Mendoza Law, LLC

1000 University Ave., W. Suite 222
Saint Paul, MN 55104
651-330-8062 (Main)
www.mendozalawoffice.com

Anthony S. Mendoza, Esq.
Direct Dial: 651-340-8884
tony@mendozalawoffice.com

A SUMMARY OF MINNESOTA'S DATA BREACH NOTIFICATION STATUTE

There is no federal or uniform law governing data breach notifications. Therefore, 48 states have separate data breach notification laws, with South Dakota and Alabama being the only states that do not. The Minnesota statute (Minn. Stat. section 325E.61) provides that a business or person that owns or licenses data that includes "personal information" must disclose a breach of the system holding that data to any person whose "unencrypted data" was or is "reasonably believed" to have been acquired by an unauthorized person. A breach of data not owned by the person or business breached must disclose the breach immediately after discovery to the owner of the data. If disclosure would impede a law enforcement investigation, the person or business experiencing the breach is allowed to delay notification at law enforcement's direction to a date certain as directed by law enforcement.

Minnesota's data breach notification law defines "personal information" as an individual's first name or first initial and last name, in combination with certain types of other information (such as a social security number or driver's license number) when the data element is not secured by encryption or if it was secured and the encryption key, password, or other means necessary for reading or using the data was also acquired." This so-called "safe harbor" provision effectively exempts a person or business from the disclosure requirement when the person or business handling the data has protected the data with encryption unless the encryption key was also compromised.

Notice of a data breach may be provided through: (i) written notice to the person whose data has been breached at their last known mailing address; (ii) electronic communication if electronic communication has been the primary method of communication with the person whose data was breached, or if the electronic communication is made in compliance with the federal Electronic Signatures in Global and National Commerce Act; (ii) substitute notice if the cost of providing notice under one of the other two methods would cost more than $250,000, or the number of people to be notified exceeds 500,000, or the business does not have sufficient contact information. Substitute notice must include all of the following: (i) email notice if the person affected has an email address; (ii) conspicuous posting on

the web site of the company experiencing the breach; and (iii) notification to major statewide media.

If a firm has its own data breach notification procedures in an information security policy and otherwise complies with the timing requirements set forth in the Minnesota notification statute, the firm or business is deemed to be in compliance with the Minnesota statute if that policy is followed. Also, "financial institutions" are subject to a different data breach notification statute (Minn. Stat. §325E.64).

If the person or business breached discovers that more than 500 people must be notified of the breach, the person or business affected must notify all nationwide credit reporting agencies of the breach.

The Minnesota Attorney General is solely responsible for enforcement of Minnesota data breach notification statute. In 2014, a Minnesota federal district court ruled that there is no private cause of action for non-compliance with Minnesota's data breach notification law because the statute provides exclusive enforcement authority to the Minnesota Attorney General.