PROSKAUER ROSE LLP®

Client Alert

A report
for clients
and friends
of the firm

October 2005

States Continue to Pass Security Breach Notification Laws: Businesses Must Comply With Various and Sometimes Conflicting Regulations

This year, legislators across the country responded to consumer fears of identity theft, heightened by highly publicized data security breaches, by passing laws requiring consumer notification when there are security breaches involving private information. In all, twenty states and New York City have passed security breach notification laws.[1] The new laws largely follow California's first-in-the nation information security breach notification law, but with key differences and compliance requirements.

The California Framework

The Security Breach Information Act, California Civil Code § 1798.82 *et seq*, was the first law passed in the United States that requires notification to customers for security breaches of personal information. The California law, and most state security breach notification schemes, *require notification to individuals if their computerized personal information "was, or is reasonably believed to have been, acquired by an unauthorized person."*[2]

Personal Information, in California and elsewhere, 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.*

Subsequent sections of the California Code provide for three exemptions from the disclosure requirements. One broad exemption is for personal information in encrypted form. The second is to maintain a present interest in a criminal investigation by law enforcement. The third is for breaches that are either immaterial or are not "reasonably likely to subject the customers to unauthorized disclosure of personal information." Other states have developed exemptions for unauthorized access to information that is made available to the public by government agencies or for entities that are already regulated under federal privacy laws (*e.g.* Gramm-Leach-Bliley Act or the Health Insurance Portability and Accountability Act).

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, more than 500,000 people are affected, or the individual's contact information is unknown, then notice may be effected through media outlets.

Beyond this basic framework, several new state laws have other data security provisions, including:

---

[1] For a more detailed analysis of California's security breach notification law, the ChoicePoint data theft, and the New York City security breach notification laws, please review the respective Proskauer Rose LLP Client Alerts on those issues.

New California Law Requires All Companies That Do Businesses In State To Provide Notice Of Computer Security Breaches, Proskauer Rose Client Alert, January 2003.

ChoicePoint Data Theft a Wake-Up Call for Companies to Evaluate Their Legal Exposure for Computer and Data Security Breaches, Proskauer Rose Client Alert, March 2005.

New York City Enacts Laws Imposing New Burdens on Businesses Holding Personal Data, Proskauer Rose Client Alert, May 2005.

[2] Cal. Civil Code §§ 1798.82 (b).

- A requirement for preventative security measures, including reasonable security policies for maintenance and disposal of personally identifying information
- Notification requirements to national Consumer Reporting Agencies documenting customers affected by security breaches of personal information
- A private right of action to recover actual damages from businesses who fail to notify customers of a security breach without unreasonable delay
- Expansion of the definition of "personal information"
- Civil penalties for failure to promptly notify customers of a security breach
- Granting consumers the right to place a "credit freeze" on their credit reports, preventing outside review of a credit report without actual authorization from the consumer
- Restrictions on the sale and use of Social Security Numbers
- Enhanced criminal penalties for the organic violation of fraudulently acquiring or using the personal information of another

Unique Provisions of the State Laws

Below is a review of the key provisions that impact security breach notification procedures in each of the jurisdictions that passed legislation regulating this area. These summaries discuss each jurisdiction's defining, but not exhaustive, differences with the basic California framework.

Arkansas S.B. 1167, Act 1526 (effective March 31, 2005)
Arkansas includes in its definition of personal information medical records in physical and computerized form, adding a substantial amount of information that businesses must manage with care. Further, the law mandates that personal information no longer retained by an entity must be properly disposed of in order to avoid liability. The Arkansas law requires businesses to "implement and maintain reasonable security procedures and practices...to protect the personal information from unauthorized access, destruction, use, modification or disclosure."[3]

Connecticut S.B. 650, Public Act No. 05148 (effective January 1, 2006)
A business may forego notice to Connecticut residents if law enforcement determines that there is no reasonable likelihood of harm to consumers.[4] Notification options for businesses to affected individuals are expanded to include notification by telephone.[5]

Delaware H.B. 116 (effective June 28, 2005)
Written notification of a security breach must be provided to the Consumer Protection Division of the Delaware Department of Justice, in addition to individual consumers. Delaware also expands the definition of "personal information" to include medical information.[6] The statute contains a private right of action whereby a harmed individual can recover treble damages and attorney's fees.[7]

Florida H.B. 481 (effective July 1, 2005)
In Florida, there is a forty-five day grace period for notification after the security breach is reported to law enforcement. If notification to consumers is not performed within this time period, fines of up to $1,000 per day for thirty days are possible. If customers are not notified of the security breach after thirty days, fines increase to $50,000 for each subsequent thirty day period, continuing for the next 180 days. If no notification of the security breach occurs within 255 days, the State may issue a $500,000 administrative fine. Further fines of up to $50,000 are specified for failure to document the breach, or for failure to keep records of the breach for up to five years.[8]

Georgia S.B. 230 (effective May 5, 2005)
Georgia's law applies only to computerized data held by consumer "information brokers", such as credit agencies and background investigation firms. Information brokers must notify affected consumers in the event of a security breach relating to personal information "that is sufficient to perform, or attempt to perform an identify theft."[9] The bill includes a safe harbor provision for information brokers that follow their own security and notification policies that are consistent with the Georgia law. No substitute notice provision exists in this law, regardless of cost of notification or the number of people affected.

---

[3] Ark. Act 2526 Sec. 1, part 4-110-104 (b).

[4] Conn. S.B. 650, Sec. 3(b).

[5] Conn. S.B. 650, Sec. 3(e)(2).

[6] Del. H.B. 116 §12B-101(2).

[7] Del. H.B. 116 §12B-104(a).

[8] Fla. H.B. 481, amending Sec. 817.5681 (2)(b).

[9] Ga. S.B. 230, § 10-1-911 (5)(E).

Illinois H.B. 1633, Public Act 94-36 (effective January 1, 2006)
Entities responsible for protecting personal information are expanded to include "government agencies, public and private universities, privately and publicly help corporations, financial institutions, retail operators, and any other entity that, for any purpose, handles, collects, disseminates, or otherwise deals with nonpublic personal information."[10]

Indiana S.B. 503, Act 503 (effective July 1, 2006)
Indiana's notification law applies only to state agencies. In addition to security breach notification requirements, the law calls for increased restrictions on disclosing Social Security Numbers held by agencies. The Indiana law requires individuals who prepare documents for recording by the County Recorder to review the entire document and redact Social Security Numbers, under penalty of perjury. Starting in 2008, the bill requires County Recorder officers to redact Social Security Numbers before documents are released for public inspection.[11]

Louisiana S.B. 205, Act 499 (effective Jan. 1 2006)
Louisiana's legislation illustrates the evolving standards to trigger notification. Louisiana requires notification if, "after a reasonable investigation, there is reasonable likelihood of harm to customers."[12] This will require notification in fewer instances than the prevailing norm, which requires notification when personal information "was, or is reasonable believed to have been, acquired by an unauthorized person."[13] In Louisiana, a wider range of business entities must notify customers of a data security breach because the statute defines "person" to include corporations, partnerships, sole proprietorships, joint stock companies, or any other legal entity.[14]

Maine Ch. 379, 210-B (effective Jan. 1 2006)
In Maine, data brokers must report unauthorized access to a consumer's personal information to the consumer, Consumer Reporting Agencies and state regulators.[15] The Department of Professional and Financial Regulation, Office of Consumer Credit Regulation will enforce this law, which provides for civil violation penalties ranging from $500 to $2,500 for each day a broker is in violation of the notice requirements.[16]

Minnesota H.F. 2121, Ch. 167 (effective Jan. 1, 2006)
Minnesota mandates notification to consumer reporting agencies within 48 hours if notice is required under the statute to more than 500 consumers.[17]

Montana H.B. 732, Ch. 518 (effective March 1, 2006)
The new Montana law expands the definition of "personal information" to include: telephone numbers, personal addresses, passport numbers and insurance policy numbers. A Social Security Number *alone* is also considered personal information.[18] The legislation prohibits printing the last five numbers of a credit card on electronically printed receipts. Businesses with more than twenty employees will be required to disclose, upon request, all parties who have received an individual's personal information.

Nevada S.B. 347 (rolling effective dates)
Nevada is the first state to *require* encryption for all transmissions of personal information outside of secure networks. Encryption is defined more rigorously than other states, meaning any protective or disruptive measure, including cryptography, enciphering, encoding or a computer contaminant, to: 1) prevent access, impede, delay or disrupt access to any data; 2) make data unintelligible or unusable; or 3) prevent normal operation or use of any component, device, equipment, system or network.[19] This definition suggests a requirement of Secure Socket Layer (or comparable) encryption technology. In order to provide businesses with time to modify their information technology, these provisions become effective October 1, 2008.

Under the new Nevada law, businesses whose contracts involve disclosure of personal information, must include a provision requiring parties receiving personal information to implement and maintain reasonable security measures to protect the personal information from unauthorized access, acquisition, destruction, use, modification or disclosure.[20] Data collectors are granted their own right of action against a person that unlawfully obtains personal information from

---

[10] Ill. S.B. 1633 Sec. 5.

[11] 2005 Ind. Act 503, Ch. 7.5, Sec. 1 *et seq.*

[12] La. S.B. 205, Act. 499, § 3073(2),(3)(emphasis added).

[13] California Civil Code § 1798.82 (b).

[14] La. S.B. 205, Act. 499, § 3073(2),(3).

[15] Maine Ch. 379 sec 1.10 c.210-B § 1348. The Maine definition of "data broker" does not include a state agency.

[16] Maine Ch. 379 sec 1.10 c.210-B § 1349(2).

[17] Minn. Ch. 167, H.F. 2121 Subd. 2.

[18] Mont. H.B. 732 Sec. 3 (3).

[19] Nev. S.B. 347 Sec. 29(2)(a). The definition of encryption is incorporated by reference to the 1995 "Computer Crime Act", NEV. REV. STAT. § 205.4742.

[20] Nev. S.B. 347 Sec. 23(2).

the data collector's records.[21] These provisions of the Nevada law are effective January 1, 2006.

New Jersey A. 4001 (effective July 2, 2006)
New Jersey expands the definition of personal information to include, "dissociated data that, if linked, would constitute personal information. . . . if the means to link the dissociated data were accessed in connection with access to the dissociated data."[22] Unique to the New Jersey law is a provision requiring written documentation of a security breach investigation that excuses notification to consumers by determining misuse of the information was not possible. All security breaches must be reported to the State Police before notifying customers.[23]

New York A.B. 4254—A (effective Dec 8, 2005)
New York law mandates notification of security breaches to the Attorney General and relevant state regulatory offices, in addition to individual consumer notification.[24] While there is no private right of action, the Attorney General may sue on behalf of affected parties for actual and consequential damages. For knowing or reckless violations there may be fines of the greater of $5,000 or $10 per failed notification, provided a per occurrence fine does not exceed $150,000.[25]

The new legislation allows for notice by telephone, but all telephone and electronic notifications of a data security breach must be logged. Further, electronic notification must be consented to, and this consent cannot be a condition of establishing a business relationship or engaging in a transaction.[26] The notification to individuals must include contact information for the notifying party and a full disclosure of the extent and categories of compromised personal information.

Finally, the law explicitly preempts local and city government laws that are inconsistent or more restrictive then the state law, thus may override significant portions of the New York City ordinances which address security breaches.[27]

New York City
Mayor Bloomberg signed three bills into law which took effect in September 2005.[28] The measures require businesses licensed by the Department of Consumer Affairs ("DCA") to notify consumers of security breaches when the consumer's personal information is compromised due to unauthorized access and to securely destroy records containing personal information. Businesses that are licensed or regulated by the DCA must immediately report security breaches of personal information to the DCA in the following situations: (1) an adverse judgment for identity theft against the business, or (2) any criminal conviction of a business, associate, or employee for either identity theft or illegal possession of personal information. DCA is authorized to revoke or deny the license of any business convicted of identity theft. City agencies that own or lease data containing personal information must first notify the police, and then notify affected individuals when unauthorized access to personal information has occurred.

North Carolina S.B. 1048, Session Law 2005-414 (effective October 1, 2006)
The content of the consumer notice in North Carolina must include: 1) the incident in general terms, 2) the type of personal information that was the subject of the breach, 3) the general acts of the business to protect the personal information from further unauthorized access, 4) a telephone number that the person may call for further information and assistance, and 5) advice that directs the consumer to remain vigilant by reviewing account statements and monitoring free credit reports.[29]

North Dakota S.B. 2251 (effective June 1, 2005)
The category of personal information is expanded to include: date of birth, mother's maiden name, employee identification numbers, an employer's name or address, digital or electronic signatures or an individual's birth, death, or marriage certificate.[30]

Rhode Island (H. 6191-Sub A/2) (effective March 1, 2006)
The Rhode Island legislation only requires notification if the security breach "poses a significant risk of identity theft."[31] Notification is not required if, after a consultation with law enforcement authorities, it is determined that a breach will not likely result in identity theft. Rhode Island specifies

---

[21] Nev. S.B. 347 Sec. 25.

[22] N.J. A. 4001 Sec. 10.

[23] N.J. A. 4001 Sec. 12(c)(1), 12 (f).

[24] Consumer Protection Board and State Office of Cyber Security and Critical Infrastructure Coordination.

[25] N.Y. A.B. 4254-A, S. 899-AA S. 9, Sec. 6(a).

[26] N.Y. A.B. 4254-A, S. 208 5 (B).

[27] N.Y. A.B. 4254-A S. 899-AA S. 9

[28] New York City Intro. Nos. 139-A, 140-A, 141-A (2004).

[29] N.C. Session Law 2005-414 § 75-65(d).

[30] N.D. CENT. CODE § 51-30-01 (2)(a).

[31] R.I. H. 6191-Sub A/2, Sec 1, 11-49.2-3 (b).

monetary penalties for notification failures, up to $100 per occurrence and not more than $25,000.

Tennessee H.B. 2170, Ch. 473 (effective July 1, 2005)
This was the first law granting a private right of action for damages and injunctive relief for injury resulting from a violation of the security breach notification statute.[32]

Texas S.B. 122 (effective September 1, 2005)
Texas requires notification to national Consumer Reporting Agencies if more then 10,000 Texas residents are affected by a security breach.[33] Texas requires the notice to Consumer Reporting Agencies include an explanation of the timing, distribution, and content of the notification provided to individuals affected by the security breach.

Washington S.B. 6043, Ch. 368 (effective July 24, 2005)
Washington creates a private right of action for civil damages or injunctive relief against entities that violate its law requiring notification of security breaches relating to personal information.[34] The law applies equally to agencies, businesses, and individuals. The law contains a safe harbor provision under which an agency "shall not be required to disclose a technical breach of the security system that does not seem reasonably likely to subject customers to a risk of criminal activity."[35]

Federal Legislation

The compliance difficulties presented to industry by this patchwork of state laws has prompted federal legislators to take action. Several data security bills were introduced in Congress this year, the most prominent are:

Identity Theft Protection Act of 2005, S. 1408
Approved July 28, 2005 by the Senate Commerce Committee, this legislation would require companies to notify consumers and the FTC when their personal information is compromised and there is a "reasonable risk of identity theft." Businesses, schools and other organizations that hold sensitive personal information would be required to secure it with physical and technological safeguards specified by the FTC. This legislation, sponsored by Senators Smith (R-Ore.) and Nelson (D-Fla.), would preempt state security breach notification laws.

Personal Data Privacy and Security Act of 2005. S. 1789
On September 29, 2005 Senators Specter (R-PA) and Leahy (D-VT) introduced an amended version of this legislation that requires a company that collects personal information to notify individuals whose information is compromised if there is a "significant risk" that the security breach will result in harm. The bill requires companies to notify individuals "without unreasonable delay" (revised from the bill's previous 14-day requirement). Under the bill's current provisions, individuals within a company that intentionally withhold consumer notification face criminal liability. The extent of the measure's preemption of state notification laws remains unclear. This legislation was discussed in the Judiciary Committee on October 20, 2005 but no action was taken.

The Personal Data Security Act, S. 1326
This measure, introduced in June by Sen. Sessions (R-Ala.), contains significantly less regulation of data security technology and practices than the Specter-Leahy legislation. This bill requires notice when "a reasonable investigation" determines there is a significant risk of identity theft. The Sessions measure would completely preempt any state or local law that relates to electronic data security or breach notification. This legislation was passed by the Judiciary Committee on October 20, 2005.

Financial Data Protection Act of 2005, H.R. 3997
Introduced by several members of the House Financial Services Committee, this bill requires notice to consumers only if breached information is reasonably likely to be misused. Institutions are required to provide consumers with a free six-month nationwide credit monitoring service upon notification of a breach. In order to ensure uniformity, national standards for the protection of sensitive consumer information would be jointly issued by the Secretary of the Treasury, the Federal Reserve Board and the Federal Trade Commission. A safe harbor from lawsuits is included in the bill for companies with reasonable data protection polices and procedures in place. The bill contains strong preemption language that would not permit states to set their own standards. The House Financial Services Committee heard this legislation on October 27, 2005.

Federal legislation that preempts state law would make security breach notification obligations clearer for businesses. However, until such federal legislation becomes law, businesses must do all they can to comply with the various and sometimes conflicting requirements imposed by states.

For further information, contact Christopher Wolf, Chair of the Proskauer Privacy and Data Security Practice Group, 202-416-6818, *cwolf@proskauer.com*.

---

[32] Tenn. Title 47, Ch. 18, p. 21.

[33] Texas S.B. 1222, Sec. 48.103(h).

[34] Wash. S.B. 6043 Sec 1. 10(a).

[35] Wash. S.B. 6043 Sec. 2 (9)(d).

NEW YORK • LOS ANGELES • WASHINGTON

BOSTON • BOCA RATON • NEWARK

NEW ORLEANS • PARIS

Client Alert

Privacy law is a relatively new area of law, but it is one of increasing importance to business. Although the United States does not have an across-the-board privacy law, there is a wide array of legislation and case law affecting specific information and industries. For more information about this practice area, contact:

Christopher Wolf
202.416.6818 – cwolf@proskauer.com

Proskauer Rose is an international law firm that handles a full spectrum of legal issues worldwide.

You can also visit our Website at **www.proskauer.com**