VORYS

Publications

Client Alert: The State of Washington Expands Breach Notification Requirements

Related Professionals

John L. Landolfi

Christopher L. Ingram

Related Services

Data Strategy, Privacy and Security

CLIENT ALERT | 5.15.2019

Governor Jay Inslee recently signed Substitute House Bill 1071, amending Washington's data breach notification law. In relevant part, the amendment expands the definition of personal information, shortens the timeframe for reporting a breach to Washington regulators, and expands the information that must be provided to individuals impacted by the incident.

In addition to requiring entities to notify individuals whose names in combination with their Social Security Numbers, driver's license numbers, state identification card numbers or financial account information were compromised, the amendment also requires notification if the individuals' names are compromised along with their:

- Full date of birth;
- Health insurance policy number or health insurance identification number;
- Student, military, or passport identification number;
- Medical history information;
- Biometric data (such as fingerprints); or
- Private key that is unique to the individual and that is used to authenticate or sign an electronic record.

The amendment also requires that individuals be notified if their "username or email address in combination with a password or security questions and answers that would permit access to an online account" is compromised, regardless of whether their name was involved. If the personal information was not encrypted or redacted, or if the compromised personal information would enable a person to commit identity theft, any of these data elements or combination of these data elements without the individuals' names requires notification to affected individuals.

The amendment also shortens the time period organizations are required to notify Washington's Attorney General of a data breach. Under the amendment, entities that have experienced a data breach involving the personal information of more than 500 Washington residents are now required to report the breach to the Washington Attorney General within thirty days of discovering the breach.

The amendment also prescribes new content that must be included in breach notifications to Washington residents affected by the compromise and to the Washington Attorney General. Regarding notice to Washington residents, the notice must now also specify, among other things, the:

- Timeframe of the personal information's exposure;
- Date the incident was discovered; and
- Date the breach commenced.

Notifications to the Washington Attorney General, must now also include the information provided to Washington residents as well as:

- the number of Washington residents reasonably believed to be affected by the incident;
- a summary of steps taken to contain the incident; and
- a sample copy of the consumer notification excluding any personally identifiable information.

Finally, the amendment requires companies to update the attorney general with any of the required information to the extent that information was unknown at the time the notice was due.

Companies should update their incident response plans to incorporate these changes. For assistance with compliance questions, policy review, or incident response preparation, please contact John Landolfi, Christopher Ingram, Sarah Boudouris your Vorys attorney.