

Privacy & Data Security

E-ALERT

September 30, 2008

States Enact New Privacy and Data Security Requirements

This memorandum provides an update on important data security and privacy-related requirements that will become effective on October 1, 2008, in Connecticut and Nevada, and on January 1, 2009, in Massachusetts. It also summarizes amendments to California's breach notice law that are awaiting final action. These developments could directly impact the manner in which entities transmit sensitive information, collect and use Social Security numbers ("SSNs"), and handle security breaches.

Connecticut SSN Policy Requirement

On October 1, Connecticut will begin requiring entities that collect SSNs in the course of business to create a privacy protection policy that protects the confidentiality of, prohibits the unlawful disclosure of, and limits access to SSNs. The policy must be published or publicly displayed, a requirement that is satisfied if the policy is posted on an Internet website.

The Connecticut law imposing these requirements on the use and disclosure of SSNs also includes separate requirements regarding the disposal of personal information. Specifically, the law requires "any person" in possession of "personal information of another person" to safeguard the media containing the information and destroy or render unreadable such media prior to disposal. The disposal law's definition of "personal information" is broader than that found in Connecticut's breach notification statute. It includes "information capable of being associated with a particular individual through one or more identifiers, including, but not limited to," a Social Security, driver's license, passport, or state identification number; account information; and an alien registration or health insurance identification number.

Violations of the Connecticut requirement are subject to a civil penalty of \$500 per incident, not to exceed \$500,000 for a single event. The requirements of the new law are in addition to and do not preempt those imposed by Conn. Gen. Stat. § 42-470, which prohibits persons from, *inter alia*, publicly displaying an individual's Social Security number or requiring an individual to transmit his or her Social Security number over the Internet unless the connection is secure or the number is encrypted.

Nevada Data Encryption Requirements

On October 1, Nevada will become the first state to require commercial businesses to encrypt customers' personal information before electronically transmitting it (other than by facsimile) outside their "secure system." Personal information is defined as a person's first name or initial and last name in combination with any of the following: (a) SSN, (b) driver's license or identification card number or (c) account number, credit card number, or debit card number, in combination with any required security code, access code, or

COVINGTON

COVINGTON & BURLING LLP

BEIJING

2301 Tower C Yintai Centre
2 Jianguomenwai Avenue
Chaoyang Dist., Beijing 100022
T: 86.10.5910.0591
F: 86.10.5910.0599

BRUSSELS

Kunstlaan 44 /
44 Avenue des Arts
1040 Brussels
T: 32.2.549.5230
F: 32.2.502.1598

LONDON

265 Strand
London WC2R 1BH
T: 44.(0)20.7067.2000
F: 44.(0).20.7067.2222

NEW YORK

The New York Times Building
620 Eighth Avenue
New York, NY 10018
T: 212.841.1000
F: 212.841.1010

SAN FRANCISCO

One Front Street
San Francisco, CA 94111
T: 415.591.6000
F: 415.591.6091

WASHINGTON

1201 Pennsylvania Avenue NW
Washington, DC 20004-2401
T: 202.662.6000
F: 202.662.6291

WWW.COV.COM

password that would permit access to the person's financial account. The law makes clear that permissible methods of encryption include cryptography, enciphering, encoding, or computer containment.

Notably, the law does not define "secure system." In addition, although the new provision applies only to businesses "in" Nevada, its effects will extend outside the state. The statute does not define what constitutes a "business in this state," but the Nevada Supreme Court has interpreted "doing business" in Nevada by evaluating the nature of a company's business and the quantity of business conducted by that company in the state. Furthermore, the Nevada legislature drafted the new data encryption requirement as part of S.B. 347, which established the state's data security breach notification laws. These breach notification laws, like those of 43 other states, apply to any company that owns or licenses personal information of state residents. Accordingly, businesses with customers in Nevada should comply with the encryption law, even if their headquarters or operational facilities are located elsewhere.

Massachusetts Data Security Requirements

On January 1, 2009, comprehensive Massachusetts data storage and protection rules will take effect. The new regulations, issued on September 22, 2008, by the Office of Consumer Affairs and Business Regulation, apply to private parties that own, license, store, or maintain personal information about Massachusetts residents. Much like the FTC Safeguards Rule, the Massachusetts regulations require businesses to develop and maintain a comprehensive written information security program consistent with industry standards and commensurate with the size, scope, and type of business. At a minimum, businesses must:

- encrypt personal information sent over the Internet or saved on laptops or other portable devices, and encrypt all wirelessly transmitted data;
- develop security policies for whether and how employees are allowed to access and transport records outside of business premises;
- use up-to-date firewall and anti-virus protections;
- train employees on security issues and permit only authorized users to access or transmit data;
- contractually bind service providers to protect personal information, and have the service providers certify in writing that they are in compliance with the Massachusetts data security regulations; and
- review the scope of their security measures at least once a year, or more often if there is a material change in business practices.

The rules define "personal information" to include first name or initial and last name in combination with any one or more of: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account. The definition of "encrypted" includes "the transformation of data through the use of an algorithmic process, or an alternative method at least as secure, into a form in which meaning cannot be assigned without the use of a confidential process key, unless further defined by regulation."

Massachusetts Governor Deval Patrick also signed an executive order requiring all state agencies to immediately take steps to implement security measures consistent with the requirements established under the new regulations for private companies.

California Data Security & Breach Notification Amendments

On August 31, the California legislature passed proposed amendments to the California data security and breach notice laws that would require any person, business, or government agency that sells goods or services to any resident of California and accepts credit or debit cards or other payment devices to implement certain safeguards modeled on the Payment Card Industry Data Security Standards ("PCIDSS"). Financial institutions subject to the requirements of the federal Gramm-Leach-Bliley Act would be exempt from these requirements.

Unlike a prior version of the bill that was vetoed by Governor Schwarzenegger last year, the California legislation does not require retailers to pay for the costs of replacing credit cards compromised by a data breach — a provision the retail industry strongly opposed. However, in a victory for the payment card and financial institution industry, the revised California bill passed last month would hold retailers and others who accept credit cards responsible for any costs incurred by the retailers or their service providers when notifying consumers regarding data breaches.

A.B. 1656 is linked to an amended breach notification measure (S.B. 364, which passed the Senate on August 30). Together, these bills would implement several content requirements and other modifications to the data breach notices required to be provided to California residents.

Under California law, the Governor has until the end of September to sign or veto A.B. 1656 and S.B. 364. If the Governor does not act by signing or vetoing the bills, they will become law automatically, with an effective date of January 1, 2009.

Finally, in addition to the bills addressing merchant responsibility for credit card breaches and imposing the new requirements on breach notifications to California residents, the California legislature passed two health care-related bills in the final days of its session. Together, the two bills (A.B. 211 and S.B. 541, which also await the Governor's action) would require health care providers to safeguard confidential patient data and give the state the authority to fine entities up to \$250,000 for violating the safeguard provisions.

If you have any questions concerning the material discussed in this client alert, please contact the following members of our privacy & data security practice group:

Erin Egan	202.662.5145	eegan@cov.com
David Fagan	202.662.5291	dfagan@cov.com
Brandon Almond	202.662.5677	balmund@cov.com
Josephine Liu	202.662.5270	jliu@cov.com

.....
This information is not intended as legal advice, which may often turn on specific facts. Readers should seek specific legal advice before acting with regard to the subjects mentioned herein.

Covington & Burling LLP is one of the world's preeminent law firms known for handling sensitive and important client matters. This alert is intended to bring breaking developments to our clients and other interested colleagues in areas of interest to them. Please send an email to unsubscribe@cov.com if you do not wish to receive future alerts.

© 2008 Covington & Burling LLP. All rights reserved.