THOMPSON HINE

Privacy & Cybersecurity Update

July 2024

Pennsylvania Amends Data Breach Reporting Law; Requires Credit Monitoring for Victims

On June 28, Pennsylvania Governor Josh Shapiro signed into law Senate Bill (SB) 824, which amended the state's personal data breach notification statute, commonly known as the Breach of Personal Information Notification Act (PA Notification Act). In particular, SB 824 amends the term "personal information," requires organizations to notify government authorities of certain types of data breaches and mandates that organizations (under certain conditions) provide credit monitoring services to individuals whose personal information was compromised during a data breach. The law goes into effect on September 26, 2024. Organizations impacted by the law should update their data breach response plans to account for new notification requirements and assess whether their cyber insurance policies cover new credit monitoring services obligations.

Background: State and Private Sector Breach Reporting Obligations

Like most data breach notification laws, the PA Notification Act requires organizations that maintain "computerized data that includes personal information" to provide notice of a data breach wherein an individual's "unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person." This notice must "be made without unreasonable delay."

The law also provides that if a Pennsylvania state agency determines that it is the subject of a data breach affecting personal information **"maintained by the State agency or State agency contractor,"** then it must provide notice of the breach to affected persons within 7 business days following determination of the breach. The Pennsylvania state agency must also concurrently provide notification of the breach to the Pennsylvania Office of Attorney General.

The PA Notification Act further provides that a "vendor that maintains, stores or manages computerized data on behalf of another entity shall provide notice of any breach of the security of the system following discovery by the vendor to the entity on whose behalf the vendor maintains, stores or manages the data." In turn, it is the private sector entity or state agency that maintains the personal information that is "responsible for making the determinations and discharging [its] remaining duties" with respect to facilitating its data breach notification obligations under the law.

SB 824 Narrows a Key Term

An important aspect of the PA Notification Act is that private sector entities and state agencies are only required to notify individuals of a data breach when certain types of personal information have been compromised. SB 824 narrows the definition of what constitutes personal information. Previously, the term "personal information" was defined as an individual's name, in connection with any of the following identifiable (i.e., non-encrypted) data elements:

- Social Security number.
- Driver's license number or a state identification card number issued in lieu of a driver's license.
- Financial account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

- Medical information (but see changes below).
- Health insurance information.
- A username or e-mail address, in combination with a password or security question and answer that would permit access to an online account.

Importantly, SB 824 amends the definition of "personal information" to add a qualifier to "medical information" so the phrase is now "[m]edical information **in the possession of a State agency or State agency contractor,**" which is similar to the terminology used in other parts of the law where defining the reporting obligations for state agencies and their contractors (see above). SB 824 did not change the definition of "medical information," which the PA Notification Act defines as "[a]ny individually identifiable information contained in the individual's current or historical record of medical history or medical treatment or diagnosis created by a health care professional."

According to the Fiscal Notes by the PA Senate Appropriations Committee (PA Senate Fiscal Notes), SB 824 amends the definition of "personal information" to "specifically *include* medical information in the possession of a state agency or state agency contractor." However, with the specific changes mandated by SB 824, it appears that now *only* a state agency or state agency contractor (and not a private sector entity) is required to notify individuals of a data breach impacting medical information. It is unclear whether the intent of SB 824 was to *exclude* private sector entities from having to inform individuals of a data breach that impacts medical information, and this ambiguity appears to be a consequence of the amendment.

Consumer Reporting Agency and Regulatory Notifications

As previously written, the PA Notification Act only required private sector entities to provide notice of a data breach affected individuals, and in some instances, to consumer reporting agencies. SB 824 now requires organizations impacted by a data breach to furnish notice to the PA Attorney General.

First, with respect to consumer reporting agencies, the PA Notification Act previously required organizations to furnish (without reasonable delay) notice of a data breach to consumer reporting agencies when more than 1,000 individuals were affected by the breach at one time. SB 824 changed this notification threshold from 1,000 individuals to 500 individuals affected by a data breach at one time. This notice to consumer reporting agencies must address the timing, distribution and number of data breach notices delivered to affected individuals.

Next, SB 824 mandates that when a private sector organization provides notice of a data breach to more than 500 affected Pennsylvania residents, then it must also "concurrently" furnish notice of the same to the Office of Attorney General. This notice to the PA Attorney General must include the following information, to the extent known by the notifying organization:

- The organization's name and location.
- The date of the breach.
- A summary of the breach incident.
- An estimated total number of individuals affected by the breach.
- An estimated total number of individuals in Pennsylvania affected by the breach.

This regulatory reporting requirement, however, does not apply to an entity subject to Pennsylvania law regulating data security requirements for certain types of insurance-related companies. Organizations should update their data breach response plans to justify these new consumer agency and regulatory reporting requirements.

Credit Reporting and Monitoring Services

For organizations that are required to provide notice of a data breach to consumer reporting agencies under the law (see above), and the notice concerns a confidentiality breach of a person's Social Security number, bank account number, driver's license number, or state identification number, they are now required to incur additional obligations. More specifically, SB 824 provides that these entities must "assume all costs and fees" with respect to providing the affected individuals with the following:

- Access to one independent credit report from a consumer reporting agency if the individual is not eligible to obtain an independent credit report from a

consumer reporting agency for free under 15 U.S.C. § 1681.
- Access to credit monitoring services for 12 months following notification. An entity may satisfy this requirement by providing notice to the individual of the availability of monitoring services for 12 months at no cost to the individual.

According to the PA Senate Fiscal Notes, the "[r]etail prices for credit monitoring services can range between $8.99 per month to $39.95 per month" and "[a]ssuming a breach of 500 individuals, the incurred costs for monitoring services range from $54,000 to $240,000 annually." According to PA Senate Fiscal Notes, this cost would be paid by the organization that was responsible for the data breach and "would likely be accommodated within existing budgeted amounts." It will be important for organizations to ensure their cyber insurance coverage addresses credit monitoring services.

FOR MORE INFORMATION

For more information, please contact:

Steven G. Stransky
216.566.5646
202.263.4126
Steve.Stransky@ThompsonHine.com
Certified Information Privacy Professional/Government (CIPP/G)
Certified Information Privacy Professional/United States (CIPP/US)

Thomas F. Zych
216.566.5605
Tom.Zych@ThompsonHine.com

Marla M. Izbicky
312.998.4253
Marla.Izbicky@ThompsonHine.com
Certified Information Privacy Professional/United States (CIPP/US)

Thora Knight, Ph.D.
212.908.3971
Thora.Knight@ThompsonHine.com