THOMPSON HINE

Privacy & Cybersecurity Update

January 2025

New York Data Breach Law Amended: New Timelines and Expanded Regulatory Reporting

On December 21, 2024, a new amendment (Senate Bill S2659A) to the New York State Data Breach Notification Law came into force. The amendment establishes specific timelines that dictate when organizations must complete data breach notification, removes notification timeline exceptions that were favorable to businesses, and expands regulatory reporting obligations. Organizations should update their data security incident response plans to account for these changes.

Scope of the New York State Data Breach Notification Law

The data breach notification law contains multiple definitions that are key to understanding its scope of applicability. Specifically, the law regulates when an organization is required to report a "breach of the security of the system," which is defined, in relevant part, as the "unauthorized access to or acquisition of, or access to or acquisition without valid authorization, of computerized data that compromises the security, confidentiality, or integrity of private information maintained by a business."

The term "private information" essentially has two parts and includes another term: "personal information." The phrase "personal information" is broadly defined as "any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person." In turn, the term "private information" means personal information that consists of any information in combination with any one or more of the following data elements when either the data element or the combination of personal information plus the data element is not encrypted or is encrypted with an encryption key that has also been accessed or acquired:

- social security number;
- driver's license number or non-driver identification card number;
- account number, credit, or debit card number, in combination with any required security code, access code, password, or other information that would permit access to an individual's financial account;
- account number, credit, or debit card number, if circumstances exist wherein such number could be used to access an individual's financial account without additional identifying information, security;
- code, access code, or password; or
- biometric information, meaning data generated by electronic measurements of an individual's unique physical characteristics, such as a fingerprint, voice print, retina or iris image, or other unique physical representation or digital representation of biometric data used to authenticate or ascertain the individual's identity.

Separately, the term "private information" also includes "a user name or e-mail address in combination with a password or security question and answer that would permit access to an online account." However, the term categorically excludes "publicly available information which is lawfully made available to the general public from federal, state, or local government records."

New 30-Day Data Breach Timeline for Businesses and Service Providers

The existing New York Data Breach Notification Law requires any person or business that "owns or licenses

computerized data which includes private information" to disclose a security breach of this private information to each affected New York resident, subject to certain "good faith" exceptions and "harm" applicability thresholds. The recently enacted amendment mandates that disclosures be made as expediently as possible, without unreasonable delay, and within thirty (30) days of discovering the breach unless a "law enforcement" exception applies.

Unlike other U.S. states, the New York State Data Breach Notification Law did not previously include this 30-day timeframe, and it only required data breach notifications to be made in the most expedient time possible and without unreasonable delay. The amendment originally envisioned a fifteen (15) day notification timeline but ultimately changed to thirty (30) days during the legislative process.

Importantly, the data breach law previously allowed organizations to delay data breach reporting consistent with an organization's measures necessary to determine the scope of the breach and restore the integrity of the system; however, the law removed this framework and no longer provides an excuse for businesses to delay its data breach notification obligations.

New York's existing data breach notification law requires any person or business that "maintains computerized data which includes private information" on behalf of a third party to notify the owner or licensee of the information of any security breach immediately and in any event within thirty (30) days following the discovery of the breach. The law previously did not include this 30-day timeframe.

Expanded Regulatory Reporting

Many U.S. state data breach notification laws commonly require organizations to notify affected residents and state regulatory agencies directly about data breaches. Previously, the New York State Data Breach Notification Law required organizations that suffered reportable data breaches to notify the state attorney general, the Department of State, and the division of state police of "the timing, content, and distribution of the notices and approximate number of affected persons" notified of the breach. The new amendment to New York State's data breach notification now requires organizations to disclose the incident to the department of financial services, in addition to these other New York State agencies.

The law requires this notification to New York State agencies to include "a copy of the template of the notice sent to affected persons" and expressly states that this regulatory notice "shall be made without delaying notice to affected New York residents." This framework remains unaltered, and organizations can access the New York Department of State website for more information.

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

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