

ClientAlert

April 7, 2010

Privacy and Information Security Law Update, March, 2010

Recent news reports concerning hacking attacks on Google and other companies highlight the growing threat of privacy and information security breaches. We thought this might be an opportune time to update you on recent legal developments in this area. A number of these developments will affect Chadbourne and our clients in the financial, technology, health care and insurance industries, among others.

Health Net Lawsuit

On January 13, 2010, the Connecticut Attorney General sued Health Net of Connecticut, Inc. for alleged failure to secure patient medical records and financial information on a portable computer disk drive that was taken from a Health Net office most likely by thieves. The data was not encrypted or otherwise protected from viewing by unauthorized third parties, according to an investigative report. As a result, the suit alleges that Health Net failed to properly supervise, train and enforce policies and procedures required under applicable privacy and data security laws such as HIPAA and HITECH.

This case follows and builds on the **CVS Caremark** settlement reached by the Federal Trade Commission ("FTC") last January, 2009. As you will recall, in that case the FTC alleged that CVS failed to protect customer and employee information and CVS agreed to pay a \$2.5 million fine and be subject to auditing every two years *for the next 20 years*.

PricewaterhouseCoopers LLP Settlement

On January 28, 2010, the Alaska Attorney General reached a settlement with PricewaterhouseCoopers LLP ("PWC") regarding the alleged failure of PWC firm to protect information regarding 77,000 former and current public employees that allegedly was misplaced. PWC agreed to pay for identity theft protection and credit-monitoring for each of the 77,000 employees.

LifeLock Settlement

On March 9, 2010, the FTC announced a settlement with LifeLock, Inc. ("LifeLock") that requires the company to pay \$11 million to the FTC and \$1 million to 35 state attorneys general with regard to claims that LifeLock protected its customers from various forms of identity theft that the FTC alleged were false or misleading. This case, like the Health Net lawsuit, also involved a failure to encrypt private customer information. LifeLock expressly represented to customers that data collected by LifeLock would be encrypted while the FTC alleged that in fact LifeLock did not encrypt the data.

Massachusetts Data Breach Law Goes Into Effect

The much-publicized Massachusetts data breach law went into effect on March 1, 2010. The Massachusetts law contains a number of specific requirements detailing how companies that collect information concerning Massachusetts residents must protect that data. The law purports to cover data of Massachusetts residents no matter where it is collected or used, *i.e.*, Massachusetts purports to assert authority to apply its law to companies located in other states (or countries) so long as the data relates to a resident of Massachusetts.

FTC Safe Harbor Thrown Into Question

The Massachusetts law throws into question what might have been considered safe harbor practices under the FTC rules and cases on overseeing service providers. Many companies that collect data on their customers and employees outsource data storage and processing functions to a third party service provider. Under FTC rules, a company that collects data cannot escape its liability for privacy and data security breaches by outsourcing data storage and processing functions to a third party service providers. The FTC has promulgated and enforced a reasonableness standard governing the selection, contracting and monitoring of service providers that handle data collected by companies. To the extent that Massachusetts and other states adopt more specific and possibly conflicting requirements, the safe harbor of compliance with the FTC standards is thrown into question. Bills are pending before Congress that may broaden FTC authority but preemption of state laws poses thorny political issues that Congress may not tackle in an election year.

Insurance for Privacy and Data Protection Liability

Not surprisingly, given the much-publicized cases involving privacy and security breaches some of which are highlighted above, interest has increased in insurance for liability for privacy and data security breaches. General provisions in business insurance policies increasingly are regarded as potentially insufficient and customers are seeking more specific policy provisions. Insurance underwriters are evaluating the rapidly evolving legal landscape at both the federal and state level in order to define coverage and set premium and liability amounts. The insurance defense bar is welcoming into its ranks a new crop of litigators with expertise in the legal and technical aspects of privacy and data security breaches, damages and remedies.

For additional information on privacy and data security issues, please contact our Communications, Media and Technology group.

Our client alerts are for general informational purposes and should not be regarded as legal advice. If you would like additional information or have any questions, please contact:

Washington, DC

Dana Frix
+1 (202) 974-5691
dfrix@chadbourne.com

James A. Stenger
+1 (202) 974-5682
jstenger@chadbourne.com