

DATA BREACH NOTIFICATION ANOTHER “HAPHAZARD PATCHWORK” OF STATE-BY-STATE REQUIREMENTS

Frances R. Roggenbaum, Esq.
717.975.8806

While Federal Congress has focused on legislation that would bring relief to multi-state insurers, producers, and the surplus lines industry from the “haphazard patchwork” of state-by-state insurance regulation,¹ its failure to date to pass comprehensive legislation that would set a uniform national data breach notification standard has resulted in another “haphazard patchwork” of state-by-state requirements for all types of businesses that operate on a multi-state basis.

This article will briefly examine the history and purpose of data breach notification laws and discuss several of the types of differences in the current state laws that make multi-state compliance a complex task.

History and Purpose

In February 2005 ChoicePoint disclosed that it had inadvertently sold personal information on nearly 145,000 individuals to identity thieves in California. Shortly thereafter, Bank of America and CitiFinancial revealed the loss of backup tapes that held nearly one million and one million customer records, respectively. Since ChoicePoint’s disclosure, hardly a week goes by without one or more data breach disclosures where personally identifiable information, such as social security, financial account and driver’s license numbers, has been compromised.

But data breach disclosures have not been limited to data brokers and financial institutions. The insurance industry has had its share, including Aetna’s announcement in April 2006 of the theft of a laptop computer that held personal information on approximately 38,000 insureds, AIG’s disclosure in June 2006 that computer equipment holding personal information on more than 900,000 applicants had been stolen, and Marsh’s announcement in July 2006 that a computer holding the names, addresses, telephone and social security numbers of more than 540,000 workers’ compensation claimants had been lost. And, governmental entities have not been immune to data breaches, including the May 2006 theft of a laptop that held personal records on nearly 27 million veterans and the more recent August 2006 disclosure by the Virginia Bureau of Insurance that social security numbers of an unknown number of agents licensed in the state were inadvertently disclosed on its website.

The Privacy Rights Clearinghouse, a non-profit group that maintains a chronology of data breaches that have been publicly disclosed since the ChoicePoint data breach, as well as a running total of individual records that have been compromised, indicates that nearly 100 million records have been subject to possible unauthorized access since February 2005.²

While data breaches certainly occurred prior to February 2005, the high-profile ChoicePoint disclosure drew national attention and served as a catalyst for the introduction of data breach notification legislation in almost every state in the country³ and in Federal Congress⁴ as well as the issuance of standards and recommendations by and/or for Federal agencies.⁵ However, states have been at the forefront in demonstrating a capacity for prompt action, with more than 30 states having enacted data breach notification laws since March 2005.

The post-ChoicePoint state laws are all modeled generally on the nation’s first data breach notification law, California’s Notice of Security Breach Act (the “California Notice Law”), enacted by the California legislature in September 2002.⁶ As with more recent state laws, the catalyst for passage of the California Notice Law was a high-profile security breach in April 2002 where hackers broke into the payroll database for the state of California and accessed the social security numbers, bank account information and home addresses of more than 260,000 state employees, including then-Governor Gray Davis.⁷ The delay in notifying employees of the data breach (the break-in was not discovered until early May 2002 and another two weeks passed before employees were notified) prompted the California legislature to act swiftly to enact notification requirements intended to give consumers a warning that their personal information had been compromised and the opportunity to take steps to protect themselves against possible identity theft.⁸

Shortly after enactment, the California Notice Law was touted as likely to “create a de facto national disclosure policy” because of California’s “size and prominent role in the high-tech industry.”⁹ And, indeed, ChoicePoint’s compliance with the notification requirements of the California Notice Law for California residents, and its voluntary provision of notice to all potentially affected consumers in other states, led to national media coverage of its 2005 data security breach and a public outcry for similar legislation in other states.¹⁰

Since the California Notice Law has served as the prototype for other states’ data breach notification laws, following is a brief summary of its requirements as they apply to persons or business entities:¹¹

- (1) Triggering Event For Disclosure: Any person or business entity that conducts business in California and that owns or licenses unencrypted computerized data that includes “personal information” (hereinafter, the “Data Holder”) is required to disclose “any breach of the security of the system following discovery or notification of the breach in the security of the data.”¹²
- (2) Who Must Be Notified: All California residents whose “personal information was, or is reasonably believed to have been, acquired by an unauthorized person”.¹³
- (3) Timing For Notification: Notification must be made “in the most expedient time possible and without unreasonable delay,” but delay is permitted until the Data Holder takes measures necessary to determine the scope of the data breach. In addition, delay is permitted if a law enforcement agency determines that notification will impede a criminal investigation, but notice must then be given after the law enforcement agency determines that such action will not compromise the investigation.¹⁴
- (4) Form & Types of “Personal Information” Covered: The only form of information protected by the notification requirement is information maintained in unencrypted computerized format. The only types of information protected are the following, but only if not otherwise publicly and legally available from Federal, state or local government records:

An individual’s first name or initial and last name in combination with one or more of the following data elements:

- social security number.
 - Driver’s license number or California Identification Card number.
 - Account, credit or debit card number in combination with any security or access code or password that would permit access to an individual’s financial account.¹⁵
- (5) Permitted Forms of Notice/Substitute Notice Triggers & Options: Written or electronic notice in accordance with provisions of the Federal Electronic Signatures in Global and National Commerce Act (“E-Sign Act”)¹⁶ is required in all circumstances, except that “substitute notice” is permitted if the Data Holder is able to demonstrate that:
 - The cost of providing the required written or electronic notice would exceed \$250,000;
 - The number of persons that must be notified exceeds 500,000; or
 - The Data Holder does not have sufficient contact information on all affected persons to provide written or electronic notice.

When substitute notice is permitted, it must include all of the following:

- E-mail notice when the Data Holder has an e-mail address for an affected person;
 - Conspicuous posting on the website of the Data Holder if one exists; and
 - Notice to major statewide media.¹⁷
- (6) Required Content of Notice: None specified.

- (7) Notice Exceptions: A Data Holder that maintains its own notification procedures as part of an information security policy is deemed to be in compliance with the Law’s notification requirements as long as notice is actually given under such a policy and timing of the notice is consistent with the Law’s requirements. No other exemptions or exceptions apply.¹⁸
- (8) Penalties/Remedies For Failure To Comply:
- A customer of the Data Holder (i.e. an individual “who provides personal information to a business for the purpose of purchasing or leasing a product or obtaining a service from the business”) is permitted to institute a civil action to recover damages.
 - The Data Holder may be enjoined.¹⁹

State-By-State Differences That Complicate Multi-State Compliance

While all states’ data breach notification laws are similar with respect to a requirement that a business that possesses sensitive personal information about individuals must disclose the unauthorized access to such information to all individuals potentially affected, sufficient differences exist in each of the eight categories set forth above to make compliance on a multi-state basis extremely complex. Following is a brief discussion of just several of the types of differences and examples from several states to demonstrate the differences.

- (1) Triggering Event for Notification: While some states follow the notification trigger of the California Notice Law, i.e. any unauthorized access to unencrypted computerized data that compromises the security, confidentiality or integrity of an individual’s covered personal information, most states give the Data Holder discretion to determine whether notice must be given. For example, Louisiana provides that notice is not required “if after a reasonable investigation the person or business determines that there is no reasonable likelihood of harm to customers;”²⁰ and Ohio limits a breach subject to the notice requirements to one that has caused, or is reasonably believed will cause, “a material risk of identity theft or other fraud.”²¹
- (2) Who Must Be Notified: All states require notice to any resident of the state whose personal information was subject to unauthorized access. Some states also require that notice be given to others, but the trigger for additional notice typically is the involvement of more than a specified number of state residents and frequently differs on a state-by-state basis. For example, Florida requires notice to all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis but only if more than 1,000 Florida residents are affected by the data breach.²² Minnesota requires notice to consumer reporting agencies if more than 500 Minnesota residents are affected,²³ and New York requires notice to consumer reporting agencies when more than 5,000 New York residents are affected, but also requires notice to the New York Attorney General, Consumer Protection Board, and State Office of Cyber Security and Critical Infrastructure regardless of numbers of persons affected.²⁴
- (3) Form & Types of Personal Information Covered: While most states define “personal information” to include the same form and types of information set forth in the California Notice Law, in some states the form and types of covered personal information differ. With respect to form, a few states cover not only data in computerized format, but also certain personal information in paper or other format. For example, Delaware includes all individually identifiable information regarding medical history, medical treatment or diagnosis in either electronic or physical form,²⁵ and North Carolina covers personal information in any form “whether computerized, paper, or otherwise.”²⁶ Moreover, some states protect additional types of personal information not protected by the California Notice Act, e.g. North Carolina includes such things as digital signatures, biometric data, fingerprints, and parent’s legal surname prior to marriage,²⁷ and North Dakota includes date of birth, mother’s maiden name, and identification number assigned by an employer.²⁸
- (4) Penalties/Remedies for Failure to Comply: In a departure from the California Notice Law, most states provide exclusive enforcement authority to a state’s attorney general or similar state official. However, a few states follow the California approach in providing a private right of action that allows persons who have been injured by a Data Holder’s failure to comply with the data breach notification requirements to sue for damages. For example, Louisiana permits a private right of action to recover actual damages

resulting from failure to disclose a data breach in a timely manner,²⁹ and Delaware permits not only a private right of action for recovery of damages, but also provides for a violating Data Holder to pay treble damages and attorney fees.³⁰

In addition to data breach notification requirements, a number of states have adopted related requirements as part of a broader legislative effort to address the security of personal information through such things as credit report freezes, limitations on the collection and use of social security numbers, requirements for data destruction, and the criminalization of identity theft – none of which are uniform and all of which add to the “haphazard patchwork” of state-by-state requirements.

Conclusion

Unless and until Federal Congress enacts a national uniform standard for data breach notification that preempts state law, insurers, producers and all other businesses that operate on a multi-state basis face the complicated task of complying with a “haphazard patchwork” of state-by-state notification laws that follow a similar pattern, but include some significantly differing requirements. While it is possible to apply only those minimum requirements necessary to comply in each affected state, few businesses want to risk a public relations disaster from treating similarly affected individuals differently based solely on state of residence. The more practical approach, and one that appears to have been used by most businesses that suffer a data security breach that affects individuals in multiple states, is to voluntarily combine and apply the most stringent standards of all involved states (not only for notification, but also for such things as credit report freezes) to affected individuals in all states – even in states that have not yet enacted data breach notification or related requirements.³¹ Perhaps, then, what California started, and other states have added to, is indeed a de facto national disclosure policy that in practical effect requires multi-state businesses to monitor, combine and apply the most rigorous standards set forth in this “haphazard patchwork” of state-by-state laws.

Endnotes

¹ See, National Insurance Act legislation (S 2509 and HR 6225) and the Nonadmitted and Reinsurance Reform Act (HR 5637).

² See, “A Chronology of Data Breaches” at www.privacyrights.org/ar/ChronDataBreaches.htm.

³ The National Conference of State Legislatures maintains a list of all state data breach notification legislation proposed and adopted since 2002. The list is available at www.ncsl.org/programs/lis/cip/priv/breach.htm.

⁴ A number of bills that include data breach notification requirements have been introduced by Congress, including but not limited to, the Financial Data Protection Act (HR 3997); the Data Accountability and Trust Act (HR 4127); the Identity Theft Protection Act (S 1408); the Personal Data Privacy and Security Act (S 1789); the Data Security Act (S 3568); and the Notification of Risk to Personal Data Act (S 751).

⁵ See, e.g., INTERAGENCY GUIDANCE ON RESPONSE PROGRAMS FOR UNAUTHORIZED ACCESS TO CUSTOMER INFORMATION AND CUSTOMER NOTICE, published in March 2005 by, and applicable to all financial institutions regulated by, the Federal Reserve System, Federal Deposit Insurance Corporation, and Department of the Treasury – Offices of the Comptroller of the Currency and Thrift Supervision (available at www.occ.treas.gov/consumer/customernoticeguidance.pdf); and the Interim Recommendations of the President’s Identity Theft Task Force, released September 2006, that includes factors that should govern whether and how notice should be given to affected individuals in the event of a government agency data breach (available at www.ftc.gov/opa/2006/09/idtheft.htm).

⁶ Cal. Civil Code §§ 1798.29, 1798.82 and 1798.84.

⁷ See, Associated Press, “Hackers Steal California State Employees Social Security Numbers?” May 24, 2002; NAMIC Issue Brief – “Security Breach Notification Laws: What Threats Do They Pose for Insurers?” July 2005 (available at www.namic.org/policy/papers.asp), citing “Computer Break-Ins: Your Right to Know,” BusinessWeek Online, November 11, 2002.

⁸ “Computer Break-Ins: Your Right to Know,” BusinessWeek Online, *supra*.

⁹ *Id.*

¹⁰ See, e.g., “Into the Breach,” The National Law Journal Online, August 4, 2006.

¹¹ The California Notice Law also applies to state governmental agencies. Cal. Civil Code § 1798.29. Some, but not all, other states' laws apply to both businesses and state governmental entities or just to governmental entities. *See, e.g.*, Pennsylvania's data breach notification requirements apply to all businesses as well as state agencies and political subdivisions (73 Pa. Cons. Stat. § 2301 *et seq.*); Oklahoma's data breach notification requirements apply only to state agencies and political subdivisions (74 Okla. Stat. § 3113.1 *et seq.*).

¹² Cal. Civil Code § 1798.29 (emphasis added). Note that a person or business that maintains but does not own or license the data is required to provide notice to the Data Holder, who is then required to meet the notification requirements to affected individuals.

¹³ *Id.*

¹⁴ *Id.*

¹⁵ *Id.*

¹⁶ 15 U.S.C. 7001 *et seq.* Under the E-Sign Act, sending a notice in electronic form is acceptable only if the individual has affirmatively consented to receive an electronic notice in lieu of a paper notice.

¹⁷ *Id.*

¹⁸ *Id.*

¹⁹ Cal. Civil Code §§ 1798.80 and 1798.84.

²⁰ La. Rev. Stat. Ann. § 3074.

²¹ Ohio Rev. Code Ann. § 1349.19.

²² Fla. Stat. ch. 817.5681.

²³ Minn. Stat. § 325E.61.

²⁴ N.Y. Gen. Bus. Law § 899-aa.

²⁵ 6 Del. Code Ann § 12B-101.

²⁶ N.C. Gen. Stat. § 75-65.

²⁷ N.C. Gen. Stat. §§ 75-605 and 14-113.20.

²⁸ N.D. Cent. Code §§ 51-30-01.

²⁹ La. Rev. Stat. Ann. § 3075.

³⁰ 6 Del. Code Ann § 12B-104.

³¹ "Into the Breach," The National Law Journal Online, *supra*.