SEYFARTH SHAW LLP
ATTORNEYS

One Minute Memo™

Seven More States Implement Data Breach Reporting Statutes

The costs and legal issues resulting from the loss of customer personal information continue to grow. Data security breaches can occur from criminal hacking or something as mundane as a lost laptop computer. According to a recent study of 31 companies that experienced a data breach, the cost from each event ranged from less than $1 million to more than $22 million, not including costs in terms of lost customers, public relations problems, lawsuits, and the like. Thus, data security is becoming a top priority for businesses and consumers. Indeed, the number of states enacting data security statutes continues to grow. On January 1, 2007, the following seven states joined twenty-seven other states in enacting data breach notification statutes: (i) Arizona; (ii) Hawaii; (iii) Kansas; (iv) Nebraska; (v) New Hampshire; (vi) Utah; and (vii) Vermont.

The main focus of enforcement by the states is currently in the area of notification of a data breach. Each state's laws governing data breach notification differ. Generally they impose the following restrictions:

- The statutes generally apply only to state residents or entities conducting business in the state; meaning that if you do business in more than one state, you will need to comply with multiple reporting requirements;
- "Personal Information" is usually defined to mean some combination of a person's name (*e.g.*, first initial and last name), in combination with some other identifying information such as a social security number, driver's license number, or credit/debit card information;
- The statutes often apply only if unencrypted information was lost and there is reason to believe that it was acquired by an unauthorized person or entity;
- When a breach is discovered, expedient notification to state residents is usually required; and
- Parties that maintain, but do not own personal information, must notify the owner of the information when a breach occurs, and it then falls on the data owner to inform customers and state authorities.

Some states explicitly provide for private enforcement actions (*e.g.*, New Hampshire), while others specifically limit enforcement to their Attorney General (*e.g.*, Arizona). Most statutes, however, do not address the availability private lawsuits. The Plaintiffs class action bar has already begun to file suits based on data breach notification laws.

States are also beginning to implement other requirements for protecting data and requiring the destruction of personal information. Likewise, the FTC continues to take an aggressive approach with respect to privacy and security breaches, and has expanded its taskforce dedicated to the enforcement of federal statutes such as the Gramm-Leach-Bliley Act (directed towards financial institutions), the Children's Online Privacy Protection Act, and general enforcement under §5 of the FTC Act.

Even in states that have not yet implemented a reporting statute, broader regularity authority is being used to address data security breaches. For example, in December 2006, based on authority to regulate the securities industry, the Massachusetts Secretary of State required one brokerage company to pay a substantial fine and hire an independent consultant to conduct a data security audit due to the theft of one laptop computer.

Even if a company complies with the myriad notification requirements of every state in which it is currently doing business, that company could still be held liable for not timely or improperly reporting a security breach. In this field, we have found that the best defense is a good offense; which means that a company should make certain it has an effective and proactive data security policy, and that employees should be trained on the policy as well as how to spot and report security breaches.

If you have questions or would like additional information, please contact the Seyfarth Shaw attorney with whom you work or any member of the Commercial Class Action Defense Group listed on our website www.seyfarth.com.