EDWARDS ANGELL PALMER & DODGE

eapdlaw.com

Client Advisory | *January 2010*

Deadlines for Data Security Requirements

This advisory provides a brief summary of new data security requirements with effective and enforcement dates in early 2010 that will affect innumerable businesses.

State Data Security Developments

January 1, 2010: New Amendment to Nevada Privacy Law

- A new amendment to Nevada privacy law that became effective January 1, 2010 requires companies doing business in Nevada that accept payment cards to comply with the Payment Card Industry Data Security Standards ("PCI DSS").
- The new amendment also requires that other data collectors doing business in Nevada encrypt personal information contained in certain kinds of transmissions and when stored on a data storage device.
- While Nevada appears to be the first state to require such compliance, others may follow.
- To view the new amendment to Nevada privacy law, click here.

March 1, 2010: Massachusetts Security Regulation Affecting All Companies with Personal Information of Massachusetts Residents

- Under the Massachusetts Security Regulation (201 CMR 17.00) (the "Regulation"), every person or company that owns or licenses certain personal information about a Massachusetts resident must develop, implement, maintain and monitor a comprehensive written information security program ("WISP").
- The applicability of the Regulation is very broad, extending to any company that has personal information of Massachusetts residents, whether or not the company is doing business in Massachusetts. The Regulation does not exempt any industry, sector or out-of-state business, and does not exempt a de-minimus number of Massachusetts customers, employees or other residents.
- Compliance is required by March 1, 2010. For more information on the Massachusetts Security Regulation, please see our November 2009 Client Advisory.

Federal Data Security Developments

February 17, 2010: Expanded Reach of Federal HITECH Act Protecting Health Information

- The HITECH Act imposed substantial parts of the HIPAA privacy rule and the HIPAA information security rule directly on business associates.
- HITECH imposed changes to the "minimum necessary rule" for the use and disclosure of protected health information for uses and disclosures other than treatment, with the limited data set serving as a "safe harbor" pending further regulations. The Act also requires covered entities to provide patients with a copy of their electronic protected health information ("PHI") in electronic format, or to transmit electronic PHI to other providers in electronic format at the patient's request. Also, new restrictions on the use and disclosure of protected health information for marketing purposes will take effect. Covered entities should have new business associate agreements in place that reflect new privacy and security requirements by this date.
- For more information concerning the health data breach security and notification rules of the HITECH Act, please see our September 2009 Client Advisory.

February 22, 2010: Full Enforcement of Health Data Breach Notification Rules

- Full enforcement of the HIPAA data breach notification rule for covered entities and business associates will begin on February 22, 2010. Similarly, the Federal Trade Commission will begin enforcing the data breach rules applicable to personal health record vendors and their contractors on February 22, 2010.

June 1, 2010: Broad Upcoming Federal Requirements – Red Flags Rule

- The federal Red Flags Rule (16 CFR 681.1) requires that financial institutions and "creditors" (which is very broadly defined) develop and implement written Identity Theft Prevention Programs in order to detect, prevent, and mitigate identity theft.
- For financial institutions, compliance has been required since November 28, 2008.
- For "creditors" that maintain "covered accounts," the Red Flags Rule will go into effect June 1, 2010. The term "creditor" is broadly defined, causing concern that the Red Flags Rule reaches entities other than traditional financial institutions

or creditors that engage in regular loans or advances, including businesses that offer forbearance in the collection of debts or bills, or which allow multiple or extended payments for goods or services that have been previously provided.

- For more information on the Red Flags Rule, please see our November 2009 Client Advisory.

European Data Security Developments

In addition to complying with US data protection, most US companies with subsidiaries in the European Union need to be aware of the data protection laws in the EU, enforcement, and the penalties for non-compliance. There are new penalties for data protection violations and breaches in Germany, and a proposal for increased penalties pending in the UK, as noted below. Further, those publicly traded firms implementing whistleblowing programs for subsidiaries in the EU in order to comply with two important US laws, the Sarbanes-Oxley Act of 2002 and the Foreign Corrupt Practices Act, should also take note of recent important whistleblower decisions, guidelines or directions in France, Denmark, Sweden, Portugal, Austria, and Hungary.

United Kingdom

- Pending the outcome of a recent Ministry of Justice consultation, the Information Commissioner's Office (ICO) in the UK may be given increased statutory powers to impose fines up to £500,000.
- This would apply when the ICO is satisfied that: (i) there has been a serious breach of one or more of the data protection principles of the organizations; and (ii) the breach was likely to cause substantial damage/distress, i.e., if the breach was deliberate or the organization knew or should have known there was a risk, such as by the reckless handling of personal data.
- As some data breaches may include individual names in other countries, the fine levels of those authorities become increasingly important.

Germany

- The German Federal Parliament passed comprehensive amendments to the Federal Data Protection Act, effective September 1, 2009, that cover a broad variety of data protection issues and give fine authority of € 50,000 for simple violations and € 300,000 for serious violations.
- The data protection authorities have been given these new powers to enable them to impose higher fines for failure to comply with data protection requirements, especially on the security side.

For more information on US data security legislation and regulations imposing requirements for the prevention of and responses to data breaches, please see our complimentary webinar, The Continuing Nightmare of Data Breach and Privacy Risks and Regulations: Increasing Risks, New Regulations, and Changing Deadlines.

For more information on EU data protection and whistleblower requirements, see our ABA book chapter, Anonymous Sarbanes-Oxley Hotlines for Multi-National Companies: Compliance with E.U. Data Protection Laws, or link to our "Data Privacy Rules in the EU" podcast interview with *Compliance Week*.

Mark E. Schreiber, Chair, Privacy Group	617.239.0585	mschreiber@eapdlaw.com
Theodore P. Augustinos, Partner	860.541.7710	taugustinos@eapdlaw.com
Laurie A. Kamaiko, Partner	212.912.2768	lkamaiko@eapdlaw.com
David S. Szabo, Partner	617.239.0414	dszabo@eapdlaw.com
Barry J. Bendes, Partner	212.912.2911	bbendes@eapdlaw.com
Eric D. Fader, Counsel	212.912.2724	efader@eapdlaw.com
Socheth Sor, Associate	860.541.7773	ssor@eapdlaw.com