MINTZ LEVIN
When You Need More...

PRIVACY AND SECURITY
ALERT

FEBRUARY 21, 2007

Boston

Washington

New York

Stamford

Los Angeles

Palo Alto

San Diego

London

www.mintz.com

One Financial Center
Boston, Massachusetts 02111
617 542 6000
617 542 2241 fax

701 Pennsylvania Avenue, N.W.
Washington, D.C. 20004
202 434 7300
202 434 7400 fax

666 Third Avenue
New York, New York 10017
212 935 3000
212 983 3115 fax

707 Summer Street
Stamford, Connecticut 06901
203 658 1700
203 658 1701 fax

Six Additional State Data Security Breach Notification Laws Become Effective in 2007

With heightened awareness of the value and vulnerability of personal and financial information collected by businesses and governments, more states are enacting legislation to require consumer notification when there are security breaches involving this information. In 2006, 35 states and the District of Columbia introduced legislation addressing security breach notification. The latest legislation—Arizona, Hawaii, Maine, New Hampshire, Utah and Vermont—became effective in January 2007.

Below is a brief summary of the newly effective laws. A full comparison matrix of the various state data breach laws is available here.

Arizona

The Arizona law covers any person that conducts business in Arizona and owns or licenses computerized data that includes personal information. If the business becomes aware of an incident of unauthorized acquisition of data that includes personal information, the business is required to investigate to determine if there has been a breach in the security system. If there is a breach, the business is required to notify the affected Arizona consumer. Notification is not required if the business or law enforcement officials determine after a reasonable investigation that the breach will not cause or is unlikely to cause "substantial economic loss" to an individual. Willful and knowing violations of the law can result in a fine of up to $10,000 per breach incident. The law became effective December 31, 2006 and is codified at Arizona Revised Statutes, Title 44, Chapter 32, 44-7501.

Hawaii

Hawaii's security breach notification law is different from most states in that it also covers paper records as well as computerized data of personal information. Businesses and state agencies are required to

1620 26th Street
Santa Monica, California 90404
310 586 3200
310 586 3202 fax

1400 Page Mill Road
Palo Alto, California 94304
650 251 7700
650 251 7739 fax

9255 Towne Centre Drive
San Diego, California 92121
858 320 3000
858 320 3001 fax

The Rectory
9 Ironmonger Lane
London EC2V 8EY England
+44 (0) 20 7726 4000
+44 (0) 20 7726 0055 fax

alert Hawaiian residents if an unauthorized user gains access to their unencrypted or unredacted personal data. Notice is required to the affected person only when illegal use of the information has occurred or is "reasonably likely to occur or that creates a material risk of harm to the person." Businesses found to be in violation of the law can be liable for a fine of up to $2,500 per violation and for any actual damages faced by an individual. The law became effective January 1, 2007 and it is codified at Hawaii Revised Statutes, Title 26, Act 135.

Maine

On January 1, 2006, Maine enacted a law requiring only information brokers to notify customers when unauthorized persons obtain personal data that could result in identify theft. In April 2006, the Maine legislature amended the law to apply it more broadly to include other individuals and business entities who maintain computerized data that includes personal information. If a security breach is suspected, a covered entity is required to determine the scope of the breach, take steps to prevent future breaches and to notify the affected individuals. Notification is required if the personal information has been or is reasonably possible to be misused. Maine also requires the covered entities to notify the national consumer reporting agencies if more than 1,000 persons must receive notification of the breach. Covered entities found to be in violation of the act can be fined up to $500 per violation for each day the person violates the law up to $2,500. The revised law became effective January 1, 2007. The law is codified at Maine Revised Statutes Title 10, Chapter 210-B, §§ 1346–1349.

New Hampshire

New Hampshire's data breach notification law requires any person doing business in New Hampshire to notify (or cooperate in notifying) individuals who are affected by a security breach of unencrypted computerized data that contains personal information. Suspected misuse of personal information must be investigated to determine if there has been misuse or if there is reasonable likelihood of misuse. Prompt notification to the affected persons is required. If the business cannot determine whether the information has been misused, the New Hampshire law requires notification. Delay in notification is only permitted if prompt notice would impede a criminal investigation or jeopardize national security. If the total cost of providing notice is more than $5,000 or if more than 1,000 people must be notified, notification can occur through a form of publication in a statewide media outlet, posting on the business website or by email. When more than 1,000 persons must be notified, all consumer credit reporting agencies must be notified also. Regulated businesses must notify their primary regulator and all other businesses must

notify the state attorney general's office. The law became effective January 1, 2007 and is codified at New Hampshire Revised Statutes, Title XXXI, § 359-C.

Utah

Persons maintaining personal information in connection with a business are required to implement procedures to protect the personal information. They are also required to destroy certain records and disclose security breaches involving personal information. The Utah law is unique from other states in that notice to affected individuals can be accomplished through publication in a newspaper in lieu of personalized notification through email or mail for instance. Notification is not required if the business conducts an investigation and determines that there is not a likelihood of misuse of the data for identity theft or fraud. The law also requires businesses to destroy electronic and paper records of personal data they do not plan to retain. Violations can result in fines of $2,500 per violation and not more than $100,000 in the aggregate for violations involving more than one person. The law became effective January 1, 2007 and is codified at Utah Code, Title 13, Chapter 42, §§ 101–301.

Vermont

Vermont enacted a comprehensive law that addresses data security breaches, social security number protection and the safe destruction of documents. The Security Breach Notice Act requires "data collectors" to notify affected Vermont residents when misuse of personal information has occurred or is occurring. A data collector includes state agencies, universities, corporations, limited liability companies, financial institutions, retail operators, or other entities that handle, collect, disseminate or otherwise deal with nonpublic information. Notice must be provided to the affected individuals unless the data collector would spend more than $5,000 to provide notice or the class of affected consumers exceeds 5,000 persons. In that case, notice can be accomplished through the data collector's website or through statewide or regional media outlet. With data breaches involving more than 1,000 consumers, the consumer reporting agencies must be notified of the breach. The Vermont law became effective January 1, 2007 and it is codified at Vermont Statutes, Title 9, §§ 2430–2445.

What Does All This Mean for Your Business?

The electronic nature of business and the portability of data now means that business is often conducted across state lines, thus bringing a business with its principal office in Massachusetts, for example, under the regulation of many states with respect to the

responsibilities and obligations to residents of other states on whom the Massachusetts business may have data. Companies need to prepare to address data breaches in advance and prepare response plans that include notification and that outline when and under what circumstances to notify law enforcement and those responsible to notify regulators and shareholders.

Federal legislation that could preempt state laws and address many issues could be forthcoming in this session of Congress, however, a full preemption may be difficult to obtain. Mintz Levin will continue to monitor federal and state developments in this critical area.

Privacy and security issues touch virtually ever aspect of an organization's operations, including online activities, to cross-border commerce, to workplace policies and procedures.

*****

For assistance in this area, please contact:

Cynthia Larose
617.348.1732 | CJLarose@mintz.com

Stefani Watterson
202.661.8706 | SVWatterson@mintz.com

or any Mintz Levin attorney with whom you regularly work.