Mesmer & Deleault, PLLC
41 Brook Street, Manchester, NH 03104
Seacoast Office: One New Hampshire Ave., Suite 125
Portsmouth, NH 03801

Seasons Greetings

"Tip of the Month"

Data Governance in the Digital Age

Nowadays, data security breaches at businesses and major retail outlets seem common. Recently, Target and Home Depot were both hit by hackers within a year. Sensitive and personal identifying information may be compromised and exposed.

A complex array of state, federal, and international data security breach-specific laws and requirements have been employed to help combat the problem. Data breach notification requirements are now law in 47 of 50 states. These statutes require businesses and organizations to notify people whose personal information has been compromised. While most state notification statutes have similar elements, the requirements vary from state to state and sometimes even conflict. Therefore, businesses are advised to seek legal help to navigate the maze of state data breach notification laws and avoid potential liability down the road.

After discovering a breach, a business must first determine which state laws apply. While most companies are subject to the data breach notification statutes of each state in which their customers reside, organizations that conduct business globally may be required to comply with data breach notification laws of foreign countries.

The business must then determine whether the notification obligation has been triggered at all, and if so, in what states. Many states require notification when personal identifiable information is acquired or accessed by an unauthorized individual. Many state statutes use a common definition of "personal information." This consists of the consumer's name and at least one of the following pieces of information: Social Security Number, driver's license number or state identification card number, or financial information, such as credit or debit card numbers, account numbers, passwords, etc. Some states have expanded the definition to include such things as health insurance information and unique biometric data, such as fingerprints, retina scans, or iris images.

When a notification requirement is triggered, the business must then prepare a notification letter to the consumer. The letter must include and clearly describe: (1) the incident; (2) the type of personal information compromised; (3) the steps the company is taking to protect individuals against further data security breaches; (4) guidance as to how the affected individuals can protect themselves against identity theft in the future; and (5) a dedicated telephone number to answer questions about the data security breach.

To better understand your company's legal responsibilities with respect to data breach notification requirements, or for help in planning and implementing policy relating to data breach notification requirements, contact the attorneys at Mesmer & Deleault, PLLC by giving us a call at 603-668-1971 or contact us by email at *mailbox @ biz-patlaw.com*.

Happy Holidays!

Frank B. Mesmer, Jr.
Robert R. Deleault
Ross K. Krutsinger
Joshua N. Mesmer
Steven H. Slovenski – *of Counsel*
1214

(603) 668-1971
Fax (603) 622-1445
E-mail: mailbox@biz-patlaw.com
Website: www.biz-patlaw.com