy protections than the federal standards.[18] In sum, the GLB Act – and the regulatory guidance issued thereunder, including the Interagency Guidance – establishes the "floor," and states are free to adopt higher standards.

III. STATE LEGISLATIVE RESPONSES TO DATA BREACHES

As noted above, the states have been quick to respond to the data breach scandals. In fact, twenty-three states enacted new data breach notice laws in 2005.[19]

---

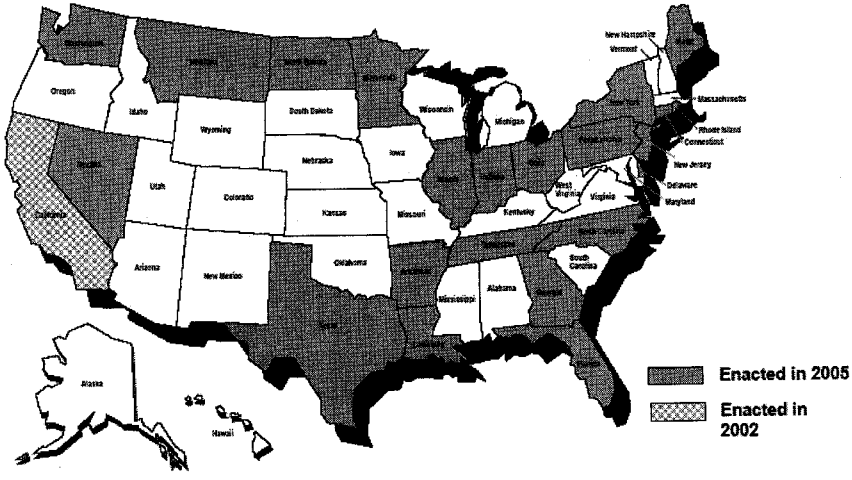
16. *See id.* The Interagency Guidance also directs banks to require their service providers, both domestic and foreign, (1) to notify the bank immediately in the event of unauthorized access to the confidential information of its customers, and (2) to take appropriate action to respond to such incidents. *See id.* at 15,752. Such service provider notice is designed to allow affected banks to implement their own response programs in the event of a data breach at a service provider.

17. *See id.* at 15,738.

18. 15 U.S.C. § 6807 (2000); *accord* 70 Fed. Reg. at 15,738 n.9.

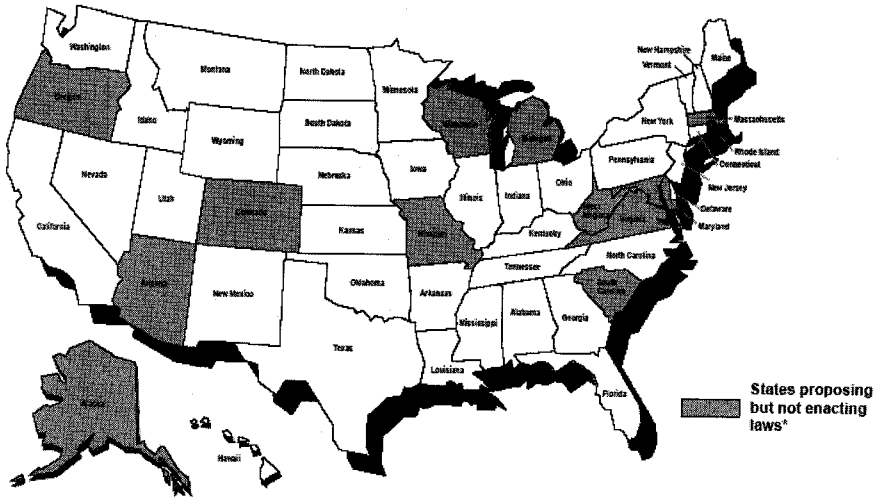
19. Of these state laws, Indiana's law applies only to state agencies and, for this reason, will not be discussed in this Article. New York City has enacted an ordinance requiring notice of security breaches be given by entities licensed by the New York City Department of Consumer Affairs. The ordinance also is outside the scope of this Article.

States With Notice Laws



Furthermore, twelve additional states have considered similar data breach legislation.

States Proposing Notice Bills, But No Law Enacted in 2005



*At the end of 2005, Massachusetts and Wisconsin bills were still active.

The various state laws generally are modeled on California's notice requirement, which was enacted prior to ChoicePoint and the recent wave of other data breaches. Most states follow the general structure of the California law and cover similar entities and data.

Yet, the state laws also differ in many respects. For example, although the state notice laws generally protect similar customer data, some state laws cast a broader net. In addition, some states have authorized private rights of action where the required notice of a security breach is not given. Most (but not all) states require a delay in customer notification if law enforcement deems the delay necessary.

These variations and differences worry banks and other institutions that need to comply with these laws. Under the current regime, a financial institution addressing a breach affecting citizens of multiple states could face differing or even conflicting requirements in

addressing the breach. We examine below the commonalities and differences in the state notice regimes.[20]

A. *Entities Covered by State Laws*

The state notice laws generally apply more broadly than the federal bank regulators' Interagency Guidance; that is, state laws cover not only banks but also other institutions and entities. Most state notice laws apply to persons or entities doing business in the state who own or license computerized data containing information on state citizens. Although three state laws do not explicitly require that the entity suffering a data breach do business in the state,[21] some presence appears to be required for the state to gain jurisdiction.

Still, there are variations in the state regimes. Georgia's law imposes requirements only on those who collect information for the purpose of disseminating that information to unaffiliated third parties – i.e., data brokers like ChoicePoint.[22] Georgia law, thus, is likely to exclude most banks and other financial institutions, as they are unlikely to collect information for dissemination to non-affiliated third parties. Even when a financial institution uses a third-party data processor, the purpose in collecting the data is likely to be for the institution's own use.

B. *Exemptions from Requirements*

All but one of the state notice laws exempt some entities from the requirement to notify consumers of a breach.[23] The precise scope of these exemptions, however, vary.

---

20. Some of the state notice laws, especially those enacted most recently, also cover other topics such as data safekeeping and consumer security freezes, which allow consumers to freeze credit reports under certain circumstances. This Article focuses only on the data breach notice requirements in state laws.

21. GA. CODE ANN. §§ 10-1-911(2), 10-1-912(a) (2005); 815 ILL. COMP. STAT. 530/5 (2005); Act effective January 1, 2006, ch. 485, 2005 Nev. Stat. § 20 (to codified at NEV. REV. STAT. Title 52, new chapter).

22. GA. CODE ANN. § 10-1-912(a) (2005).

23. New York departs from the formula followed by the other states; its notice law does not contain an exemption by which a financial institution otherwise subject to the law may avoid notice. *See* Information Security Breach and Notification Act, 2005 N.Y. Laws § 4 (to be codified at N.Y. GEN. BUS. LAW §§ 899-aa.2 and 3).

Several states have exemptions in their notice laws for financial institutions.[24] For example, eight states exempt banks (and other financial institutions) that are subject to and in compliance with either the Interagency Guidance or the sections of the GLB Act under which the Interagency Guidance was issued.

Three states exempt entities that are subject to and in compliance with federal or other state notice requirements that provide greater protection than under the states' notice law.[25] These states were among the first to adopt notice laws, and these laws likely were drafted prior to the issuance of the Interagency Guidance. Banks in compliance with the Interagency Guidance may find it difficult to claim that this federal bank regulatory guidance offers greater protection than the state laws.

Eighteen states have included in their notice laws an exception for entities maintaining their own notice procedures as part of a security policy when the timing of a notice under those procedures is consistent with the timing requirements of the state notice law.[26] California's notice law contained such an exemption, and most states subsequently adopting notice laws have stayed close to the California model in this respect.[27]

---

24. *See* 2005 Conn. Acts No. 05-148 § 3 (Reg. Sess.); LA. REV. STAT. ANN. § 51:3076 (2005); MINN. STAT. § 325E.61(4) (2005); Act effective January 1, 2006, ch. 485, 2005 Nev. Stat. § 14 (to codified at NEV. REV. STAT. Title 52, new chapter); N.C. GEN. STAT. § 75-65 (2005); N.D. CENT. CODE § 51-30-06 (2005); OHIO REV. CODE ANN. § 1349.19 (F) (2006); Breach of Personal Information Notification Act, Act No. 94, 2005 Pa. Laws §§ 2, 7; R.I. GEN. LAWS § 11-49.2-7 (2005).

25. ARK. CODE ANN. § 4-110-106(a) (2005); DEL. CODE ANN. tit. 6, § 12B-103(b) (2005); FLA. STAT. § 817.5681(9)(b) (2005).

26. ARK. CODE ANN. § 4-110-105(f) (2005); CAL. CIV. CODE §§ 1798.29(h), 1798.82(h) (2005); DEL. CODE ANN. tit. 6, § 12B-103(a) (2005); FLA. STAT. § 817.5681(9)(a) (2005); GA. CODE ANN. § 10-1-911(3) (2006); 815 ILL. COMP. STAT. 530/10 (2005); LA. REV. STAT. ANN. § 51:3074.F (2005); ME. REV. STAT. ANN. tit. 10, §1348.6 (2005) (Maine does not require the timing of notice be similar to under its notice law); MINN. STAT. § 325E.61(1)(h) (2005); MONT. CODE ANN. § 30-14-1704(6) (2005); Act effective January 1, 2006, ch. 485, 2005 Nev. Stat. § 24 (to codified at NEV. REV. STAT. Title 52, new chapter); N.J. STAT. ANN. § 56:8-163.12.b (2005); N.D. CENT. CODE § 51-30-06 (2005); Breach of Personal Information Notification Act, Act No. 94, 2005 Pa. Laws § 7; R.I. GEN. LAWS § 11-49.2-7 (2005); TENN. CODE ANN. § 47-18-2107(f) (2005); TEX. BUS. & COM. CODE ANN. § 48.103(g) (2005); WASH. REV. CODE § 19.255.010(8) (2005).

27. CAL. CIV. CODE § 1798.82(h) (2005).

C. *Types of Data Protected*

The various state notice laws generally take a similar approach with respect to the data that is protected – that is, the types of data the improper access to which would trigger a customer notice. Most states, following California's lead, require a breach notice if unencrypted or unredacted computerized data containing a person's first name or first initial and last name is disclosed in conjunction with any of the following pieces of information about that same person:

- Social security number
- Driver's license or other state identification number
- Account number, credit card or debit card number along with a personal identification number or password that permits access to the person's account.[28]

Some states, however, go further and include more information under the definition of protected data. For example, Arkansas includes medical information in this list.[29] In Georgia and New Jersey, even where the three categories of information above are not associated with the consumer's name, the information will be treated as personal information in certain circumstances.[30] North Dakota adds to the list the person's date of birth, mother's maiden name, employee ID number and digitized or electronic signature.[31]

North Carolina law varies from the formula described above in several respects. North Carolina includes within the protected data a catch-all category of any information that would allow someone to log

28. *See, e.g.*, CAL. CIV. CODE § 1798.80(e) (2005); Personal Information Protection Act, Pub. Act No. 094-0036, 815 ILL. COMP. STAT. ANN. 530/5 (2005); LA. REV. STAT. ANN. § 51:3073(4)(a) (2005); MINN. STAT. § 325E.61(1)(e) (2005); Act effective January 1, 2006, ch. 485, 2005 Nev. Stat. § 21 (to codified at NEV. REV. STAT. Title 52, new chapter); TEX. BUS. & COM. CODE ANN. § 48.002(1) (2006); WASH. REV. CODE § 19.255.010(5) (2005).

29. *See* ARK. CODE ANN. § 4-110-103 (2005).

30. GA. CODE ANN. § 10-1-911(5) (2005) (where compromise of the above listed items would permit identity theft even without association with the person's name, the data in these three categories is treated as personal information); N.J. STAT. ANN. § 56:8-161.10 (2005) (if disassociated data is improperly accessed and if the means to link the disassociated data also was accessed, the disassociated data will be treated as personal information).

31. *See* N.D. CENT. CODE § 51-30-01.2.a (2005).

onto or access the customer's account.[32] North Carolina also adds to the list a person's electronic identification numbers, e-mail names or addresses, Internet account numbers or Internet identification names, digital signatures, biometric data, fingerprints, and mother's maiden name.[33] In addition, North Carolina law covers paper records as well as digital records.[34]

D. How Breach is Defined

Most state notice laws define a data security breach – the event that triggers a customer notice – as an "unauthorized acquisition of computerized data" that compromises "the security, confidentiality, or integrity of personal information maintained by the person or business," or use language that is substantively similar.[35] This is the approach taken in California's notice law.[36]

This approach differs from the Interagency Guidance, which requires that the unauthorized access create harm or possible harm for consumers. Several states follow the approach taken by the federal bank regulators and require notice only in situations of actual, likely or possible harm to consumers. Florida, Montana, Nevada and Pennsylvania require that the unauthorized access "materially affect" the security of personal data in order to constitute a security breach.[37] The definition of breach in North Carolina requires that "the illegal use of personal information has occurred or is reasonably likely to occur or that creates a material risk of harm to a consumer."[38] In Ohio, a notice

---

32. *See* N.C. GEN. STAT. §§ 75-61, 14-113.20(b) (2005).

33. *See* N.C. GEN. STAT. §§ 75-61, 14-113.20(b) (2005).

34. *See* Identity Theft Protection Act, 2005 N.C. Sess. Laws § 1 (to be codified at N.C. GEN. STAT. § 75-65).

35. ARK. CODE ANN. § 4-110-103(1)(A) (2005); CAL. CIV. CODE § 1798.82(d) (2005); GA. CODE ANN. § 10-1-911(1) (2005); 815 ILL. COMP. STAT. 530/5 (2005); LA. REV. STAT. ANN. § 51:3073(2) (2005); MINN. STAT. § 325E.61(1)(d) (2005); N.J. STAT. ANN. § 56:8-161.10 (2005); Information Security Breach and Notification Act, 2005 N.Y. Laws § 4 (to be codified at N.Y. GEN. BUS. LAW § 899-aa.1(c)); N.D. CENT. CODE § 51-30-01.1 (2005); R.I. GEN. LAWS § 11-49.2-5(b) (2005); TENN. CODE ANN. § 47-18-2107(a)(1) (2005); TEX. BUS. & COM. CODE ANN. § 48.103(a) (2005); WASH. REV. CODE § 19.255.010(4) (2005).

36. CAL. CIV. CODE § 1798.82(d) (2005).

37. FLA. STAT. § 817.5681(4) (2005); MONT. CODE ANN. § 30-14-1704(4)(a) (2005); Act effective January 1, 2006, ch. 485, 2005 Nev. Stat. § 19 (to be codified at NEV. REV. STAT. Title 52, new chapter); Breach of Personal Information Notification Act, Act No. 94, 2005 Pa. Laws § 2.

38. Identity Theft Protection Act, 2005 N.C. Sess. Laws § 1 (to be codified at N.C.

is required if the breach caused or is reasonably believed to have caused or is likely to cause in the future a material risk of identity theft or other fraud to the affected person.[39]

E. *Who Must be Notified*

In the event of a security breach (meeting the requirements of the triggering definitions described above), all of the state notice laws require notice to affected citizens. New Jersey and New York also require that certain state agencies be informed of any security breach requiring notice to consumers.[40] Most states notice laws, including California's law, do not expressly require that law enforcement be notified of a security breach.[41] That said, nearly all state notice laws have a provision requiring notice to consumers be delayed if required by law enforcement; accordingly, a requirement to notify law enforcement may be inferred in such notice laws.[42]

In addition to notifying affected persons, some states require notice be provided to the national consumer reporting agencies if a threshold number of persons are affected by the breach.[43]

F. *Means of Notice*

California and most other states permit three types of notice for security breaches: (1) written notice, (2) electronic notice consistent with federal electronic records and signatures requirements, and (3) "substitute notice" if the cost of providing notice to affected persons

---

GEN. STAT. § 75-61).

39. OHIO REV. CODE ANN. § 1349.19(A)(1)(a) (2005).

40. N.J. STAT. ANN. § 56:8-163.12.c(1) (2005) (requiring notice be given to the state police); Information Security Breach and Notification Act, 2005 N.Y. Laws § 4 (to be codified at N.Y. GEN. BUS. LAW § 899-aa.8(a)).

41. *See, e.g.*, CAL. CIV. CODE § 1798.82 (2005).

42. *Id.* A breach may trigger notice to law enforcement under other laws. For example, a breach at a bank or broker-dealer likely would trigger a Suspicious Activity Report filing under the Bank Secrecy Act.

43. *See, e.g.*, MINN. STAT. § 325E.61(2) (2005); Act effective January 1, 2006, ch. 485, 2005 Nev. Stat. § 24 (to be codified at NEV. REV. STAT. Title 52, new chapter); N.J. STAT. ANN. § 56:8-163.12.f (2005); Information Security Breach and Notification Act, 2005 N.Y. Laws § 4 (to be codified at N.Y. GEN. BUS. LAW § 899-aa.8(b)); N.C. GEN. STAT. § 75-65 (2005); OHIO REV. CODE ANN. § 1349.19(G) (2005); TEX. BUS. & COM. CODE ANN. § 48.103(h) (2005).

would exceed $250,000, the number of persons to be notified exceeds 500,000 or the notifying entity does not have sufficient contact information on the person to be notified.[44] Substitute notice typically consists of an e-mail to persons for whom the notifying entity has an e-mail address, conspicuous posting on a website if the notifying entity maintains one, and notification to major statewide media. Connecticut, Delaware, Montana, New York, Ohio and Pennsylvania also permit notification by telephone.[45]

Four states have somewhat lower thresholds for permitting substitute notice. Delaware's law permits substitute notice when the costs of normal notice would exceed $75,000 or the Delaware residents to be given notice exceed 100,000.[46] Ohio allows businesses with fewer than ten employees to give substitute notice in a prescribed method where notification costs would exceed $10,000.[47] Under Pennsylvania's notice law, substitute notice is permitted where the cost of notice exceeds $100,000 or the affected subject class or persons to be notified exceeds 175,000.[48] Rhode Island permits substitute notice where the cost of providing notice would exceed $25,000 or the persons to be notified exceed 50,000.[49]

New York has a somewhat more stringent notice requirement. The New York notice law requires that for a person to be given notice by electronic means, that person must have consented to such notice. In addition, a log of all persons notified electronically must be kept.[50]

---

44. *See* ARK. CODE ANN. § 4-110-105(e) (2005); FLA. STAT. § 817.5681(6) (2005); GA. CODE ANN. § 10-1-911(3) (2005); 815 ILL. COMP. STAT. 530/10 (2005); LA. REV. STAT. § 51:3074(E) (2005); MINN. STAT. § 325E.61(1)(g) (2005); Act effective January 1, 2006, ch. 485, 2005 Nev. Stat. § 24 (to codified at NEV. REV. STAT. Title 52, new chapter); N.J. STAT. ANN. § 56:8-163.12.d(3) (2005); N.D. CENT. CODE § 51-30-05 (2005); TENN. CODE ANN. § 47-18-2107(e) (2005); TEX. BUS. & COM. CODE ANN. § 48.103(e), (f) (2006); WASH. REV. CODE § 19.255.010(7) (2005).

45. *See* 2005 Conn. Acts No. 05-148 § 3 (Reg. Sess.); DEL. CODE ANN. tit. 6 § 12B-101(3) (2005); MONT. CODE ANN. § 30-14-1704(5)(a)(iii) (2005); Information Security Breach and Notification Act, 2005 N.Y. Laws § 4 (to be codified at N.Y. GEN. BUS. LAW § 899-aa.5(c)); OHIO REV. CODE ANN. § 1349.19(E)(3) (2005); Breach of Personal Information Notification Act, Act No. 94, 2005 Pa. Laws § 2.

46. *See* DEL. CODE ANN. tit. 6, § 12B-101(3)(d) (2005).

47. *See* OHIO REV. CODE ANN. § 1349.19(E)(5) (2005).

48. *See* Breach of Personal Information Notification Act, Act No. 94, 2005 Pa. Laws § 2.

49. *See* R.I. GEN. LAWS § 11-49.2-5(c)(3) (2005).

50. *See* Information Security Breach and Notification Act, 2005 N.Y. Laws § 4 (to be codified at N.Y. GEN. BUS. LAW § 899-aa.5(b)).

G. *Timing of Notice*

The requirements for when notice must be given vary. California law provides that "disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system."[51] Most other states also follow this model.[52] Florida and Ohio also follow this general formula but specify that notice must occur within forty-five days.[53] Illinois does not permit a delay in notification for law enforcement purposes.[54]

As a practical matter, because law enforcement may require that notice to consumers be delayed, notice to law enforcement will generally need to precede notice to consumers. Those states with an express requirement to notify state agencies or law enforcement do not set a time frame for doing so.[55]

H. *Data Not Owned or Licensed*

All of the state notice laws contain provisions governing situations in which a breach exposing personal information occurs and the breached entity does not own or license the data but, instead, holds such data for another person or entity.[56] These provisions in the state notice laws generally mirror the one originally enacted by California,

---

51. CAL. CIV. CODE § 1798.82(a) (2005).

52. *See, e.g.*, ARK. CODE ANN. § 4-110-105(a)(2) (2005); DEL. CODE ANN. tit. 6, § 12B-102(a) (2005); LA. REV. STAT. ANN. § 51:3074(C) (2005); MINN. STAT. § 325E.61(1)(a) (2005); Information Security Breach and Notification Act, 2005 N.Y. Laws § 4 (to be codified at N.Y. GEN. BUS. LAW § 899-aa.2); TENN. CODE ANN. § 47-18-2107(b) (2005); TEX. BUS. & COM. CODE ANN. § 48.103(b) (2005); WASH. REV. CODE § 19.255.010(1) (2005).

53. FLA. STAT. § 817.5681(1)(a) (2005); OHIO REV. CODE ANN. § 1349.19(B)(2) (2005).

54. 815 ILL. COMP. STAT. 530/10 (2005).

55. N.J. STAT. ANN. § 56:8-163.12.c(1) (2005); Information Security Breach and Notification Act, 2005 N.Y. Laws § 4 (to be codified at N.Y. GEN. BUS. LAW § 899-aa.8(a)).

56. *See, e.g.* ARK. CODE ANN. § 4-110-105(b) (2005); DEL. CODE ANN. tit. 6, § 12B-102(b) (2005); FLA. STAT. § 817.5681(2)(a) (2005); 815 ILL. COMP. STAT. 530/10 (2005); LA. REV. STAT. § 51:3074(C) (2005); Information Security Breach and Notification Act, 2005 N.Y. Laws § 4 (to be codified at N.Y. GEN. BUS. LAW § 899-aa.3); N.C. GEN. STAT. § 75-65 (2005) (permits delay of this notice consistent with the legitimate needs of law enforcement); TEX. BUS. & COM. CODE ANN. § 48.103(c) (2005); WASH. REV. CODE § 19.255.010(2) (2005).

which requires that the breached entity notify the owner or licensee for whom the data is held immediately following discovery of the breach.[57] Using a similar construction, Louisiana requires that such notice be "made in the most expedient time possible," and Ohio requires the notice to be "in an expeditious manner."[58] Florida requires that such notice be given as soon as practicable, but within ten days of determination of the breach.[59]

I. Enforcement/Private Rights of Action

The state notice laws differ considerably on their means of enforcement. Five of the states expressly create a private right of action for persons harmed by an entity failing to give proper notice of a security breach.[60] In eight states only the attorney general may commence an action for failure to provide notice.[61] Two additional states allow actions by specified state agencies.[62] In the remaining states, the notice laws are silent on who may enforce the notice provisions.[63]

J. Conclusion

The variations, large and small, in the state regimes raise obvious compliance difficulties and issues for banks and other financial

57. CAL. CIV. CODE § 1798.82(b) (2005).

58. LA. REV. STAT. ANN. § 51:3074(C) (2005); OHIO REV. CODE ANN. § 1349.19(C) (2005).

59. FLA. STAT. § 817.5681(2) (2005).

60. CAL. CIV. CODE § 1798.84(b) (2005); LA. REV. STAT. ANN. § 51:3075 (2005); Identity Theft Protection Act, 2005 N.C. Sess. Laws § 1 (to be codified at N.C. GEN. STAT. § 75-65(i)); TENN. CODE ANN. § 47-18-2107(g) (2005); WASH. REV. CODE § 19.255.010(10)(a) (2005).

61. ARK. CODE ANN. § 4-110-108 (2005); 2005 Conn. Acts No. 05-148 § 3 (Reg. Sess.); Act effective January 1, 2006, ch. 485, 2005 Nev. Stat. § 28 (to codified at NEV. REV. STAT. Title 52, new chapter); Information Security Breach and Notification Act, 2005 N.Y. Laws § 4 (to be codified at N.Y. GEN. BUS. LAW § 899-aa.6(a)); N.D. CENT. CODE § 51-30-07 (2005); OHIO REV. CODE ANN. § 1349.19(I) (2005); Breach of Personal Information Notification Act, Act No. 94, 2005 Pa. Laws §8; TEX. BUS. & COM. CODE ANN. § 48.201(b)(2005).

62. ME. REV. STAT. ANN. tit. 10, § 1349 (2005) (actions are permitted by the Department of Professional and Financial Regulation) and MONT. CODE ANN. § 30-14-1705 (2005) (actions are permitted by the Department of Administration).

63. FLA. STAT. § 817.5681 (2005); GA. CODE ANN. § 10-1-910-912 (2005); 815 ILL. COMP. STAT. 530/10 (2005); R.I. GEN. LAWS § 11-49.2 (2005)

institutions that operate in more than one jurisdiction. To avoid the difficulties of complying with the patchwork of state laws, many financial institutions have sought a single, unified federal standard on data breach notifications. We discuss the federal approaches next.

IV. FEDERAL LEGISLATION ON DATA BREACHES AND NOTICES

As many states began enacting laws requiring notice of security breaches, Congress also began to examine the issue. As of the end of 2005, approximately twenty bills requiring consumers be given notice of security breaches had been introduced in Congress, though – as of this writing[64] – none had come to a floor vote. The congressional bills, most of which had been introduced after passage of some of the state notice laws, generally are more comprehensive (covering issues beyond notice requirements – such as broader topics of data security or consumer security freezes) than many of the state laws.

At the end of 2005, four bills had emerged as front runners most likely to be enacted or, at a minimum, to influence any eventually enacted federal law on the topic. They are as follows:

- H.R. 3997. This bill from Rep. Steven LaTourette (R-OH) is called the Financial Data Protection Act of 2005.[65] The LaTourette bill has bi-partisan sponsorship and generally is regarded as industry friendly. The House Financial Services Committee held a hearing on this bill on November 9, 2005, but has not yet voted on the bill.
- H.R. 4127. Rep. Cliff Stearns' (R-FL) bill, titled the Data Accountability and Trust Act, is generally considered the most industry friendly of the four leading contenders and has only Republican co-sponsors.[66] The Stearns bill was forwarded by a subcommittee on a 13 to 8 vote to the House Energy and Commerce Committee on November 3, 2005.
- S. 1408. Sen. Gordon Smith (R-OR) introduced a bill entitled the Identity Theft Protection Act in the Senate.[67]

64. January 6, 2006.
65. H.R. 3997, 109th Cong. (2005).
66. H.R. 4127, 109th Cong. § 3 (2005).
67. S. 1408, 109th Cong. (2005).

The bill has bi-partisan support, and the Senate Commerce Committee reported the bill and placed it on the legislative calendar on December 8, 2005.

- S. 1789. Sen. Arlen Specter's (R-PA) bill entitled the Personal Data Privacy and Security Act of 2005 is considered by many the most likely to be enacted and has three Democratic co-sponsors.[68] The Senate Judiciary Committee approved S. 1789 by unanimous consent on November 17, 2005.

All four federal notice bills would pre-empt state notice laws.[69]

A. Covered Institutions and Data

The four key federal bills vary in terms of which institutions and what type of data are covered. The bill by Rep. LaTourette only covers those entities that qualify as "consumer reporters" under the federal Fair Credit Reporting Act.[70] The other bills take a broader approach. Rep. Stearns' bill, for instance, covers anyone engaging in interstate commerce who owns or possesses electronic data.[71] The breach notice provisions of the bill from Sen. Specter addresses entities engaged in interstate commerce that use, access, transmit, store, dispose of, or collect sensitive personally identifiable information.[72]

The four key federal bills cover similar information to the state breach notice laws. For example, Sen. Smith's bill protects sensitive personal information, a term defined to include an individual's name, address or telephone number, combined with either (1) the individual's Social Security number, taxpayer identification number, or employer identification number (if derived from the Social Security number), (2) the individual's financial account number or credit card or debit card number, combined with any required security code, access code, or password permitting account access, or (3) the individual's state

68. S. 1789, 109th Cong. (2005) (co-sponsors of the bill are Russell Feingold (WI), Dianne Feinstein (CA) and Patrick Leahy (VT)).

69. H.R. 3997, § 2; H.R. 4127, § 6; S. 1408, § 7; S. 1789, § 329.

70. H.R. 3997, § 2.

71. H.R. 4127, § 3(a).

72. S. 1789, § 321(a).

driver's license number or state resident identification number.[73] The bill from Sen. Specter additionally includes certain biometric, password, and other information used to access an account when the information is accompanied by the individual's name.[74]

B. Exemptions

Importantly, Rep. LaTourette's bill exempts from notification requirements those entities subject to and in compliance with regulations issued under section 501 of the GLB Act.[75] Sen. Smith's bill similarly exempts those entities subject to section 501 of the GLB Act and the Interagency Guidelines.[76] Therefore, banks and other financial institutions subject to the Interagency Guidelines would be exempt from the requirements of the Smith and LaTourette bills. The Stearns and Specter bills do not contain such an exemption.

C. How Is Breach Defined

Each of the key federal notice bills contains a different definition of "security breach." Rep. LaTourette's bill defines data breach to include data revealed through an unauthorized acquisition that could be used to commit financial fraud and also defines security breach to include "an unusual pattern or use of such information indicative of financial fraud."[77] Rep. Stearns' bill defines security breach as an unauthorized acquisition of data that provides a "reasonable basis to conclude that there is a significant risk of identity theft to the individual to whom the personal information relates."[78] The bill from Sen. Smith defines a breach as "unauthorized access to and acquisition of data" containing sensitive personal information that "compromises the security or confidentiality of such information and creates a reasonable risk of identity theft."[79] In Sen. Specter's bill, security breach is more broadly defined as "compromise of the security, confidentiality, or

73. S. 1408, § 10(a)(A).
74. S. 1789, § 3(11)(A).
75. H.R. 3997, § 2.
76. S. 1408, § 5(g).
77. H.R. 3997, § 2.
78. H.R. 4127, § 5(1).
79. S. 1408, § 10(1).

integrity of computerized data through misrepresentation or actions that result in, or there is a reasonable basis to conclude has resulted in, acquisition of or access to sensitive personally identifiable information that is unauthorized or in excess of authorization."[80]

D. Who Must be Notified

The four federal bills take different approaches on who, in addition to customers, must be notified in the event of a data breach. Rep. LaTourette's bill would require notice to the Secret Service and the breached entity's functional regulator where a breach may result in substantial harm or inconvenience to a consumer.[81] The major consumer reporting agencies also would need to be notified if the breach would affect more than 1,000 consumers.

Rep. Stearns' bill requires notice (1) to affected individuals, (2) to the Federal Trade Commission ("FTC"), (3) on the breached entity's website (if applicable), and (4) when the breached entity is a merchant and the breach involves financial account information, to the financial institution that issued the account.[82]

Sen. Smith's bill requires notice to customers and the FTC.[83] If the breach involves more than 1,000 persons, the major consumer reporting agencies also must be notified.[84]

Sen. Specter's bill requires notice to be given to affected U.S. residents whose sensitive personally identifiable information has been or is reasonably believed to have been improperly accessed or acquired.[85] Otherwise required notice may be avoided if (1) a risk assessment determines the breach created no significant risk of harm to the persons involved, (2) the breached entity notifies the Secret Service within forty-five days of discovery of the breach, and (3) the Secret Service does not respond within ten days that notice should be given.[86] The bill also contains an exemption from notice requirements for

80. S. 1789, § 3(10)(A).
81. H.R. 3997, § 2.
82. H.R. 4127, § 3(a)(1)-(4).
83. S. 1408, § 3(b)(1).
84. *Id.* § 3(a)(1).
85. S. 1789, § 321(a).
86. *Id.* § 322(b).

entities utilizing a security program meeting certain requirements and providing notice to persons affected by fraud resulting from a security breach.[87]

E. *Means and Timing of Notice*

For the LaTourette and Stearns bills, notice to the consumer may be given by mail or, if consent has been given by the consumer, by e-mail.[88] Like most state notice laws, the Smith bill permits three types of notice for security breaches: (1) written notice, (2) electronic notice consistent with federal electronic records and signatures requirements, and (3) substitute notice if the cost of providing notice to affected persons would exceed $250,000, the number of persons to be notified exceeds 500,000, or the notifying entity does not have sufficient contact information on the person to be notified.[89] In addition to mail and e-mail notice, S. 1789 also permits notice by telephone in all cases and through major media outlets if more than 5,000 residents of a state or jurisdiction are impacted.[90] All of the federal notice bills require that required notices be given promptly, but only Sen. Specter's bill requires that some notices occur within thirty days.[91]

F. *Enforcement/Private Right of Action*

The four key federal notice bills each establish different regimes for their enforcement. The LaTourette bill provides that the requirements of the bill are to be enforced by a covered entity's federal functional regulator.[92] Rep. Stearns' bill is enforced by the FTC.[93] For financial institutions under Sen. Smith's bill, a covered entity's primary federal regulator enforces the law. However, the bill also permits actions to be brought by state attorneys general.[94] Sen. Specter's bill grants enforcement authority to the U.S. Attorney General but still

87. *Id.* § 322(c)
88. H.R. 3997, § 2; H.R. 4127, § 3(c)(1)(A).
89. S. 1408, § 3(d)(1).
90. S. 1789, § 323.
91. *Id.* § 321(d)(2).
92. H.R. 3997, § 2.
93. H.R. 4127, § 4.
94. S. 1408, § 5(f)(2).

permits state attorneys general to pursue non-preempted state law violations.[95]

Three of the federal notice bills expressly prohibit a private right of action.[96] The LaTourette bill also does not appear to allow a private suit against entities failing to provide proper notice of a security breach.

G. *Non-owned or Licensed Data*

The LaTourette and Specter bills contain requirements for those possessing non-owned or licensed data similar to those under the California law and that of most states.[97] The other federal notice bills do not address this issue.

V. CONCLUSION

The wave of publicity surrounding data security breaches has resulted in a myriad of federal and state regulatory and legislative responses. Banks and other financial institutions will need to be watchful for additional laws governing data security issues generally – and breach notices specifically – in the coming year.

95. S. 1789, §§ 326, 327.
96. H.R. 4127, § 6(b)(1); S. 1408, § 5(f)(1); S. 1789, § 328(f).
97. H.R. 3997, § 2; S. 1789, § 321(a).