EDWARDS ANGELL PALMER & DODGE

eapdlaw.com

Client Advisory | *October 2008*

Information Security Breaches and Appropriate Responses — New Mandatory Security Rule in Massachusetts and Privacy Policy in Connecticut

An increase in data breaches affecting various industries, including banking, insurance and other financial services, has been profiled recently. These developments require companies to anticipate problems, develop new responsive policies and protective procedures, and react quickly to near-crisis situations resulting from data breaches.

Mark E. Schreiber, Partner
Chair, Privacy Group

Theodore P. Augustinos, Partner

The legislative changes and new rules in this area will require more activity and rigor by companies and employers holding personal data. Massachusetts, for example, has become one of the first states in the country to require, as of January 1, 2009, that all companies which store personal data, as defined, have a comprehensive written security plan with required elements, including encryption, wireless protections and third party vendor scrutiny.

Federal prosecutors have charged 11 people, from the United States, Estonia, Ukraine, China and Belarus, with stealing more than 41 million credit and debit card numbers from national stores in the US—a scheme considered to be the largest in US history. The accused individuals allegedly obtained the credit and debit card numbers by finding security holes in the wireless networks of retailers. They reportedly installed "sniffer" programs which then tapped into the networks that retailers used for processing credit cards and intercepted the PIN, debit and credit card numbers of customers. The numbers were then sold online or imprinted onto magnetic strips of blank cards for withdrawal from ATMs.

The recently disclosed loss of data transmitted by a large regional bank to its transfer agent affected about 556,000 of the bank's consumers. The information was transmitted in encrypted format. However, the transfer agent apparently converted the information to an unencrypted format and stored it with customer information it had received from other institutions, according to reports. The combined, unencrypted information, affecting about 4.5 million people nationwide, was lost. Each of the institutions was required to notify its customers and the transfer agent offered to provide two years of credit monitoring services and up to $25,000 in identity theft insurance.

These dramatic events illustrate the potential pitfalls related to the handling, storage and transmission of personal financial information in the current legal and regulatory environment. Even absent any fault of their own, institutions can incur significant cost, reputational injury and inquiries of states' Attorneys General or other agencies as a result of a data breach.

Other more mundane breaches have been reported on a nearly daily basis during the past few years. These incidents regularly include lost and stolen laptops, pda's, other devices or backup tapes; office break-ins; computer hacks; or data exposures of many different varieties, including by employees or as a result of human error.

New Notification, Alert and Privacy Laws

With some 46 jurisdictions now having data breach notification laws, state requirements continue to develop and additional changes in statutes and regulations concerning information privacy and security are expected. As of November 1, 2008, so-called "red flag" rules for the financial industry will be

in effect, driving even further security and alert procedures.

New Massachusetts Security Rule

The Massachusetts Office of Consumer Affairs and Business Regulation recently issued 201 CMR 17.00, Standards for the Protection of Personal Information of Residents of the Commonwealth (the "Regulation"). The Regulation, effective January 1, 2009, establishes minimum standards for safeguarding personal information contained in both paper and electronic records, and in some instances go beyond federal law. Under the Regulation, every person (the definition of "person" includes business entities) that owns, licenses, stores or maintains personal information about a resident of Massachusetts is required to develop, implement, maintain and monitor a comprehensive, written information security program applicable to any records containing such personal information.

The comprehensive information security program must be reasonably consistent with industry standards and must contain administrative, technical and physical safeguards to ensure the security and confidentiality of such records. The following are several elements required by the Regulation for every comprehensive information security program: security policies for employees that take into account whether and how employees should be allowed to keep, access and transport records containing personal information outside of business premises; reasonable steps to verify that third party service providers with access to personal information have the capacity to safeguard the personal information, including training and contractually requiring such safeguards; and documentation of responsive actions taken in connection with any incident involving breach of security and mandating post-incident review of events and changes made to business practices.

The Regulation also sets forth security requirements for computer systems. Under the Regulation, every person that owns, licenses, stores or maintains personal information about a Massachusetts resident and electronically stores or transmits such information must include the establishment and maintenance of a security system covering its computers, including any wireless system, in its written, comprehensive information security program. Specifically, the Regulation sets forth required user authentication protocols, access control measures, encryption requirements, monitoring requirements and software features. See link: http://www.mass.gov/?pageID=ocatermina l&L=3&L0=Home&L1=Consumer&L2 =Identity+Theft&sid=Eoca&b=termin alcontent&f=idtheft_201cmr17&csid =Eoca

Of particular concern to many businesses are the encryption requirements, which apply to all personal information stored on laptops and other portable devices, and all transmitted records and files traveling across public networks and wirelessly.

New Connecticut Law on Privacy Policy

In the first half of 2008, Connecticut amended its laws about using SSN's and requiring mandatory posted privacy policies, and Alaska, Iowa, South Carolina, Virginia and West Virginia enacted data breach laws that are either now effective or will be next year. New York has also passed the Social Security Number Protection Law, which penalizes employers for failure to manage the documentation and use of employee Social Security numbers.

In June 2008, Connecticut adopted "An Act Concerning the Confidentiality of Social Security Numbers." That law, which becomes effective October 1, 2008, requires any person who collects Social Security numbers in the course of business to create a privacy protection policy. The policy, which must be published or publicly displayed, must: (1) protect the confidentiality of Social Security numbers; (2) prohibit unlawful disclosure of Social Security numbers; and (3) limit access to Social Security numbers. The policy may be posted on an Internet website to satisfy the public display requirement.

Under the new Connecticut law, any person in possession of personal information of another person must safeguard the data, computer files and documents containing the information from misuse by third parties and destroy, erase or make unreadable the data, computer files and documents prior to disposal. The Act defines "personal information" as information capable of being associated with a particular individual through one or more identifiers, including, but not limited to, a Social Security number, a driver's license number, a state identification card number, an account number, a credit or debit card number, a passport number, an alien registration number or a health insurance identification number. Although the Act does not provide a private right of action, anyone who intentionally violates the Act is subject to a civil penalty of $500.00 for each violation.

Responding to Data Breaches

Developing and maintaining an active data breach response process and policy is rapidly becoming a best practice, and, as noted, is already required in some jurisdictions. Once a data breach incident occurs, facts must be gathered, remediation and preventative measures undertaken, and consumers and state agencies notified. First, the details and scope of the incident involving the data breach must be obtained and ascertained. The nature of the breach and the types of information lost or stolen must be determined. The number and identities of affected individuals, and their places of residence must be identified.

Once an investigation to obtain such information has been conducted (often by forensic experts), a review of data breach laws of the states in which affected individuals reside is necessary. The goal of this review is to determine whether the data breach law of a state is triggered and whether notice is required. Some factors that

trigger notice requirements include the following: whether the type of information lost or stolen constitutes "personal information," or like terms, as defined in the state's data breach law; whether the unauthorized acquisition or use constitutes "breach of security of the system," as defined; whether the company subject to the breach owns or licenses the lost or stolen information or is a third party vendor; and, if the state's data breach law provides for a harm threshold, whether there is harm or likelihood of harm.

If it is determined that the data breach laws of certain states are triggered, the specific, and sometimes conflicting, legal and regulatory requirements for notifying appropriate state agencies and affected individuals must be analyzed and addressed. Decisions about whether to offer credit monitoring or credit restoration, along with a call-in number facility need to be made. All of these factors, taken together, will determine whether the company has to send notices to individuals and agencies and in which states and with what content – which can be a ponderous and expensive exercise with obvious legal implications.

"One size fits all" notices of data breach will surely be defective in multiple jurisdictions. For example, in connection with the Massachusetts statute, some states specifically require disclosure of certain information concerning an incident that is expressly prohibited from disclosure in Massachusetts. In addition to content, states have different timing requirements for notices to individuals, as well as requirements to notify various state agencies, with different content required in various formats.

Companies need to protect against the significant financial, legal, regulatory and reputational risks related to security breaches by assessing their individual risk level based on the nature of their business and existing technology and infrastructure. The assessment, conducted by the right personnel supported by knowledgeable professionals, may need to be reported to the board of directors. The risk assessment must be followed by the development of an even more robust security program, integrating systems, policies and procedures that address the risk and establish protocols in the event of a breach. As illustrated by the breach events described above, the security program must also extend to vendors and other third parties.

Data breach or cyberinsurance is now frequently being considered as a risk reduction device. This will be an ongoing process for years to come.

"One size fits all" notices of data breach will surely be defective in multiple jurisdictions. For example, as noted above in connection with the Massachusetts statute, some states specifically require disclosure of certain information concerning an incident that is expressly prohibited from disclosure in some other states.

This advisory is for guidance only and is not intended to be a substitute for specific legal advice. If you would like any further information please contact:

Mark E. Schreiber, Partner and Chair, Privacy Group — tel: 617.239.0585 — mschreiber@eapdlaw.com
Theodore P. Augustinos, Partner — tel: 860.541.7710 — taugustinos@eapdlaw.com

EDWARDS ANGELL PALMER & DODGE

111 Huntington Avenue
Boston, MA 02199
Tel 617.239.0100
Fax 617.227.4420
eapdlaw.com