To Disclose or Not to Disclose: A Primer on Data Breach Notification Rules

Aaron P. Minster
612-877-5263 | Aaron.Minster@lawmoss.com
LawMoss.com/people-aaron-p-minster

Aaron is a member of Moss & Barnett's Litigation group. He has experience with ligation involving shareholder derivative actions, real estate, employment, trade secrets, malpractice actions, and construction disputes.

When hackers breach a company's network, disclosure of the breach is generally required by law. But did you know that something as innocuous as an employee's missing cell phone, tablet, or laptop might also constitute a "data breach" and trigger related notification laws? In fact, according to Verizon's 2022 Data Breaches Investigations Report, 82% of data breaches involved human error.

Defining "Data Breach"

Minnesota law requires a business to disclose "any breach of the security of the system" once discovered. A "breach of the security of the system" means an "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business." Because the statutory definition of a "breach" is extremely broad, seemingly innocuous events may require a business to provide notice of a data breach. Consider the following examples:

- An employee loses an iPhone, and the iPhone had access to personal information maintained by the business.
- An employee accidentally copies an individual, who does not work for the business, on an email containing personal or confidential information.
- An employee falls victim to a phishing scam and unknowingly provides a hacker with company credentials and access to databases with personal or confidential information.

When Providing Notice of the Breach Is Required

Minnesota's data breach notification law is triggered as soon as it is reasonable to believe that personal information has been "acquired" by a third party. Minnesota's definition of "personal information" includes first and last names or a first initial and last name, in combination with one of the following: a Social Security number; a driver's license number; a Minnesota identification card number; or an account, credit, or debit card number, in combination with any access or security information. Wisconsin's data breach notification law has similar rules. North Dakota's law expands the definition of "personal information" to include date of birth and health insurance numbers, among other information.

Data breach notification rules for organizations working within federally regulated industries, like health care and banking, are generally governed by federal privacy laws and regulations. Public entities and educational institutions also have their own data breach notification rules.

Form and Timing of Notice

Under Minnesota law, notification must be provided by mail to the most recent available address of the person or business affected, or by electronic notice (if electronic communication is the organization's primary method of communication with that individual). Under certain circumstances, substitute notice with notification on statewide media is permitted. Most data breach laws also require that notification be given to government agencies and law enforcement authorities.

In Minnesota, notice must be provided to affected individuals "in the most expedient time possible" unless law enforcement directs otherwise. Similarly, South Dakota's law requires disclosure within 60 days of discovery unless there is a legitimate law enforcement reason to delay disclosure.

Exceptions to the Rules

So, what of the employee's lost iPhone and other seemingly innocuous data breaches? There are exceptions to data breach notification laws for information that is protected by encryption and secured with an appropriate password or PIN.

"To Disclose or Not to Disclose:" Continued on Page 7

"To Disclose or Not to Disclose" Continued from Page 2

Consider company policies that require strong encryption, passwords, and remote erase technologies on all employee devices, including employee-owned devices that have access to company data. If lost devices are secured and can be remotely erased, then there is no reasonable likelihood that personal information on that device will have been "acquired" and data breach notification rules are likely not triggered.

Conclusion

Laws involving data breach notification are complicated. Obtaining legal advice early on is key to implement prevention policies and navigate a data breach. This article is not intended to provide a comprehensive survey of data breach notification rules, which vary across states and industries. If your employee's iPhone goes missing or you want to review your company's data privacy policies, please contact your Moss & Barnett attorney.