Oregon, New York, Alabama, and Rhode Island Join List of States Considering Data Breach Legislation Post-Equifax

By David M. Stauss, Gregory Szewczyk, and J. Matthew Thornton*

The authors of this article discuss proposed data breach legislation in Oregon, New York, Alabama, and Rhode Island.

Any entity that does business in these states or maintains confidential information of their residents should monitor the proposed data breach legislation discussed below: Oregon, New York, Alabama, and Rhode Island.

OREGON

Oregon's proposed legislation, Senate Bill 1551,[1] makes several notable amendments to the state's existing data breach statute, O.R.S. §§ 646A.602 to 622. For starters, the proposal would expand the existing scope of coverage, requiring not only that owners and licensees of personal information provide notice in the event of a security breach, but also anyone who "otherwise possesses" such information for use in the course of their business, vocation, occupation, or volunteer activities, as well as those who receive notice of a breach from "another person that maintains or otherwise possesses personal information on the person's behalf."

The proposed legislation also imposes new requirements governing when notice must be sent and to whom. Under the bill, notice must be given to consumers "in the most expeditious manner possible, without unreasonable delay, but not later than 45 days after discovering or receiving notification of the breach." A copy of the notice must also be sent to the state attorney general.

Also of note in Senate Bill 1551 are restrictions imposed on provision of credit monitoring services or identity theft prevention and mitigation services. For example, the bill prohibits a person from offering to provide these services to affected consumers

* David M. Stauss is a partner at Ballard Spahr LLP and head of the Denver office's Privacy and Cybersecurity Practice Group. Gregory Szewczyk is an associate at the firm handling corporate and commercial litigation, as well as privacy and cybersecurity matters. J. Matthew Thornton is an associate in the firm's Litigation Group focusing his practice on individual actions and class action defense, as well as privacy and cybersecurity matters. The authors may be reached at staussd@ballardspahr.com, szewczykg@ballardspahr.com, and thorntonj@ballardspahr.com, respectively.

[1] https://olis.leg.state.or.us/liz/2018R1/Measures/Overview/SB1551. The legislation discussed herein is subject to change based on the legislative process. The reader should consult with each state's legislative website to determine the current status of each bill.

free of charge if the offer is conditioned on the consumer providing a credit or debit card number or accepting other services for a fee.

NEW YORK

New York's proposed legislation is Senate bill S6933A.[2] The bill was proposed in November 2017 and referred to Rules and Consumer Protection Committees. It was then reported to the Finance Committee.

The legislation would make several important changes to existing law, including by expanding the definition of "private information," the unauthorized access to or acquisition of which triggers notification obligations. Specifically, the bill adds the following categories to private information when in combination with "personal information" that allows the individual to be identified: credit or debit card numbers if circumstances exist where such number could be used to access a financial account without additional information, code, or password; and biometric information.

The bill also adds the following to "private information" regardless of whether "personal information" is also disclosed: user name or email address in combination with a password or security question and answer that would permit access to an online account; and any unsecured information protected under HIPAA.

The bill would also require covered entities to "develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the private information." The bill provides that a covered entity shall be deemed in compliance if it implements a program that includes:

- administrative safeguards (including designating a responsible employee, identifying reasonably foreseeable risks, assessing the sufficiency of safeguards, training employees, selecting third-party service providers that maintain reasonable security measures, and adjusting the program based on new information);
- technical safeguards (including risk assessments and regularly monitoring effectiveness); and
- physical safeguards (including risk assessments of storage and disposal procedures, protecting against unauthorized access during the collection, transportation, and disposal of information, and reasonable disposal procedures).

The bill would apply a separate standard for defined small businesses based on their size and complexity, and deem entities regulated by state or federal rules to be in compliance if they comply with pertinent requirements of the applicable regulator.

The proposed legislation would also extend the statute of limitations for attorney general enforcement actions from two years to three. It would also change the accrual

[2] http://nyassembly.gov/leg/?default_fld=&leg_video=&bn=S06933&term=2017&Summary=Y&Text=Y.

date for actions—previously, actions accrued on the date of the act complained of or the date of discovery of that act. Under the bill, actions would accrue after either the date on which the attorney general became aware of the violation or the date the entity sent notice to the attorney general. Finally, the bill would raise the maximum fine for reckless or knowing violations from $10 per instance of failed notification, with a cap of $150,000, to $20 per instance, with a cap of $250,000.

ALABAMA

Alabama's senate bill, SB318,[3] would require covered entities to notify individuals within 45 days if their unencrypted "sensitive personally identifying information" is compromised. The bill defines sensitive personally identifying information broadly to include:

- Social Security numbers;
- driver's license numbers;
- state-issued identification numbers;
- password numbers;
- military identify numbers;
- financial account numbers;
- some medical or health information; and
- a user name or email address in combination with the required password or security question.

The bill also would create an extensive information security structure whereby covered entities and third-party agents would be required to implement and maintain reasonable security measures to protect sensitive personally identifying information. Those measures include:

- designating a responsible individual;
- performing a risk assessment;
- adopting appropriate information safeguards;
- requiring third-party service providers to maintain appropriate safeguards, evaluating and adjusting those measures as necessary; and
- keeping company management informed of the measures.

Finally, the bill provides for various penalties for noncompliance, including a civil penalty of not more than $5,000 "per day for each consecutive day that the covered entity fails to take reasonable action to comply with" the notice provisions.

[3] http://alisondb.legislature.state.al.us/ALISON/SearchableInstruments/2018RS/PrintFiles/SB318-eng.pdf.

RHODE ISLAND

Rhode Island's proposed legislation is House Bill 7387.[4]

By way of background, in 2015, Rhode Island enacted the Rhode Island Identity Theft Protection Act,[5] which requires covered entities to implement and maintain a risk-based information security program and to notify individuals if their personal information is compromised.

The proposed legislation does not reference Rhode Island's existing law but instead seeks to enact a separate statutory requirement for breach notifications. According to reports of interviews given by the bill's sponsor, the intent is to create notification requirements for large-scale data breaches, such as Equifax's. However, it is unclear how the proposed legislation is intended to interact with existing law and whether a breach situation could implicate both laws.

The proposed law conflicts with existing law in many important respects. Existing law has a broader definition of personal information, requires notification in 45 days, provides that entities must notify the state attorney general if more than 500 state residents are to be notified, and specifies what type of information must be provided in the notification. On the other hand, the proposed legislation would go further than existing state law by authorizing the attorney general to seek a civil penalty of up to $150,000 for each security breach.

[4] http://webserver.rilin.state.ri.us/BillText/BillText18/HouseText18/H7387.pdf.
[5] R.I. Stat. § 11-49.3-1 to -6.