

THE OREGON LEGISLATURE STRENGTHENS DATA BREACH LAWS, ADDING TOUGHER NOTIFICATION AND SAFEGUARDING REQUIREMENTS

Date: 29 May 2018

U.S. Cyber Law and Cybersecurity / Privacy, Data Protection and Information Management Alert

By: Samuel Hernandez, John C. Rothermich

In response to widely reported data breaches affecting millions of consumers, the Oregon Legislature recently took steps in Senate Bill ("SB") 1551 to strengthen Oregon's consumer data protection laws by expanding breach notification and data safeguarding requirements. The amendments will take effect on June 2, 2018.

THE CURRENT STATUTE

The Oregon Consumer Identify Theft Protection Act (ORS 646A.600–646A.628) already requires "persons" that own or license "personal information" to provide notice of a data breach in the most expeditious manner possible, without unreasonable delay. The statute defines (1) "consumer" to mean an individual resident of this state; (2) "person" to mean an individual, private or public corporation, partnership, cooperative, association, estate, limited liability company, organization, or other entity; and (3) "personal information" to mean a consumer's first name or first initial and last name in combination with the consumer's social security number, drivers license number, passport number, financial account number, data from automatic measurements of a consumer's physical characteristics, insurance policy number, and medical history. The statute protects personal information of both customers and employees.

AMENDMENT TO NOTIFICATION DUTIES AND DEADLINES

The amendment expanded the definition of "person" to individuals or entities that own, license, or otherwise possess personal information. The duty to notify is also now triggered where the person receives a report of a breach from another person that maintains or otherwise possesses personal information on the person's behalf, such as payroll service providers. The amendment also broadens the definition of "personal information" to include "any other information or combination of information that a person reasonably knows or should know would permit access to the consumer's financial account[.]"

In addition to requiring notification "in the most expeditious manner possible, without unreasonable delay[.]" the amendment now adds that such notice must be made no later than 45 days after discovering or receiving notification of the breach of security. The statute continues to require notice to the individual to whom the personal information pertains and to the attorney general in cases where the breach affects more than 250 individuals.

The amendment also provides that if a person offers credit-monitoring services or identity-theft prevention and mitigation services without charge to the consumer, the person may not condition such services on receiving

credit or debit card information from the affected consumer or the consumer's acceptance of a service provided by the person for a fee.

AMENDMENT TO INFORMATION SAFEGUARDING REQUIREMENTS

The amendment added additional requirements to ORS 646A.622, dealing with safeguarding and protecting personal information. The notable changes provide that a person complies with safeguarding requirements where the person implements a security program that includes, among other things:

- Identifying reasonably foreseeable internal and external risks *with reasonable regularity*;
- Training and managing employees in security program practices and procedures *with reasonable regularity*;
- *Reviewing user access privileges with reasonable regularity*; and
- *Applying security updates and a reasonable security patch management program to software that might reasonably be at risk of or vulnerable to a breach of security.*

(changes in italics).

Given the renewed emphasis on safeguarding personal information, organizations of all sizes should take this time to evaluate their security programs and make changes where necessary.

This publication/newsletter is for informational purposes and does not contain or convey legal advice. The information herein should not be used or relied upon in regard to any particular facts or circumstances without first consulting a lawyer. Any views expressed herein are those of the author(s) and not necessarily those of the law firm's clients.