

To our clients and friends:

MINTZ LEVIN

When You Need More...

PRIVACY AND SECURITY

ALERT

AUGUST 22, 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

Massachusetts and Oregon Join Numerous Other States by Adopting Data Breach Notification Legislation

Massachusetts and Oregon have become the two latest states to join the flood of data breach notification legislation, bringing the total number of such state laws to 39.

Although there are several pieces of federal legislation working their way through Congress that may help businesses to address the growing compliance problem by preempting conflicting state laws, as of this writing, no federal action has been forthcoming.

Beginning February 3, 2008, businesses and Massachusetts government agencies that maintain, store, lease or own personal information of Massachusetts residents will be required to notify consumers when that information is lost or stolen. The data breach notification legislation, which was signed into law on August 3, 2007, has several features that differentiate it from other state data breach notification laws, including civil penalties. In addition to the owners or licensors of personal data, the Massachusetts law imposes specific notification requirements on businesses that merely *store or maintain* personal data. The law requires business entities that store or maintain, but do not own, personal data to provide notice as soon as possible to the owner or licensor of the data. As with other similar state laws, entities that own or license the personal data are required to provide notice to Massachusetts residents if there has been a security breach compromising personal information. Another requirement of which to be aware is the additional reporting requirement: The owner or licensor must also provide notice to the Massachusetts' attorney general, director of consumer affairs and business regulation and ultimately to the consumer reporting agencies and state agencies identified by the director of consumer affairs. Notice must be given "as soon as possible" and "without unreasonable delay."

203 658 1701 fax

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

Like most states with data breach notification laws, personal information includes first name or initial and last name combined with one of the following: social security number, driver's license number, state identification card or passport number or financial account information along with password or security code information. A breach is defined as an unauthorized acquisition or use of unencrypted data. A breach also occurs when the security of encrypted data is compromised.

Businesses that own or lease the data must provide notice to Massachusetts' residents by written or electronic means. Substitute notice is permitted if the cost of providing written notice exceeds \$250,000 or the number of affected residents exceeds 500,000. The notice must include information about a consumer's right to obtain a police report and detailed information about how a consumer requests a security freeze. The notice should *not* include the nature of the breach or unauthorized use or the number of residents affected by it.

Businesses in compliance with federal laws covering protection and privacy of personal information are considered in compliance with Massachusetts law as long as affected Massachusetts residents are notified in accordance with the federal law. Civil penalties of not more than \$5,000 per violation may be imposed along with costs of any investigation and litigation including attorneys' fees.

The law also requires companies and state agencies to destroy documents and erase data containing personal information when disposing of records.

Oregon's recently adopted breach notification law is somewhat different than Massachusetts' in that it requires businesses to develop, implement and maintain reasonable safeguards to protect the security and confidentiality of personal information. A business is considered in compliance with the Oregon law if it implements a data security program that meets certain technical, physical and administrative standards. Notice is required in Oregon if unauthorized access of data "materially compromises" the confidentiality or security of personal information. For a comparison of the Massachusetts and Oregon laws, and other pending and enacted state data breach notification laws, [click here](#).

Businesses should take action to limit exposure by reviewing their data collection practices and implementing an incident response plan that would comply with the notice requirements in the various states in which they have customers.

For assistance in this area, please contact:

Cynthia Larose, CIPP
617.348.1732 | CJLarose@mintz.com

Stefani Watterson, CIPP
202.661.8706 | SVWatterson@mintz.com

or any Mintz Levin attorney with whom you regularly work.

Copyright © 2007 Mintz, Levin, Cohn, Ferris, Glovsky and Popeo, P.C.

The above has been sent as a service by the law firm of Mintz, Levin, Cohn, Ferris, Glovsky and Popeo, P.C. and may be considered an advertisement or solicitation under federal law. The distribution list is maintained at Mintz Levin's main office, located at One Financial Center, Boston, Massachusetts 02111. If you no longer wish to receive electronic mailings from the firm, please notify our marketing department by going to www.mintz.com/unsubscribe.cfm.