U.S. State Privacy Profiles

OREGON

David J. Oberly of Blank Rome LLP, Cincinnati, provided expert review of the Oregon Profile and wrote the Risk Environment section

I. APPLICABLE LAWS AND REGULATIONS

I.A. **Constitutional Provisions** —

There are no constitutional provisions in Oregon conferring a general right of privacy on Oregon residents.

I.B. **Personal Data Protection Provisions** —

The primary privacy and data security law in Oregon is the Oregon Consumer Identity Theft Protection Act (CITPA; Or. Rev. Stat. §§ 646A.600 et seq.). This law governs data breach notification requirements (see Section I.C.80.), security freezes (see Section I.D.40.), prohibitions on the printing or display of social security numbers (see Section I.D.100.), and data security and disposal requirements (see Section I.C.60. and Section I.C.70.). Each of these is outlined in brief below and discussed in detail at the cited Sections of this profile.

There are additional privacy laws in Oregon, including laws governing eavesdropping and electronic surveillance (see Section I.F.), do-not-call laws (see Section I.E.10.), and employment law provisions (see Section I.E.60.). Finally, laws related to privacy and data security applicable to specific sectors, such as health care and insurance, are set forth in the portions of this profile dedicated to those sectors.

I.B.10. **Who is covered?** —

The provisions of the CITPA cover “consumers,” defined as individual residents of Oregon (Or. Rev. Stat. § 646A.602(2)). Provisions specifically governing security freezes also cover “protected consumers,” who are individuals who are younger than age 16 at the time that a security freeze is requested on their behalf by a representative, or who are incapacitated or have had a guardian or conservator appointed by a court (Or. Rev. Stat. § 646A.602(13)).

I.B.20. **What is covered?** —

Under the CITPA, a person that owns or licenses personal information that is subject to a breach of security must give notice of the breach to specified persons (Or. Rev. Stat. § 646A.604(1)). For specific information on data breach notification requirements, see Section I.C.80.

The CITPA also provides that consumers and protected consumers may request a credit reporting agency (CRA) to place a security freeze on their security reports under statutorily specified provisions (Or. Rev. Stat. §§ 646A.606 et seq.). For a comprehensive discussion of the security freeze laws, see Section I.D.40.

The CITPA prohibits persons from printing, displaying, or posting social security numbers of consumers under specified circumstances; see Section I.D.100. for details.

Finally, under the CITPA, persons owning, maintaining, or otherwise possessing data including a consumer's personal information must develop, implement, and maintain reasonable security safeguards. For a complete discussion of these requirements, see Section I.C.60.

I.B.30. **Who must comply?** —

The provisions of the CITPA covering data breach notifications, the display of social security numbers, and data security requirements apply to “persons,” defined as individuals, private or public corporations, partnerships, cooperative associations, estates, limited liability companies, organizations, or other entities, whether or not organized for profit, or public bodies as defined by Oregon law (including state government bodies, local government bodies, and special government bodies) (Or. Rev. Stat. § 646A.602(10)). The CITPA provisions on security freezes require the compliance of “consumer reporting agencies” as defined by federal law (Or. Rev. Stat. § 646A.602(4)).

I.C. **Data Management Provisions**

I.C.10. **Notice & Consent** —

Consumer Identity Theft Protection Act: For information on notice requirements contained in the Oregon Consumer Identity Theft Protection Act (CITPA), in particular data breach notification requirements, see Section I.C.80.

Education provisions: Under Oregon education law, certain student records may not be disclosed by educational institutions without prior consent of an eligible student. Similar requirements apply to post-secondary educational institutions. For a comprehensive discussion of these requirements, see Section I.E.20.

I.C.20. **Collection & Use** —

Educational cloud computing service providers: Specific requirements apply to the use of data by cloud computing service providers furnishing services to K-12 educational institutions (see Section I.E.20.).

Insurance and health provisions: Oregon insurance laws and regulations governing the privacy of nonpublic personal financial information of consumers maintained by insurers in Oregon contain specific collection and use provisions (see Section I.E.70.). In addition, provisions of Oregon law governing specific types of health care facilities and providers and health data contain requirements regarding collection and use of such data (see Section I.E.50.).

I.C.30. **Disclosure to Third Parties** —

Education provisions: Oregon education law governs disclosures of student record information by educational institutions (see Section I.E.20.).

Insurance and health provisions: Oregon insurance laws and regulations governing the privacy of nonpublic personal financial information of consumers maintained by insurers in Oregon contain specific requirements regarding disclosures to third parties (see Section I.E.70.). In addition, provisions of Oregon law governing specific types of health care facilities and providers and health data contain requirements regarding third-party disclosures (see Section I.E.50.).

Security freezes: For information on disclosure restrictions applicable to credit report information subject to a security freeze, see Section I.D.40.

I.C.40. **Data Storage** —

Our research has revealed no specific Oregon law provisions governing privacy with respect to data storage.

I.C.50. **Access & Correction** —

Educational records: Oregon education law has specific provisions regarding access to, and correction of, public school education records (see Section I.E.20.).

Insurance and health provisions: Oregon insurance laws and regulations governing the privacy of nonpublic personal financial information of consumers maintained by insurers in Oregon contain specific requirements regarding access to, and correction of, such records (see Section I.E.70.). In addition, provisions of Oregon law governing specific types of health care facilities and providers and health data contain requirements regarding access and correction (see Section I.E.50.).

I.C.60. **Data Security** —

Provisions governing businesses: Provisions of the Oregon Consumer Identity Theft Protection Act (CITPA) require any person who owns, maintains, or otherwise possesses, or had control over or access to, data that includes a consumer's personal information that the person uses in the regular course of business, vocation, occupation, or volunteer activities to develop, implement, and maintain reasonable safeguards to protect the security, confidentiality, and integrity of the personal information, including safeguards ensuring protection of such information when it is disposed (Or. Rev. Stat. § 646A.622(1)).

For purposes of this provision, a “person” is an individual, private or public corporation, partnership, cooperative association, estate, limited liability company, organization, or other entity, whether or not organized for profit, or a public body as defined by Oregon law (including state government bodies, local government bodies, and special government bodies) (Or. Rev. Stat. § 646A.602(10)). A “consumer” is an individual resident of Oregon (Or. Rev. Stat. § 646A.602(2)). Finally, “personal information” is defined as a consumer's first name or first initial and last name in combination with any of the following data elements, if encryption, redaction, or other methods have not rendered the elements unusable or if the data elements are encrypted but the encryption key has been acquired:

- consumer's social security number;
- consumer's driver's license number or state ID card number;
- consumer's passport number or other ID number issued by the U.S.;
- consumer's financial account number, credit card number, or debit card number, in combination with any required security code, access code, or password that would permit access to the consumer's financial accounts, or any other information or combination of information that a person reasonably knows or should know would permit such access;
- data from automatic measurements of a consumer's physical characteristics, such as images of a fingerprint, retina, or iris, that are used to authenticate a consumer's identity in the course of a financial or other transaction;
- consumer's health insurance policy number or subscriber ID number in combination with any other unique identifier used by an insurer to identify the consumer; or
- information about a consumer's medical history or mental or physical condition or about a health care professional's medical diagnosis or treatment of the consumer (Or. Rev. Stat. § 646A.602(11)(a)).

Each of the above data elements, alone or in combination, also qualifies as “personal information,” even when not in combination with a consumer's first name or first initial and last name, if encryption, redaction, or other methods have not rendered the data element unusable, and the data element or combination of data elements would enable a person to commit identity fraud against a consumer (Or. Rev. Stat. § 646A.602(11)(b)). “Personal information” does not include information in federal, state, or local government records, other than a social security number, that is lawfully made available to the public (Or. Rev. Stat. § 646A.602(11)(c)).

A person will be deemed to be in compliance with the law's data security requirements if the person complies with a state or federal law that provides greater protection to personal information than that provided under the CITPA; if the person complies with regulations under the federal Gramm-Leach-Bliley Act or the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, to the extent that the person is subject to such provisions; or if the person implements an information security program that contains administrative safeguards, technical safeguards, and physical safeguards as specified by law (Or. Rev. Stat. § 646A.622(2)). The law allows persons to contract with other persons to carry out data disposal requirements under specified conditions (Or. Rev. Stat. § 646A.622(3); see Section I.C.70.).

A person that is an owner of a small business as defined by state law is in compliance with data security requirements if the person's information security and disposal program contains administrative, technical, and physical safeguards and disposal measures that are appropriate for the size and complexity of the small business, the nature and scope of the small business's activities, and the sensitivity of the underlying personal information (Or. Rev. Stat. § 646A.622(4)).

Persons who violate the provisions of the CITPA regarding data security are subject to administrative enforcement and penalties (see Section II.C.).

State agency provisions: A number of Oregon laws govern the responsibilities of state agencies. For example, the state Chief Information Officer (CIO) is responsible for information systems security in the state's executive department, including steps reasonably necessary to protect the availability, integrity, or confidentiality of all information systems or the information stored in such systems, and is charged with establishing a state information systems security plan (Or. Rev. Stat. § 276A.300(2)). The CIO also may coordinate with the Oregon Department of Administrative Services to review the security of information systems operated by state agencies and to conduct assessments of such systems, among other actions (Or. Rev. Stat. § 276A.300(3)). Finally, the CIO is charged with developing and implementing policies for responding to events that damage or threaten information systems or the information they contain (Or. Rev. Stat. § 276A.300(5)).

Notwithstanding the above, the Secretary of State, State Treasurer, and Attorney General have sole discretion and authority over information security in their respective agencies, and each of them must establish a security plan in collaboration with the state CIO as outlined above. The law provides the minimum requirements to be included in such a plan (Or. Rev. Stat. § 276A.303).

The law requires state agencies to provide notification to the Legislative Fiscal Office of any information security incidents, including a description of steps taken by the agency to prevent or mitigate damages resulting from unauthorized access to the agency's information system or resources (Or. Rev. Stat. § 276A.306).

Consolidation of information technology security functions: Under a new law effective July 1, 2017, state agencies have been charged with cooperating with the state CIO in the implementation of a continuing statewide agency-by-agency risk-based information technology security assessment and remediation

program, and with cooperating in the development of plans, policies, and standards to unify agency information technology security functions statewide (Or. Rev. Stat. § 276A.323(2)). The new law also establishes, effective Jan. 1, 2018, a Cybersecurity Advisory Council and a Cybersecurity Center of Excellence charged with a variety of responsibilities with respect to cybersecurity issues (Or. Rev. Stat. § 276A.326 and Or. Rev. Stat. § 276A.329). Uncodified provisions in the act that enacted these requirements (Ch. 513 (HB 90), Laws 2017, § 1(2) and § 1(3)) further require state agencies to carry out any actions necessary to unify agency information security functions, including working with the state CIO to transfer agency information technology security functions, employees, records, and property to the state CIO by Jan. 1, 2018.

Student Information Privacy Act: Under the Oregon Student Information Privacy Act (SIPA), an operator of a website, service, or application used for K-12 educational purposes must implement and maintain reasonable security procedures and practices appropriate to the nature of covered information and appropriate to protect the covered information from unauthorized access, destruction, use, modification, or disclosure (Or. Rev. Stat. § 336.184(4)(a)). For more information on SIPA, see Section I.E.20.

I.C.70. **Data Disposal** —

Among the elements contained in the data security requirements set forth in the Oregon Consumer Identity Theft Protection Act (CITPA) (see Section I.C.60.), a required element of a compliant information security program must include physical safeguards ensuring that personal information no longer needed by the person for business purposes or as required by law must be disposed of by burning, pulverizing, shredding, or modifying, a physical record and by destroying or erasing electronic media so that the information cannot be read or reconstructed (Or. Rev. Stat. § 646A.622(2)(d)(C)(iv)). A person subject to this requirement is deemed to be in compliance if the person contracts with another person engaged in the business of record destruction to dispose of personal information in a manner consistent with these requirements (Or. Rev. Stat. § 646A.622(3)).

In general, persons who comply with a state or federal law that imposes more stringent data security requirements than the CITPA, or who comply with regulations promulgated under the federal Gramm-Leach-Bliley Act or federal Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, including any requirements regarding data disposal contained therein, are deemed to be in compliance with the CITPA (Or. Rev. Stat. § 646A.622(2)(a)-(c)).

Persons who violate the provisions of the CITPA regarding data disposal are subject to administrative enforcement and penalties (see Section II.C.).

Student Information Privacy Act: Under the Oregon Student Information Privacy Act (SIPA), an operator of a website, service, or application used for K-12 educational purposes must delete a student's covered information within a reasonable time if the school or school district requests such deletion (Or. Rev. Stat. § 336.184(4)(b)). For more information on SIPA, see Section I.E.20.

I.C.80. **Data Breach** —

Provisions of the Oregon Consumer Identity Theft Protection Act (CITPA) require any person that owns or licenses personal information that the person uses in the course of business, vocation, occupation, or volunteer activities that was subject to a breach of security to provide notification of the breach to specified parties (Or. Rev. Stat. § 646A.604(1)), as outlined below.

Primary definitions: A “breach of security” means an unauthorized acquisition of computerized data that

materially compromises the security, confidentiality, or integrity of personal information maintained by a person. The term does not include an inadvertent acquisition of personal information by a person or the person's employee or agent if the information is not used in violation of applicable law or in a manner that harms or poses an actual threat to the security, confidentiality, or integrity of the information (Or. Rev. Stat. § 646A.602(1)).

A “person” is an individual, private or public corporation, partnership, cooperative association, estate, limited liability company, organization, or other entity, whether or not organized for profit, or a public body as defined by Oregon law (including state government bodies, local government bodies, and special government bodies) (Or. Rev. Stat. § 646A.602(10)). A “consumer” is an individual resident of Oregon (Or. Rev. Stat. § 646A.602(2)).

“Personal information” is defined as a consumer's first name or first initial and last name in combination with any of the following data elements, if encryption, redaction, or other methods have not rendered the elements unusable or if the data elements are encrypted but the encryption key has been acquired:

- consumer's social security number;
- consumer's driver's license number or state ID card number;
- consumer's passport number or other ID number issued by the U.S.;
- consumer's financial account number, credit card number, or debit card number, in combination with any required security code, access code, or password that would permit access to the consumer's financial accounts, or any other information or combination of information that a person reasonably knows or should know would permit such access;
- data from automatic measurements of a consumer's physical characteristics, such as images of a fingerprint, retina, or iris, that are used to authenticate a consumer's identity in the course of a financial or other transaction;
- consumer's health insurance policy number or subscriber ID number in combination with any other unique identifier used by an insurer to identify the consumer; or
- information about a consumer's medical history or mental or physical condition or about a health care professional's medical diagnosis or treatment of the consumer (Or. Rev. Stat. § 646A.602(11)(a)).

“Personal information” includes user name or other means of identifying a consumer for the purpose of permitting access to the consumer's account, together with any other method necessary to authenticate the user name or means of identification (Or. Rev. Stat. § 646A.602(12)(a)).

Each of the above data elements, alone or in combination, also qualifies as “personal information,” even when not in combination with a consumer's first name or first initial and last name, if encryption, redaction, or other methods have not rendered the data element unusable, and the data element or combination of data elements would enable a person to commit identity fraud against a consumer (Or. Rev. Stat. § 646A.602(11)(b)). “Personal information” does not include information in federal, state, or local government records, other than a social security number, that is lawfully made available to the public (Or. Rev. Stat. § 646A.602(11)(c)).

Notification requirement: If a person owns, licenses, or otherwise possesses personal information that the

person uses in the course of business, vocation, occupation, or volunteer activities and that was the subject of a breach of security, or the person received notice of a breach from another person that maintains or otherwise possesses personal information on the person's behalf, the person must give notice of a breach of security to the person to whom the personal information pertains (Or. Rev. Stat. § 646A.604(1)(a) and Or. Rev. Stat. § 646A.604(2)). The person must also provide notification to the Attorney General, either in writing or electronically, if the number of consumers to whom the person must send the notice described above exceeds 250 (Or. Rev. Stat. § 646A.604(1)(b)). A person maintaining or possessing personal information on another person's behalf as described above must notify the other person as soon as practicable after discovering a breach (Or. Rev. Stat. § 646A.604(2)).

The person that must give notice under these provisions must provide it in the most expeditious manner possible, without unreasonable delay, but not later than 45 days after discovering or receiving notification of the breach. In providing the notice, the person must undertake reasonable measures necessary to determine sufficient contact information for the affected consumer, to determine the scope of the breach, and to restore the reasonable integrity, security, and confidentiality of the information (Or. Rev. Stat. § 646A.604(3)(a)).

Notification may be delayed if a law enforcement agency determines that such notification will impede a criminal investigation and the law enforcement agency requests in writing that notification be delayed (Or. Rev. Stat. § 646A.604(3)(b)).

Third-party vendors who suffer a data breach have certain notification requirements. The Oregon Consumer Information Protection Act (OCIPA) requires vendors to notify covered entities as soon as is practicable but not later than 10 days after discovering a breach. If the breach involves personal information of more than 250 consumers, the state attorney general must be notified (Or. Rev. Stat. § 646A.604(2)(a)-(c)).

Form and content of notice: Notification may be given to consumers by written notice, by electronic notice if the electronic notice provided is consistent with federal requirements regarding electronic records and signatures, by telephone if the person contacts the consumer directly, or by substitute notice under specified circumstances (Or. Rev. Stat. § 646A.604(4)(a)-(d)). Substitute notice is allowed if the person demonstrates that the cost of notice otherwise would exceed $250,000, that the number of consumers to receive notice exceeds 350,000, or the person does not have sufficient contact information. Substitute notice means posting the notice, or a link to the notice, conspicuously on the person's website if one is maintained and providing notice to major statewide television and newspaper media (Or. Rev. Stat. § 646A.604(4)(d)).

In general, the notification must include a description of the breach in general terms, the approximate date of the breach, the type of personal information subject to the breach, contact information for the person providing notification, contact information for national consumer reporting agencies (CRAs), and advice to the consumer to report suspected identity theft to the Attorney General and the Federal Trade Commission (Or. Rev. Stat. § 646A.604(5)).

Notice to CRAs: If a person discovers a breach of security that affects more than 1,000 consumers, the person also must notify, without unreasonable delay, all nationwide CRAs of the timing, distribution, and content of the notice and must include in the notice any police report number assigned to the breach. The person may not delay notification of consumers as outlined above in order to notify CRAs (Or. Rev. Stat. § 646A.604(6)).

Credit monitoring and identity theft prevention and mitigation: Effective June 2, 2018, if a person must notify a consumer of a security breach, and in connection with notification offers to provide credit monitoring services or identity theft prevention and mitigation services without charge, the person may not condition the

offer on a consumer's providing a credit or debit card number or on the acceptance of any other service of the person for a fee (Or. Rev. Stat. § 646A.604(7)(a)). If such services are offered for a fee, the person must separately, distinctly, clearly, and conspicuously disclose in the offer that the person will charge a fee (Or. Rev. Stat. § 646A.604(7)(b)). Any contract under which one person provides such services on behalf of another person also must comply with these provisions (Or. Rev. Stat. § 646A.604(7)(c)).

Exceptions: A person does not need to notify consumers of a breach of security if, after an appropriate investigation or consultation with relevant law enforcement agencies, the person reasonably determines that consumers whose personal information was subject to the breach are unlikely to suffer harm. Documentation of such a determination must be in writing and maintained for at least five years (Or. Rev. Stat. § 646A.604(8)).

In addition, the breach notification requirements do not apply to a person that complies with notification requirements established by the person's primary or functional regulator, if such requirements provide greater protection to personal information and disclosure requirements at least as thorough as those provided under the CITPA (Or. Rev. Stat. § 646A.604(9)(a)). Similar exceptions apply to persons who comply with state or federal laws that provide greater protections than those established under the CITPA (Or. Rev. Stat. § 646A.604(9)(b)), persons who comply with federal Gramm-Leach-Bliley Act regulations (Or. Rev. Stat. § 646A.604(9)(c)), and persons subject to regulation under the federal Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule that meet specified statutory requirements, including sending notice to the Attorney General (Or. Rev. Stat. § 646A.604(9)(d)).

Notwithstanding the exceptions outlined above, a person that owns or licenses personal information shall provide the Attorney General within a reasonable time at least one copy of any notice the person sends to consumers or to the person's primary regulator in compliance with statutory requirements (Or. Rev. Stat. § 646A.604(10)).

Enforcement: A violation of the data breach notification requirements constitutes an unlawful trade practice (Or. Rev. Stat. § 646A.604(11)(a)). In addition, persons who violate the provisions of the CITPA in general, including those on data breach notification, are subject to administrative enforcement and penalties (Or. Rev. Stat. § 646A.624; see Section II.C.).

I.C.90. **Data Transfer & Cloud Computing** —

State agency policies on cloud computing: Our research has uncovered no general Oregon laws addressing data transfers or cloud computing. However, in Statewide Policy No. 107-004-150, effective July 18, 2016, the Office of the State Chief Information Officer (OSCIO) sets forth standards to ensure that state agencies analyze the benefits and risks associated with cloud computing solutions, assess the readiness of a proposed cloud vendor, and ensure that state information and financial assets are properly protected when adopting a cloud solution. The policy document includes a cloud planning readiness and assessment workbook for use by state agencies in implementing OSCIO policies.

Bar association policy on use of cloud services by lawyers: Under Formal Ethics Opinion No. 2011-188, last revised in 2015, the Oregon State Bar Association states that lawyers may store client materials on a third-party server as long as they comply with their duties of competence and confidentiality to keep a client's information secure. To fulfill this obligation, a lawyer must take reasonable steps to ensure that the third-party storage company will reliably secure client data and keep information confidential. In addition, lawyers may be required to reassess the protective measures used by third-party vendors as technologies advance to ensure that their protective measures remain adequate.

I.C.100. **Other Provisions** —

Misrepresentations in privacy policies: It is an unlawful trade practice for a person to publish on a website related to the person's business, or in a consumer agreement related to a consumer transaction, a statement or representation asserting that the person will use, disclose, collect, maintain, delete, or dispose of personal information collected from the consumer and subsequently uses, discloses, collects, maintains, deletes, or disposes of the information in a manner materially inconsistent with the statement or representation (Or. Rev. Stat. § 646.607(12)).

For information on enforcement provisions and private causes of actions available in general for violations classified as unlawful trade practices, see Section I.G.10. and Section II.C.

I.D. **Specific Types of Data**

I.D.10. **Biometric Data** —

Consumer Identity Theft Protection Act: For purposes of the Oregon Consumer Identity Theft Protection Act (CITPA), biometric information (specifically, “data from automatic measurements of a consumer's physical characteristics, such as images of a fingerprint, retina or iris, that are used to authenticate a consumer's identity in the course of a financial or other transaction”) is defined as “personal information” when used in combination with a person's name, or when used not in combination with a person's name if encryption, redaction, or other methods have not rendered the information unusable, and the information would enable a person to commit identity fraud against a consumer (Or. Rev. Stat. § 646A.602(11)(a)(E) and Or. Rev. Stat. § 646A.602(11)(b)). Accordingly, such information is subject to CITPA requirements regarding data breach notifications (see Section I.C.80.), security freezes (see Section I.D.40.), data security (see Section I.C.60.), data disposal (see Section I.C.70.), and prohibitions on the display of social security numbers (see Section I.D.100.).

Student Information Privacy Act: For purposes of the restrictions on the collection and disclosure of data on operators of K-12 online services and applications under the Oregon Student Information Privacy Act (SIPA), biometric information is included in the definition of “covered information” subject to SIPA requirements. For more information, see Section I.E.20.

I.D.20. **Consumer Data** —

Identity verification in transactions: A merchant accepting a credit or debit card for a transaction may require that the holder provide personal consumer information, other than the personal information appearing on the front of the credit or debit card, for purposes of verification of the card holder's identity. The merchant may not write the information on the credit or debit card transaction form (Or. Rev. Stat. § 646A.214(1)). This provision does not prevent a merchant from requesting and keeping in written form information necessary for shipping, delivery, or installation of purchased goods or services or for warranty purposes when such information is voluntarily provided by the holder (Or. Rev. Stat. § 646A.214(2)). In addition, merchants are not required to verify the identity of a cardholder and may make and enforce their own policies regarding identity verification (Or. Rev. Stat. § 646A.214(4)).

Consumer Identity Theft Protection Act: For purposes of the Oregon Consumer Identity Theft Protection Act (CITPA), consumer data, such as a social security or account number, or other numbers or codes allowing access to an individual's accounts, is defined as “personal information” when used in combination with a person's name, or when used not in combination with a person's name if encryption, redaction, or other methods have not rendered the information unusable, and the information would enable a person to commit

identity fraud against a consumer (Or. Rev. Stat. § 646A.602(11)(a) and Or. Rev. Stat. § 646A.602(11)(b)). Accordingly, such information is subject to CITPA requirements regarding data breach notifications (see Section I.C.80.), security freezes (see Section I.D.40.), data security (see Section I.C.60.), data disposal (see Section I.C.70.), and prohibitions on the display of social security numbers (see Section I.D.100.).

Identity theft: A variety of information included in consumer data, including a person's name, address, and phone number, among others, is included in the definition of “personal information” subject to Oregon's identity theft law (see Section I.G.20.).

Student Information Privacy Act: For purposes of the restrictions on the collection and disclosure of data on operators of K-12 online services and applications under the Oregon Student Information Privacy Act (SIPA), socioeconomic data and food purchases are among the items included in the definition of “covered information” subject to SIPA requirements. For more information, see Section I.E.20.

I.D.30. **Credit Card Data** —

Limitations on information in credit card receipts: In a credit or debit card transaction with a customer, a person may not create a receipt that shows more information about a customer than the customer's name and five digits of the customer's debit or credit card number (Or. Rev. Stat. § 646A.204(1)). A person that creates a receipt containing more information about a customer than that described above must shred, incinerate, or otherwise destroy the copy on or before the date the copy is transferred onto microfilm or microfiche, or 36 months after the date of the transaction, whichever is earlier (Or. Rev. Stat. § 646A.204(2)).

A person may not sell, lease, or rent any payment processing system that provides a customer receipt that shows more information about a customer than the customer's name and five digits of the customer's credit or debit card number (Or. Rev. Stat. § 646A.202).

Violations of these provisions are subject to injunction and civil penalties (see Section II.C.).

Credit card information in connection with payment by check: No person (including an individual, corporation, partnership, or association) may require, as a condition for acceptance of a check or share draft, or as a means of identification, that a person provide a credit card number or expiration date, or both, unless the credit is issued by the person requesting the information (Or. Rev. Stat. § 646A.210(1)). However, this prohibition does not prevent a person from doing any of the following:

- requesting a person presenting a check to display a credit card as indicia of creditworthiness or as a source of additional identification;
- recording the type of credit card and the issuer when displayed for the above purpose;
- requesting and recording a credit card number or expiration date, or both, in lieu of a security deposit to assure payment in the event of default, loss, damage, or other occurrence;
- recording a credit card number or expiration date, or both, as a condition for acceptance of a check where the card issuer guarantees checks presented by the cardholder on the condition that the person to whom the cardholder presents the check records such information on the check;
- requesting and recording the name, address, motor vehicle operator license number or state ID number, and telephone number of a person offering payment by check; or
- verifying the signature, name, and expiration date on a credit card (Or. Rev. Stat. § 646A.210(2)).

Consumer Identity Theft Protection Act: For purposes of the Oregon Consumer Identity Theft Protection Act (CITPA), a consumer's credit or debit card number, in combination with any required security code, access code, or password permitting access to a consumer's financial account, is defined as “personal information” when used in combination with a person's name, or when used not in combination with a person's name if encryption, redaction, or other methods have not rendered the information unusable, and the information would enable a person to commit identity fraud against a consumer (Or. Rev. Stat. § 646A.602(11)(a)(D) and Or. Rev. Stat. § 646A.602(11)(b)). Accordingly, such information is subject to CITPA requirements regarding data breach notifications (see Section I.C.80.), security freezes (see Section I.D.40.), data security (see Section I.C.60.), data disposal (see Section I.C.70.), and prohibitions on the display of social security numbers (see Section I.D.100.).

Identity theft: A credit card account number is included in the definition of “personal information” subject to Oregon's identity theft law (see Section I.G.20.).

I.D.40. **Credit Reports** —

Security freezes: Provisions of the Oregon Consumer Identity Theft Protection Act govern the placement of security freezes on consumer reports; requirements that consumer reporting agencies (CRAs) must meet in placing, temporarily lifting, and removing such freezes; and requirements regarding the disclosure of information subject to a freeze. Specific provisions apply to the placement of security freezes on protected persons such as incapacitated or underage persons. These provisions are outlined below.

> ***Note:*** *Federal legislation effective Sept. 21, 2018—the Economic Growth, Regulatory Relief, and Consumer Protection Act (Pub. L. No. 115-174)—establishes a national security freeze law applicable to consumers in general as well as to protected consumers (i.e., those under age 16 or those who are incapacitated or for whom a guardian or conservator has been appointed). The law amends provisions of the Fair Credit Reporting Act by establishing federal parameters for placing, temporarily lifting, or removing such freezes; it also prohibits the imposition of fees by a consumer reporting agency (CRA) for such services (15 U.S.C. § 1681c-1(i) and (j)). The federal law presumably preempts state law provisions governing security freezes. In the case of state fee provisions, the federal law is more favorable to consumers, but some states have stronger protections in their security freeze laws than those under the federal provision, including states that prohibit access to a security freeze for employer background checks. The federal law specifically permits access to a report subject to a freeze for such purposes.*

Request for freeze: A consumer may elect to place a security freeze on his report, or if acting as a representative, on the report of a protected consumer, by sending a written request to the CRA at an address designated by the CRA to receive such requests or via a secure electronic request on a website designated by the CRA (Or. Rev. Stat. § 646A.606(1)). If the consumer or protected consumer is a victim of identity theft or has filed a report with a law enforcement agency, a copy of the police report, incident report, or identity theft declaration may be included with the request (Or. Rev. Stat. § 646A.606(2)). The consumer or representative must provide proper identification (Or. Rev. Stat. § 646A.606(3)(a) and, in the case of a representative, sufficient proof of authority to act on behalf of the protected person as outlined in the law (Or. Rev. Stat. § 646A.606(3)(b)). Unless an exception applies, if a freeze is in place for a report, information contained in the report may not be released without prior express authorization from the consumer or until a protected consumer or his representative removes the freeze (Or. Rev. Stat. § 646A.606(4)). CRAs are permitted to advise a third party that a security freeze is in effect with respect to a consumer report (Or. Rev. Stat. § 646A.606(5)).

Placement requirements: A security freeze requested as outlined above must be placed within five business

days of receiving a valid request, proper identification, and a fee, if applicable (Or. Rev. Stat. § 646A.608(1)(a)).

If a consumer report does not exist for a protected consumer on whose behalf a freeze is requested, a CRA must create a protective record after receiving a request, along with proper identification and proof of authority. The CRA then must place a freeze on the protective record (Or. Rev. Stat. § 646A.608(1)(b)). The protective record does not need to contain any information other than the protected consumer's personal information. The CRA may not use or release such information to another person for the purpose of assessing a protected consumer's eligibility or capacity for credit, as a basis for evaluating the protected consumer's character or reputation, or for other purposes not related to identity theft prevention (Or. Rev. Stat. § 646A.608(1)(c)).

A CRA must send written confirmation of the freeze to the consumer at his last known address within 10 days after placing the freeze and also must provide the consumer with a unique personal ID number or password or similar device that the consumer must use to authorize a temporary or permanent removal of a freeze (see below). The confirmation must include information on the process for removing or temporarily lifting a freeze. A CRA is not required to provide a consumer or representative with a personal ID number or password to be used to authorize the CRA to release information from a protective record (Or. Rev. Stat. § 646A.608(2)).

If a freeze is in place, a CRA may not change specified information, including name, date of birth, social security number, or address, without sending a written confirmation of the change to the consumer within 30 days of the change being posted to the consumer's file. Technical modifications such as abbreviations or complete spellings do not require confirmation. If an address change is made, confirmation must be sent to the new and former address of the consumer (Or. Rev. Stat. § 646A.618(1)).

Temporary lifting of freeze: A consumer wishing to lift a security freeze for a specific period of time must contact the CRA at the designated point of contact to request the temporary lifting and must provide proper identification, the unique personal ID number or password provided by the CRA, and an indication of the time period for which the report will be made available (Or. Rev. Stat. § 646A.608(3)(a)). Protected records are not subject to a temporary lifting of a freeze (Or. Rev. Stat. § 646A.608(3)(b)), nor are consumer reports for protected persons unless the freeze was placed based on a material misrepresentation of fact by the protected consumer or representative (Or. Rev. Stat. § 646A.608(3)(c) and Or. Rev. Stat. § 646A.614(2)(a)).

A CRA receiving a valid request for temporary lifting of a freeze must comply with the request within three business days after receiving proper identification and the information outlined above (Or. Rev. Stat. § 646A.608(4)(a)).

Permanent removal of freeze: A freeze must remain in place until the consumer requests its removal using a point of contact designated by the CRA. A CRA must remove a security freeze within three business days after receiving a valid request for removal that provides proper identification, the unique personal ID number or password provided by the CRA, and a fee, if applicable (Or. Rev. Stat. § 646A.608(5)(a)). Security freezes applicable to protective records must remain in place until the protected consumer or representative meets similar requirements regarding a valid request, proper identification, sufficient proof of authority, and proof that a representative's authority is no longer valid if the protected consumer attempts to remove the freeze or delete the protective record. The CRA does not have an affirmative duty to notify a protected consumer or a representative that a freeze is in place or to remove the freeze once the protected consumer loses status as a protected consumer; rather, the protected consumer or representative has the duty to request removal. Upon receipt of the required documentation, the CRA must remove the freeze within 30 days of receipt of the request from the protected consumer or representative (Or. Rev. Stat. § 646A.608(5)(b)).

Fees: Provisions governing fees for the placement, temporary lifting, or removal of credit freezes are amended effective June 2, 2018. Under law effective prior to that date, CRAs may not charge a fee for placement of a security freeze if the consumer is a victim of identity theft or has reported the theft of personal information to a law enforcement agency, provided a copy of the police report, incident report, or identity theft declaration is provided to the CRA (Or. Rev. Stat. § 646A.610(1)). However, in general, CRAs may charge a reasonable fee, up to $10, for each placement of a freeze, temporary lifting of a freeze, removal of a freeze, or replacement of a lost personal ID number or password (Or. Rev. Stat. § 646A.610(2)(a)). A fee of up to $10 also may be charged for the placement or removal of a freeze on a protected consumer's report or protective record, or to create or delete a protective record, but the fee is waived for a placement or removal of a freeze on an existing consumer report or protective record of a protected consumer who is under age 16 at the time a representative requests the placement or removal (Or. Rev. Stat. § 646A.610(2)(b)).

Effective June 2, 2018, CRAs are prohibited from charging consumers a fee or collecting any money or item of value for placing, temporarily lifting, or removing a security freeze; creating or releasing a protective record; placing or removing a security freeze on a protective record for a protected consumer; or replacing a lost personal ID number, password, or similar device previously provided to the consumer by the CRA (Or. Rev. Stat. § 646A.610(1)-(4)).

Other conditions for lifting or removing a security freeze: In addition to lifting or removing security freezes in the manner described above (see also Or. Rev. Stat. § 646A.612(1)), a CRA also may temporarily lift or remove a freeze from a consumer report or protected consumer report, or remove a freeze from or delete a protective record, if the freeze was placed based on a consumer's, protected consumer's, or representative's material misrepresentation of fact (Or. Rev. Stat. § 646A.612(2)(a)-(b)). If a CRA intends to remove a freeze or delete a protective record under this provision, it must notify the consumer, protected consumer, or representative in writing at least five business days prior to the removal or deletion (Or. Rev. Stat. § 646A.612(2)(c)).

Exceptions: The security freeze requirements do not apply to the use of a consumer report or protective record by a variety of persons and entities, including persons with whom the consumer has a financial obligation for purposes of reviewing an account or collecting an obligation; persons to whom access has been granted for facilitating the extension of credit; persons acting pursuant to warrant or court order; specified federal, state, or local agencies; or a CRA providing a copy of the report or record to the consumer, protected person, or representative at his request, among others (Or. Rev. Stat. § 646A.614(1)). In addition, security freeze provisions do not apply to protective records used by specified entities or for purposes other than an extension of credit, including compiling a criminal record, detecting or preventing fraud, compiling a personal loss history, or screening an applicant for employment, tenancy, or other background check purposes (Or. Rev. Stat. § 646A.614(2)).

In addition, specified entities are not required to place a security freeze in a credit report. These include a person that acts only as a reseller of credit information by assembling information held and maintained in the databases of one or more credit reporting agencies and that does not maintain a permanent database of information from which new credit reports are produced, although such resellers must honor any security freeze placed on a report by another CRA (Or. Rev. Stat. § 646A.618(2)(a)). Specified check services and fraud prevention companies and deposit account information service companies also are exempt from the security freeze requirements (Or. Rev. Stat. § 646A.618(2)(b)-(c)).

Requests in connection with credit or other applications: If a third party requests access to a consumer report on which a security freeze is in place in connection with an application for credit or any other use, the consumer does not allow access, and the third party cannot obtain access through any of the other exceptions

outlined above, the third party may treat the application as incomplete (Or. Rev. Stat. § 646A.616).

Enforcement: Persons who violate the security freeze provisions outlined above are subject to administrative enforcement and penalties (Or. Rev. Stat. § 646A.624; see Section II.C.).

Employer inquiries into credit history of applicants and employees: In general, it is an unlawful employment practice for an employer to obtain or use for employment purposes information contained in the credit history of an applicant or employee (Or. Rev. Stat. § 659A.320(1)). For more information on this prohibition, see Section I.E.60.

I.D.50. **Criminal Records** —

Employers' use of criminal records: Employers are permitted under specified circumstances to inquire into the criminal records of applicants for employment, but many restrictions apply. In addition, employers generally may not rely on an expunged juvenile criminal record in making employment decisions. For information on these provisions, see Section I.E.60.

Required background checks: Certain entities are required to conduct a criminal background check prior to hiring an applicant, such as intrastate for-hire carriers of household goods (see Or. Rev. Stat. § 825.325), service centers hiring ignition interlock device technicians (Or. Rev. Stat. § 813.665), and home health agencies and in-home care agencies (Or. Rev. Stat. § 443.004), among others. In addition, employees, volunteers, providers, and contractors of the Oregon Health Authority are subject to mandatory criminal background checks (Or. Admin. R. 943-007-0001).

Student Information Privacy Act: For purposes of the restrictions on the collection and disclosure of data on operators of K-12 online services and applications under the Oregon Student Information Privacy Act (SIPA), criminal records are included in the definition of "covered information" subject to SIPA requirements. For more information, see Section I.E.20.

I.D.60. **Drivers' Licenses/Motor Vehicle Records** —

Confidentiality of personally identifiable information used to report and collect road use charges: For purposes of the road usage charge imposed on registered owners of subject vehicles imposed under Or. Rev. Stat. § 319.885, personally identifiable information used for reporting metered use or for administrative use related to the collection of the per-mile road usage charge is confidential and is a public record exempt from disclosure (Or. Rev. Stat. § 319.915(2)). Such information may not be disclosed by the Department of Transportation or any certified provider having an agreement with the Department to any person except the registered owner or lessee, a financial institution for purposes of collecting the charge, employees of the Department, a certified service provider or contractor thereof, an entity expressly authorized to receive the information by the registered owner or lessee, or a police officer pursuant to a valid court order (Or. Rev. Stat. § 319.915(3)(a)). In addition, the Department must destroy records of the location and daily metered use of subject vehicles within 30 days after completion of payment processing, dispute resolution, or a noncompliance investigation, whichever is latest, although such records may be retained under specified circumstances (Or. Rev. Stat. § 319.915(4)). Certified service providers violating these provisions may be subject to penalties based on an agreement with the Department (Or. Rev. Stat. § 319.915(5)).

For information on the road usage charge, see this Final Report from the Department of Transportation.

Event data recorder information: Under Oregon's event data recorder law, the data on a motor vehicle event data recorder is owned exclusively by the vehicle owner and may not be retrieved or used by any other person

without the written consent of the owner. If there is more than one owner, all owners must consent (Or. Rev. Stat. § 105.928). Data on an event data recorder does not become the property of a lienholder or insurer that becomes a successor in ownership as a result of an accident. Insurers may not condition payment of a settlement on a claim on the owner's consent to the retrieval or use of such data, and insurers and lessors of motor vehicles may not require an owner to give such consent as a condition of providing a policy or lease (Or. Rev. Stat. § 105.932).

Data from an event data recorder may be retrieved without the owner's consent to facilitate the need for emergency care for a driver or passenger involved in a crash or other emergency, including data from a company providing subscriber services for in-vehicle safety and security communications systems (Or. Rev. Stat. § 105.942(1)). Such data also may be used for specified medical research purposes or to diagnose, service, or repair a motor vehicle (Or. Rev. Stat. § 105.942(2)). Finally, the event data recorder provisions do not apply to data stored or transmitted pursuant to a subscription service agreement for the use of a recording device to record a history of where a motor vehicle travels or for the transmission of data to a central communications system (Or. Rev. Stat. § 105.945).

Department of Transportation records: The Department of Transportation is prohibited from disclosing an individual's social security number (SSN) obtained in connection with a motor vehicle record, although it may disclose an SSN to another agency for use in carrying out the other agency's functions. Such agencies are prohibiting from redisclosing an SSN. A violation is a class A misdemeanor, and a person aggrieved by a violation may bring a civil action (see Section I.G.10.). In addition, the Attorney General or a district attorney may obtain appropriate relief (see Section II.C.) (Or. Rev. Stat. § 802.195).

Consumer Identity Theft Protection Act: For purposes of the Oregon Consumer Identity Theft Protection Act (CITPA), a consumer's driver's license number or state ID number issued by the Oregon Department of Transportation is defined as “personal information” when used in combination with a person's name, or when used not in combination with a person's name if encryption, redaction, or other methods have not rendered the information unusable, and the information would enable a person to commit identity fraud against a consumer (Or. Rev. Stat. § 646A.602(11)(a)(B) and Or. Rev. Stat. § 646A.602(11)(b)). Accordingly, such information is subject to CITPA requirements regarding data breach notifications (see Section I.C.80.), security freezes (see Section I.D.40.), data security (see Section I.C.60.), data disposal (see Section I.C.70.), and prohibitions on the display of social security numbers (see Section I.D.100.).

Identity theft: A person's driving privileges, as well as a personal ID number, are included in the definition of “personal identification” subject to Oregon's identity theft law (see Section I.G.20.).

I.D.70. **Electronic Communications/Social Media Accounts** —

Privacy of employee and student social media account information: In general, it is an unlawful employment practice for an employer to require an employee or applicant to provide access to his personal social media accounts or to take punitive action against an employee, or refuse to hire an applicant, based on his refusal to provide such access. For a comprehensive discussion of these requirements, see Section I.E.60.

Similar restrictions apply to educational institutions with respect to social media accounts of students and prospective students (see Section I.E.20.).

Obtaining personal information by false representation via electronic media: Persons may not use a website, e-mail message, text message, or other electronic means to solicit, request, or otherwise induce another person to provide personal information by representing to the other person that the person is a third

person, without the third person's authorization and consent (Or. Rev. Stat. § 646A.808(2)(a)). The prohibition does not apply to law enforcement officers or agencies engaged in official duties or to individuals authorized by law to conduct a lawful investigation (Or. Rev. Stat. § 646A.808(2)(b)). A violation is an unlawful trade practice (Or. Rev. Stat. § 646A.808(3)).

Identity theft: A person's e-mail name, signature address, or account is included in the definition of “personal identification” subject to Oregon's identity theft law (see Section I.G.20.).

Electronic surveillance: For information on electronic surveillance provisions, see Section I.F.

Student Information Privacy Act: For purposes of the restrictions on the collection and disclosure of data on operators of K-12 online services and applications under the Oregon Student Information Privacy Act (SIPA), a student's e-mail address or other information allowing online contact is included in the definition of “covered information” subject to SIPA requirements. For more information, see Section I.E.20.

I.D.80. **Social Security Numbers** —

Consumer Identity Theft Protection Act: Under the Oregon Consumer Identity Theft Protection Act (CITPA), a person may not:

- • print a consumer's social security number (SSN) on mail to the consumer that is (a) material the consumer did not request, or (b) part of any documentation the consumer requested, unless the SSN is redacted;

- print a consumer's SSN on any card required for the consumer to access products or services provided by the person;

- publicly post or display a consumer's SSN unless the SSN is redacted; or

- dispose of, or transfer to another person for disposal, material or media that display a consumer's SSN unless the person makes the SSN unreadable or unrecoverable or ensures that any person that ultimately disposes of the material or media makes the SSN unreadable or unrecoverable (Or. Rev. Stat. § 646A.620(1)).

The prohibition outlined above does not prevent the collection, use, or release of an SSN as required by state or federal law, or by rules adopted by certain Oregon state court judges, and does not prevent the use or printing of an SSN for internal verification or administrative purposes to enforce a judgment or court order (Or. Rev. Stat. § 646A.620(2)). In addition, the law does not apply to records that must be made available to the public under state or federal law or rule adopted by certain Oregon state court judges (Or. Rev. Stat. § 646A.620(3)). Finally, the provision does not apply to an SSN in (a) a record maintained by a court or the Secretary of State that was received on or before Oct. 1, 2007, (b) such a record received after that date if, by state or federal law or rule, the person submitting the record could have caused it to be filed or maintained in a manner that protected the SSN from public disclosure, or (c) any record, regardless of date, that is an accusatory instrument charging a crime, a record of oral proceedings in court, an exhibit offered as evidence, or a judgment or court order (Or. Rev. Stat. § 646A.620(4)).

Persons who violate the provision prohibiting the printing of SSNs are subject to administrative enforcement and penalties (Or. Rev. Stat. § 646A.624; see Section II.C.).

Other CITPA requirements: Because a consumer's SSN is defined as “personal information” when used in

combination with a person's name, or when used not in combination with a person's name if encryption, redaction, or other methods have not rendered the information unusable, and the information would enable a person to commit identity fraud against a consumer (Or. Rev. Stat. § 646A.602(11)(a)(A) and Or. Rev. Stat. § 646A.602(11)(b)), such information is subject to CITPA requirements regarding data breach notifications (see Section I.C.80.), security freezes (see Section I.D.40.), data security (see Section I.C.60.), and data disposal (see Section I.C.70.).

Identity theft: SSNs are included in the definition of “personal identification” subject to Oregon's identity theft law (see Section I.G.20.).

Department of Transportation records: The Department of Transportation is prohibited from disclosing an individual's SSN obtained in connection with a motor vehicle record, although it may disclose an SSN to another agency for use in carrying out the other agency's functions. Such agencies are prohibiting from redisclosing an SSN. A violation is a class A misdemeanor, and a person aggrieved by a violation may bring a civil action (see Section I.G.10.). In addition, the Attorney General or a district attorney may obtain appropriate relief (see Section II.C.) (Or. Rev. Stat. § 802.195).

Student Information Privacy Act: For purposes of the restrictions on the collection and disclosure of data on operators of K-12 online services and applications under the Oregon Student Information Privacy Act (SIPA), SSNs are included in the definition of “covered information” subject to SIPA requirements. For more information, see Section I.E.20.

Public universities and community colleges: A public university may not disclose the SSN of a student attending the university (Or. Rev. Stat. § 326.587(1)). The same restriction applies to community colleges (Or. Rev. Stat. § 326.589(1)). Exceptions apply for disclosures at the request of law enforcement, after obtaining a student's written consent, in the payment of wages or benefits, in the payment or collection of taxes or a debt, or for statistical analysis purposes (Or. Rev. Stat. § 326.587(2); Or. Rev. Stat. § 326.589(2)). Any student who suffers an ascertainable loss as a result of a violation of these provisions may bring an action for actual damages (see Section I.G.10.).

I.D.90. **Usernames & Passwords** —

Privacy of employee and student social media account information: In general, it is an unlawful employment practice for an employer to require an employee or applicant to provide his username or password to enable the employer to gain access to his personal social media accounts, or to take punitive action against an employee, or refuse to hire an applicant, based on his refusal to provide such access. For a comprehensive discussion of these requirements, see Section I.E.60.

Similar restrictions apply to educational institutions with respect to social media accounts of students and prospective students (see Section I.E.20.).

Consumer Identity Theft Protection Act: For purposes of the Oregon Consumer Identity Theft Protection Act (CITPA), a consumer's financial account number, credit card number, or debit card number, in combination with any required security code, access code, or password permitting access to a consumer's financial account, is defined as “personal information” when used in combination with a person's name, or when used not in combination with a person's name if encryption, redaction, or other methods have not rendered the information unusable, and the information would enable a person to commit identity fraud against a consumer (Or. Rev. Stat. § 646A.602(11)(a)(D) and Or. Rev. Stat. § 646A.602(11)(b)). Accordingly, such information is subject to CITPA requirements regarding data breach notifications (see Section I.C.80.), security freezes (see

Section I.D.40.), data security (see Section I.C.60.), data disposal (see Section I.C.70.), and prohibitions on the display of social security numbers (see Section I.D.100.).

I.D.100. **Information about Minors** —

Information on diagnosis and treatment: In general, minors who have come into contact with any venereal disease, including HIV, may give consent for treatment and care related to such disease if the disease is one that is required by law to be reported to a state or local health agency or officer. Consent of a parent or legal guardian is not required, although the parent is not liable for payment for services where consent is not given (Or. Rev. Stat. § 109.610).

While minors, particularly those age 15 and over, have the right to consent to a variety of medical treatments, including birth control information and services (Or. Rev. Stat. § 109.640), a physician, dentist, nurse, or other specified practitioner may advise a parent or legal guardian of the care provided to or the need for treatment of the minor, without the minor's consent, and is not liable for so advising the parent or guardian (Or. Rev. Stat. § 109.650).

Specific mental health services: Minors age 14 and older may obtain specified mental health services without parental consent, but providers must have the parents involved before the end of treatment unless the parents refuse to be involved or there are clear clinical indications to the contrary. The parental involvement requirement specifically does not apply to minors who have been sexually abused by a parent or to emancipated minors who have lived apart from the parent or guardian while being self-sustaining for a period of 90 days prior to seeking treatment (Or. Rev. Stat. § 109.675). A physician, dentist, nurse, or other specified practitioner may advise a parent or guardian of treatment provided as outlined above, when the disclosure is clinically appropriate and will serve the best interests of the minor's treatment because (a) the minor's condition has deteriorated or the risk of suicide has become such that inpatient treatment is necessary, or (b) the minor's condition requires detoxification in a residential or acute care facility. Where such disclosure is necessary, the practitioner is not subject to civil liability for advising the parent or guardian (Or. Rev. Stat. § 109.680).

Practitioners providing treatment for mental health conditions as outlined above are not subject to civil liability for providing the treatment without parental consent (Or. Rev. Stat. § 109.685). Parents who have not consented to such treatment are not liable for payment for the services (Or. Rev. Stat. § 109.690).

Substance abuse services: Although any person may voluntarily apply for admission to a substance abuse treatment facility, if the person is under age 18, the director of the facility must notify the person's parent or guardian of the admission or any referral (Or. Rev. Stat. § 430.397).

I.D.110. **Location Data** —

Personally identifiable information used to report and collect road use charges: Under laws governing the privacy of personally identifiable information collected and used to facilitate the collection of the Oregon road usage charge, any such information related to the location and daily metered use of subject vehicles must be destroyed within a specified period of time (see Section I.D.60.).

Event data recorder law: Provisions of Oregon's event data recorder law requiring consent of a vehicle owner to retrieve information from such a device do not apply to data stored or transmitted pursuant to a subscription service agreement for the use of a recording device to record a history of where a motor vehicle travels (Or. Rev. Stat. § 105.945). For more information on the event data recorder law, see Section I.D.60.

Student Information Privacy Act: For purposes of the restrictions on the collection and disclosure of data on operators of K-12 online services and applications under the Oregon Student Information Privacy Act (SIPA), geolocation information is included in the definition of “covered information” subject to SIPA requirements. For more information, see Section I.E.20.

I.D.120. **Other Personal Data** —

Our research has uncovered no other Oregon law provisions regarding personal data beyond those specified above.

I.E. **Sector-Specific Provisions**

I.E.10. **Advertising & Marketing** —

Anti-spam laws: Oregon does not have any specific statutes governing the distribution of commercial e-mails, or spam.

Obtaining personal information by false representation via electronic media: Persons may not use a website, e-mail message, text message, or other electronic means to solicit, request, or otherwise induce another person to provide personal information by representing to the other person that the person is a third person, without the third person's authorization and consent (Or. Rev. Stat. § 646A.808(2)(a)). The prohibition does not apply to law enforcement officers or agencies engaged in official duties or to individuals authorized by law to conduct a lawful investigation (Or. Rev. Stat. § 646A.808(2)(b)). A violation is an unlawful trade practice (Or. Rev. Stat. § 646A.808(3)).

Do-not-call: A person may not engage in the telephone solicitation of a party at a telephone number included on the current version of a do-not-call list maintained by Oregon or the federal Do-Not-Call Registry (Or. Rev. Stat. § 646.569(1)). As a practical matter, Oregon has adopted the federal Do-No-Call Registry for these purposes (Or. Rev. Stat. § 646.572(1)(b); see this webpage for information from the Oregon Department of Justice on telemarketing law).

For purposes of the prohibition on telephone solicitation, soliciting business from prospective purchasers who have previously purchased from the person making the solicitation, the business enterprise for which the person is calling, or a predecessor of the business enterprise for which the person is calling is not considered a prohibited “telephone solicitation” (Or. Rev. Stat. § 646.569(2)). In addition, telephone solicitations do not include calls made by or on behalf of charitable organizations; calls limited to polling or soliciting the expression of ideas, opinions, or votes; or business-to-business contact (Or. Rev. Stat. § 646.561(3)).

Oregon law also provides that a person engages in an unlawful practice if, during telephone solicitation, the called party states a desire not to be called again and the person makes a subsequent solicitation to the called party at that phone number (Or. Rev. Stat. § 646.563).

Consumer Identity Theft Protection Act: Businesses engaged in the advertising and marketing sector that own or license data that includes “personal information” as defined under the Oregon Consumer Identity Theft Protection Act (CITPA) are subject to the provisions of the CITPA governing data breach notifications (see Section I.C.80.), security freezes (see Section I.D.40.), data security (see Section I.C.60.), data disposal (see Section I.C.70.), and prohibitions on the display of social security numbers (see Section I.D.100.).

Student Information Privacy Act: For information on restrictions on targeted advertising applicable to operators of K-12 online services and applications under the Oregon Student Information Privacy Act (SIPA),

see Section I.E.20.

I.E.20. **Education** —

Oregon Student Information Protection Act: The Oregon Student Information Protection Act (SIPA) specifically restricts the activities of operators of websites and online services and applications for K-12 purposes with respect to collecting information from students or disclosing such information (Or. Rev. Stat. § 336.184). For purposes of the SIPA, an "operator" is an operator of an Internet website, online service, online application, or mobile application with actual knowledge that the site, service, or application is used primarily for K-12 school purposes and was designed and marketed for K-12 school purposes (Or. Rev. Stat. § 336.184(2)(c)). "Covered information" means personally identifiable information or materials that are created or provided by a student or parent to the operator in the course of using the operator's site, service, or application, created for an operator by an employee or agent of a K-12 school, or gathered by an operator and personally identify a student or are linked to information personally identifying a student, including, but not limited to, information in a student's record or e-mail, the student's first and last name, home address, phone number, e-mail address or other information, or various elements of a student's educational information, including discipline records, test results, grades, biometric information, social security number, criminal records, student identifiers, or geolocation information, among others (Or. Rev. Stat. § 336.184(2)(a)).

General restrictions on marketing, use, and disclosure: An operator may not engage in any of the following activities with respect to its site, service, or application:

- engage in targeted advertising;
- target advertising on any other site, service, or application where the targeting is based on information acquired through the use of the operator's site, service, or application;
- use information, including persistent unique identifiers, to create a profile about a student except in furtherance of K-12 educational purposes;
- sell a student's information, including covered information; or
- disclose covered information, unless an exception applies (Or. Rev. Stat. § 336.184(3)).

Exceptions: The prohibition on selling student information does not apply to the purchase, merger, or other type of acquisition of an operator by another entity provided that the successor entity continues to be subject to SIPA requirements (Or. Rev. Stat. § 336.184(3)(D)). In addition, covered information may be disclosed in furtherance of the K-12 purpose, provided that the recipient does not further disclose the information and is subject to the data security requirements under SIPA (see below), to ensure legal and regulatory compliance, to respond to or participate in the judicial process, or to protect the safety of users or others or the security or integrity of the site (Or. Rev. Stat. § 336.184(3)(E)(i)(iv)). Disclosures also are permitted to a service provider, but the contract with such a provider must specify that the provider is prohibited from using covered information for any purpose other than that specified by contract and from disclosing covered information except in furtherance of K-12 school purposes, and must implement and maintain reasonable security measures (see below) (Or. Rev. Stat. § 336.184(3)(E)(v)). The law does not prohibit an operator's use of information for maintaining, developing, supporting, improving, or diagnosing the operator's site, service, or application (Or. Rev. Stat. § 336.184(3)(b)).

Additional exceptions are provided for disclosures required by federal or state law, for legitimate research purposes under specified circumstances, and made to state or local educational agencies (Or. Rev. Stat.

§ 336.184(5)). Finally, operators are permitted to disclose deidentified student covered information if statutory requirements are met; may share aggregated identified student covered information for the development and improvement of educational sites, services, or applications; may use student data (including covered information) for adaptive learning or customized learning purposes; and may respond to student-initiated requests for information or feedback without a response being determined by payment or other consideration from a third party (Or. Rev. Stat. § 336.184(6)).

Security requirements: An operator must implement and maintain reasonable security procedures and practices appropriate to the nature of the covered information and appropriate to protect the covered information from unauthorized access, destruction, use, modification, or disclosure, and must delete a student's covered information within a reasonable time if the school or school district requests such deletion (Or. Rev. Stat. § 336.184(4)).

Miscellaneous: The SIPA specifies that it does not limit the authority of law enforcement agencies to obtain information from an operator, the authority of Internet service providers to provide connectivity to schools, the authority of operators to market directly to parents or legal guardians under specified circumstances, or the right of students or their parents or guardians to download or otherwise maintain their own data or documents (Or. Rev. Stat. § 336.184(7)). In addition, no duty is imposed on providers of electronic gateways or Internet stores, or on interactive computer services, to enforce compliance with SIPA by operators (Or. Rev. Stat. § 336.184(8)). SIPA does not apply to general audience websites, online services, or online or mobile applications, even if login credentials created for an operator's site, service, or application may be used to access the general audience site, service, or application (Or. Rev. Stat. § 336.184(9)).

Violations: A violation of SIPA is an unlawful practice under Or. Rev. Stat. § 646.607 (Or. Rev. Stat. § 336.184(10)).

Privacy of student social media account information: A public or private educational institution may not do any of the following:

- require, request, or otherwise compel a student or prospective student to disclose or provide access to a personal social media account through use of the student's username, password, or other authentication;

- require, request, or otherwise compel a student or prospective student to access a personal social media account in the presence of an administrator or other employee of the educational institution in a manner allowing the administrator or employee to view the contents;

- take, or threaten to take, any action to discipline or prohibit from participation in curricular or extracurricular activities a student or prospective student for refusing to do any of the above-described actions; or

- fail or refuse to admit a prospective student based on the applicant's refusal to do any of the above-described actions (Or. Rev. Stat. § 326.551(1)).

Nothing in the law prohibits an educational institution from conducting an investigation for the purpose of complying with applicable law, regulatory requirements, or prohibitions against student misconduct associated with a personal social medial account or from conducting such an investigation that requires a student to share specific content on a social media account with the institution for it to make a factual determination about the content. However, student cooperation with an investigation does not include providing a username or password providing the institution access to the student's social media account. An institution also may revoke

a student's access to equipment or networks owned or operated by the institution (Or. Rev. Stat. § 326.551(2)).

An educational institution is not liable for obtaining a username or password providing access to a student's social media account through the application of the institution's policies governing the use of equipment or networks owned or operated by the institution, but the institution may not use such information without the student's voluntary consent (Or. Rev. Stat. § 326.551(3)). In addition, the restrictions on access do not apply to social media accounts intended for use solely for education purposes at an educational institution or to social media accounts created by an institution and provided to the student if the student has been given advance notice that the account may be monitored at any time by the institution (Or. Rev. Stat. § 326.551(4)).

A person aggrieved by a violation of the provisions outlined above may file a civil action (see Section I.G.10.).

Permitted disclosures by public schools and school districts: A public school or school district must disclose personally identifiable information or other information allowed to be disclosed under federal Family Educational Rights and Privacy Act provisions from student records to law enforcement, child protective services, and health care professionals in connection with health and safety, and to courts and state and local juvenile justice agencies as specified by law (Or. Rev. Stat. § 336.187).

Disclosures of social security numbers: A public university may not disclose the social security number of a student attending the university (Or. Rev. Stat. § 326.587(1)). The same restriction applies to community colleges (Or. Rev. Stat. § 326.589(1)). Exceptions apply for disclosures at the request of law enforcement, after obtaining a student's written consent, in the payment of wages or benefits, in the payment or collection of taxes or a debt, or for statistical analysis purposes (Or. Rev. Stat. § 326.587(2); Or. Rev. Stat. § 326.589(2)). Any student who suffers an ascertainable loss as a result of a violation of these provisions may bring an action for actual damages (see Section I.G.10.).

Review of educational records: Each educational institution that has custody of a student's education records must annually notify parents and eligible students of their right to review and propose amendments to the records. If a parent or eligible student's proposed amendment to a record is rejected by the educational institution, the parent or eligible student will receive a hearing (Or. Rev. Stat. § 326.575(4)).

Civil action for disclosure of education records: A person claiming to be aggrieved by the reckless disclosure of personally identifiable information from a student's educational record as prohibited by standards issued by the State Board of Education or the governing board of a public university may file an action for equitable relief or damages (see Section I.G.50.).

Consumer Identity Theft Protection Act: Businesses engaged in the education sector that own or license data that includes “personal information” as defined under the Oregon Consumer Identity Theft Protection Act (CITPA) are subject to the provisions of the CITPA governing data breach notifications (see Section I.C.80.), security freezes (see Section I.D.40.), data security (see Section I.C.60.), data disposal (see Section I.C.70.), and prohibitions on the display of social security numbers (see Section I.D.100.).

I.E.30. **Electronic Commerce** —

Consumer Identity Theft Protection Act: Businesses engaged in the electronic commerce sector that own or license data that includes “personal information” as defined under the Oregon Consumer Identity Theft Protection Act (CITPA) are subject to the provisions of the CITPA governing data breach notifications (see Section I.C.80.), security freezes (see Section I.D.40.), data security (see Section I.C.60.), data disposal (see Section I.C.70.), and prohibitions on the display of social security numbers (see Section I.D.100.).

I.E.40. **Financial Services** —

Restriction on disclosure of financial institution records: Unless a statutory exception applies, a financial institution may not provide financial records of a customer to a state or local agency, and a state or local agency may not request or receive from a financial institution financial records of customers (Or. Rev. Stat. § 192.586(1).

Consumer Identity Theft Protection Act: Businesses engaged in the financial services sector that own or license data that includes "personal information" as defined under the Oregon Consumer Identity Theft Protection Act (CITPA) are subject to the provisions of the CITPA governing data breach notifications (see Section I.C.80.), security freezes (see Section I.D.40.), data security (see Section I.C.60.), data disposal (see Section I.C.70.), and prohibitions on the display of social security numbers (see Section I.D.100.).

Insurance information and privacy protection provisions: For a discussion of requirements applicable to licensed insurers concerning the collection and disclosure of financial information, see Section I.E.70.

Restriction on disclosure of financial institution records: Unless a statutory exception applies, a financial institution may not provide financial records of a customer to a state or local agency, and a state or local agency may not request or receive from a financial institution financial records of customers (Or. Rev. Stat. § 192.586(1)). However, this general prohibition does not preclude financial institutions from initiating contact with, and subsequently disclosing financial records to, appropriate state or local agencies in connection with law violations, the Office of the State Treasurer under specified circumstances related to commercial mortgages, or appropriate state or local agencies in connection with a business relationship between the financial institution and the customer, if the disclosure is made in the ordinary course of business and will further the legitimate business interests of the customer or institution (Or. Rev. Stat. § 192.586(2)). The law specifically exempts financial institutions releasing information in connection with a law violation from liability for any loss, damage, or injury (Or. Rev. Stat. § 192.600(5)). Additional disclosures are permitted if the financial information that is disseminated is not identified or identifiable with the records of a particular customer, for specified administrative purposes, and for certain attorney trust account transactions (Or. Rev. Stat. § 192.586(3)-(4)).

A financial institution may disclose financial records of a customer to a state or local agency, and an agency may request or receive such records, when the customer has authorized the disclosure (Or. Rev. Stat. § 192.593(1)). The authorization must be in writing, signed, and dated by the customer; identify the particular records to be disclosed and the agency to which disclosure is authorized; contain notice to the customer that the authorization may be revoked at any time; and inform the customer as to the reason for the request and disclosure (Or. Rev. Stat. § 192.593(2)). Financial institutions may not compel a customer to sign such an authorization as a condition of doing business with the institution (Or. Rev. Stat. § 192.593(3)).

Additional specific exceptions to the general prohibition on disclosures by financial institutions are provided for specified disclosures to the Oregon Department of Human Services or the Oregon Health Authority (Or. Rev. Stat. § 192.588 and Or. Rev. Stat. § 192.589), disclosures to state courts (Or. Rev. Stat. § 192.591), and disclosures under summons or subpoena or under search warrant (Or. Rev. Stat. § 192.596 and Or. Rev. Stat. § 192.598).

The law limits the duty of a financial institution to inquire into the compliance of parties seeking disclosures under the provisions outlined above (Or. Rev. Stat. § 192.600(1)). A financial institution refusing in good faith to make a disclosure is not liable to the customer or a state or local agency for any loss or damage resulting from the refusal (Or. Rev. Stat. § 192.600(2)). Institutions are neither required to notify, nor prohibited from

notifying, customers concerning requests for disclosure received by the institution, except as required by court order (Or. Rev. Stat. § 192.600(3)).

The law provides compliance provisions regarding disclosures, including time limits, permissible fees, and specific procedures for disclosures to law enforcement agencies (Or. Rev. Stat. § 192.602 and Or. Rev. Stat. § 192.603). Customers suffering a loss as a result of a willful or negligent violation of the provisions outlined above may bring a private cause of action (see Section I.G.10.).

Consumer Identity Theft Protection Act: For purposes of the Oregon Consumer Identity Theft Protection Act (CITPA), a consumer's financial account number, in combination with any required security code, access code, or password permitting access to a consumer's financial account, is defined as “personal information” when used in combination with a person's name, or when used not in combination with a person's name if encryption, redaction, or other methods have not rendered the information unusable, and the information would enable a person to commit identity fraud against a consumer (Or. Rev. Stat. § 646A.602(11)(a)(D) and Or. Rev. Stat. § 646A.602(11)(b)). Accordingly, such information is subject to CITPA requirements regarding data breach notifications (see Section I.C.80.), security freezes (see Section I.D.40.), data security (see Section I.C.60.), data disposal (see Section I.C.70.), and prohibitions on the display of social security numbers (see Section I.D.100.).

Identity theft: An identifying number of a person's depository account at a financial institution or trust company is included in the definition of “personal identification” subject to Oregon's identity theft law (see Section I.G.20.).

Insurance information and privacy protection provisions: For a discussion of requirements applicable to licensed insurers concerning the collection and disclosure of financial information, see Section I.E.70.

I.E.50. **Health Care** —

Consumer Identity Theft Protection Act: Businesses engaged in the health care sector that own or license data that includes “personal information” as defined under the Oregon Consumer Identity Theft Protection Act (CITPA) are subject to the provisions of the CITPA governing data breach notifications (see Section I.C.80.), security freezes (see Section I.D.40.), data security (see Section I.C.60.), data disposal (see Section I.C.70.), and prohibitions on the display of social security numbers (see Section I.D.100.).

Requirements related to health data: Requirements applicable to businesses and professionals in the health care sector regarding protected health information are detailed at Section I.E.50.

Protected health information: It is the specified policy of Oregon that individuals have the right to have their protected health information safeguarded from unlawful use and disclosure, as well as the right to access and review such information. Federal Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule provisions establish additional rights and privileges than those established under state law (Or. Rev. Stat. § 192.553). The Oregon protected health information provisions are detailed below.

Primary definitions: The protected health information provisions apply to “covered entities,” which are state health plans, health insurers, health care providers that transmit health information in electronic form to carry out financial or administrative activities, or heath care clearing houses (Or. Rev. Stat. § 192.556(2)). “Health care providers” include physicians, psychologists, therapists, social workers, nurses and nursing home administrators, dentists and dental hygienists, optometrists, and chiropractic practitioners, among many others, and also include health care facilities, home health agencies, hospices, clinical laboratories, pharmacies, and other persons or businesses that bill or are paid for health care (Or. Rev. Stat. § 192.556(5)).

“Health information” means any oral or written communication created or received by a covered entity or other specified entities including employers and schools that relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of such care (Or. Rev. Stat. § 192.556(6)).

“Individually identifiable health information” means any oral or written health information that is (a) created by a covered entity, employer, or health care provider that is not a covered entity and (b) identifiable to an individual, including demographic information that identifies or can reasonably be expected to identify the individual, and that relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of such care (Or. Rev. Stat. § 192.556(7)). “Protected health information” includes individually identifiable health information maintained or transmitted by a covered entity, but does not include education records covered under the federal Family Educational Rights and Privacy Act (FERPA), certain medical records under FERPA, or employment records held by a covered entity in its role as an employer (Or. Rev. Stat. § 192.556(11)).

Authorized uses and disclosures: A health care provider or state health plan may use or disclose protected health information of an individual in a manner that is consistent with an authorization provided by the individual or a personal representative (Or. Rev. Stat. § 192.558(1)). A sample authorization form is set forth in a statute (Or. Rev. Stat. § 192.566). Such a provider or plan may use or disclose such information without authorization for the provider's or plan's own treatment purposes or as otherwise permitted by state or federal law (Or. Rev. Stat. § 192.558(2)). In addition, a provider or plan may disclose such information without authorization to another covered entity under specified circumstances, primarily for health operations or fraud and abuse prevention (Or. Rev. Stat. § 192.558(3)).

Providers and plans that use or disclose personal information in accordance with the foregoing requirements do not breach a confidential relationship with the individual (Or. Rev. Stat. § 192.568), and these requirements do not create a new private right of action against a provider or plan (Or. Rev. Stat. § 192.571).

Specific provisions apply to health care providers that are participants in a coordinated care organization. Such providers must disclose protected health information to other providers in the program and to the organization itself for operations and payment purposes, and to public health entities for health oversight purposes (Or. Rev. Stat. § 192.561(1)). Such disclosures may be made without patient authorization, but the provision does not apply to psychotherapy notes (Or. Rev. Stat. § 192.561(2)-(3)).

Additional disclosures without authorization: Health care providers may use or disclose protected health information without obtaining an authorization from an individual or representative to family members, close personal friends, other relatives, or other persons identified by the individual when the protected information is relevant to the person's involvement with the individual's care, or where the purpose of the disclosure is to notify a family member, representative, or other responsible person of the location, general condition, or death of the individual (Or. Rev. Stat. § 192.567(1)(A)). However, such disclosure may only be made if the individual is not present or obtaining authorization is not practicable and, in the provider's professional judgment, the provider determines that disclosure is in the best interest of the individual; or if the individual is present, the provider gives the individual an opportunity to object to disclosure and the individual does not express an objection or the provider reasonably infers that the individual does not object (Or. Rev. Stat. § 192.567(1)(b)).

A health care provider may disclose protected health information to a person if the provider believes in good faith that the disclosure is necessary to prevent or lessen a serious threat to the health or safety of any person or the public and the information is disclosed only to a person reasonably able to prevent or lessen the threat, including the target (Or. Rev. Stat. § 192.567(2)). For individuals being treated for mental illness, the protected

information allowed to be disclosed as outlined above may include a variety of information, including diagnoses, issues concerning the individual's safety, resource information, and transition processes (Or. Rev. Stat. § 192.567(3)). All disclosures must be limited to the minimum necessary to accomplish their purpose (Or. Rev. Stat. § 192.567(4)). Providers making disclosures in accordance with these provisions are not subject to civil liability (Or. Rev. Stat. § 192.567(5)).

Authorized charges: Health care providers and state health plans receiving an authorization to disclose protected health information may charge a fee for copies, including bonus charges, as specified by statute, including postage and actual costs for preparing an explanation or summary of protected health information if requested (Or. Rev. Stat. § 192.563).

Miscellaneous provisions: Specific provisions apply to disclosures by covered entities to individuals appealing the denial of social security benefits (Or. Rev. Stat. § 192.576) and allowed disclosures for coordinating care (Or. Rev. Stat. § 192.579).

Notwithstanding specific provisions regarding the maintenance and disclosure of genetic information (see below), health care providers may retain genetic information without obtaining authorization from the individual or representative if the retention is for treatment, payment, or health care operations of the provider (Or. Rev. Stat. § 192.581(1)). In addition, a health care provider may disclose genetic information without authorization to other covered entities if it follows the requirements outlined by law related to health care operations or fraud and abuse detection or compliance (Or. Rev. Stat. § 192.581(2)).

Genetic information and DNA samples: Oregon's genetic privacy laws (Or. Rev. Stat. § 192.533 et seq.) are designed to define individual rights with respect to genetic information; to define when such information may be collected, retained, or disclosed; and to protect against discriminatory activities, among other purposes (Or. Rev. Stat. § 192.533). These provisions are described below.

In general: In general, a person may not obtain genetic information from an individual, or from the individual's DNA sample, without first obtaining the informed consent of the individual or his representative, except as provided by law, as in cases requiring identification under criminal law, for anonymous research, in cases involving deceased individuals or newborn screening or paternity, or for the purpose of furnishing genetic information relating to a decedent for medical diagnosis of a blood relative (Or. Rev. Stat. § 192.535(1)). The law sets forth the procedures for obtaining consent to be followed by physicians, other licensed health care providers and facilities, researchers, and others (Or. Rev. Stat. § 192.535(2)-(5)). Health care providers are subject to additional notice requirements regarding the potential use of biological specimens or other identifiable health information for research purposes (Or. Rev. Stat. § 192.538). In addition, a person may use an individual's DNA sample or genetic information derived from a biological specimen or coded research if the individual was deceased when the specimen or information was obtained (Or. Rev. Stat. § 192.540)).

Maintenance, retention, destruction, access, and correction: An individual's genetic information and DNA sample generally are private and must be protected. Any person authorized either by law or by an individual to obtain, retain, or use the individual's genetic information must maintain the confidentiality of the information from unauthorized disclosure or misuse (Or. Rev. Stat. § 192.537(1)). Genetic information may be used for research purposes only if the individual has granted informed consent for the specific project or for genetic research generally, was notified that the information may be used for research purposes in accordance with law, or was not notified due to legitimate emergency circumstances and the individual died prior to receiving notice (Or. Rev. Stat. § 192.537(2)).

Persons may not retain another individual's genetic information without first obtaining authorization from the

individual, unless a statutory exception applies (Or. Rev. Stat. § 192.537(3)). DNA samples must be promptly destroyed unless retention is authorized by specific state or federal law or by a court, or if they are for specified research purposes (Or. Rev. Stat. § 192.537(4)). Information retained for research purposes must be promptly destroyed on completion of the project or the individual's withdrawal from the project unless the withdrawing individual consents to retention (Or. Rev. Stat. § 192.537(5)). DNA samples taken for employment or insurance purposes must be destroyed promptly after this purpose is accomplished, except if retention is authorized by court order (Or. Rev. Stat. § 192.537(6)).

An individual or representative, promptly upon request, may inspect, request correction of, and obtain genetic records from the record of the individual (Or. Rev. Stat. § 192.537(7)). An individual or representative also may request that a DNA sample be made available for additional testing under specific conditions (Or. Rev. Stat. § 192.537(8)).

Disclosure: In general, a person may not disclose, or be compelled to disclose, the identity of an individual on whom a genetic test has been performed or the identity of a blood relative of the individual, or disclose genetic information about the individual or blood relative in a manner permitting identification, unless disclosure is:

- authorized by federal or state law concerning criminal law;
- required by court order;
- authorized by the tested individual or his representative;
- for the purpose of furnishing genetic information relating to a decedent for medical diagnosis or a blood relative; or
- for the purpose of identifying bodies (Or. Rev. Stat. § 192.539(1)).

The requirements outlined above apply to redisclosures by another person (Or. Rev. Stat. § 192.539(2)). A release or publication is not deemed to be a disclosure for purposes of the prohibition if it involves a good faith belief by the person causing the release that the person was not in violation or if it is not due to willful neglect (Or. Rev. Stat. § 192.539(3)(a)-(b)) In addition, a release will not be considered a disclosure if it is corrected in a manner prescribed by the law governing civil liability for unlawful disclosure (see below and Section I.G.50.), if a correction with respect to genetic information is completed prior to information being read or heard by a third party, and if a correction involving a DNA sample is completed before the sample is retained or tested by a third party (Or. Rev. Stat. § 192.539(3)(c)-(e)).

Regulations and procedures: The Oregon Health Authority is responsible for adopting rules to implement the provisions of the genetic privacy laws, including provisions regarding the establishment and operation of institutional review boards (Or. Rev. Stat. § 192.547(1)-(4)). The Health Authority regulations, which are promulgated at Or. Admin. R. 333-025-0100 et seq., cover informed consent procedures and retention requirements. The law also provides specific procedural provisions regarding the coding of genetic research samples (Or. Rev. Stat. § 192.547(5)-(9)).

Remedies: An individual or his blood relative, representative, or estate may bring a civil action against a person in violation of the above-outlined provisions (Or. Rev. Stat. § 192.541; see Section I.G.50). In addition, violators may be subject to criminal penalties (Or. Rev. Stat. § 192.543; see Section I.H.) and administrative enforcement by the Attorney General or district attorney (Or. Rev. Stat. § 192.545; see Section I.H.).

Public health service providers: In general, written accounts of individuals served by any health care

services provider acting as a public provider are not subject to access and may not be disclosed (Or. Rev. Stat. § 179.505(2)). Exceptions are provided for authorized disclosures, provided that statutory requirements are met (Or. Rev. Stat. § 179.505(3)), as well as for a host of other circumstances (Or. Rev. Stat. § 179.505(4)-(18)). Patients may be charged for reasonable costs for searching, abstracting, and copying, but a patient may not be denied access based on the inability to pay (Or. Rev. Stat. § 179.505(10)).

Individuals aggrieved by a violation of these provisions may bring an action for equitable relief and damages (see Section I.G.50.).

Substance abuse: The records of a person at a treatment facility or sobering center may not be revealed to any person other than the director and staff of the facility or center without the person's consent. A person's request that no disclosure may be made must be honored unless the person is incapacitated or unless disclosure of admission is required because the person is under age 18 or incompetent (Or. Rev. Stat. § 430.399(6) and Or. Rev. Stat. § 430.397).

Minors: For information on the privacy rights of minors with respect to health data, see Section I.D.120.

Cancer and tumor registry system: Identifying information contained in data required to be reported to the Oregon Health Authority for purposes of maintaining the state's cancer and tumor registry system is considered to be confidential and privileged. Except as required by law, no public health official, employee, or agent may be questioned in a proceeding about information concerning such data (Or. Rev. Stat. § 432.530(1)). All other information reported in connection with a special study is similarly confidential and privileged and may only be used for the purposes of the study (Or. Rev. Stat. § 432.530(2)). Certain exceptions apply, including for research purposes and for exchanges with other registries (Or. Rev. Stat. § 432.540).

An action for damages under these provisions may only be undertaken if a disclosure is due to gross negligence or willful misconduct (Or. Rev. Stat. § 432.550; see Section I.G.50.). Note, also, that the Director of the Oregon Heath Authority may impose a civil penalty on any person for failing to comply with the reporting requirements applicable to the cancer and tumor registry (Or. Rev. Stat. § 432.900; see Section II.C.).

Communicable disease reporting: Public health authorities may not disclose the name and address of, or otherwise disclose the identity of, any person reported as having a disease, the reporting of which is required by law, although several exceptions apply, as when necessary for administration of public health law or in cases where a person may have been exposed to a communicable disease (Or. Rev. Stat. § 433.008). A violation is a class A misdemeanor (Or. Rev. Stat. § 433.990(1)).

HIV testing: A person may not disclose, or be compelled to disclose, the identity of any individual on whom an HIV-related test is performed or the results of such a test that permits identification of the subject, except as required or permitted by federal or state law or rule or as authorized by the subject (Or. Rev. Stat. § 443.045(4)(a)). The prohibition does not apply to a person acting in a private capacity, as opposed to an employment, occupational, or professional capacity (Or. Rev. Stat. § 443.045(4)(b)).

Provisions applicable to employers: Employers are prohibited from conducting a variety of testing on employees, including genetic testing; for more information, see Section I.E.60.

Consumer Identity Theft Protection Act: For purposes of the Oregon Consumer Identity Theft Protection Act (CITPA), information about a consumer's medical history or mental or physical condition or about a health care professional's medical diagnosis or treatment of the consumer is defined as “personal information” when used in combination with a person's name, or when used not in combination with a person's name if encryption, redaction, or other methods have not rendered the information unusable, and the information

would enable a person to commit identity fraud against a consumer (Or. Rev. Stat. § 646A.602(11)(a)(G) and Or. Rev. Stat. § 646A.602(11)(b)). Accordingly, such information is subject to CITPA requirements regarding data breach notifications (see Section I.C.80.), security freezes (see Section I.D.40.), data security (see Section I.C.60.), data disposal (see Section I.C.70.), and prohibitions on the display of social security numbers (see Section I.D.100.).

Student Information Privacy Act: For purposes of the restrictions on the collection and disclosure of data on operators of K-12 online services and applications under the Oregon Student Information Privacy Act (SIPA), medical and health records are included in the definition of "covered information" subject to SIPA requirements. For more information, see Section I.E.20.

I.E.60. **HR & Employment** —

Privacy of employee social media account information: It is an unlawful employment practice for an employer to do any of the following:

- require an employee or applicant to establish or maintain a personal social media account or to disclose or provide access to such an account through use of the applicant's or employee's username, password, or other authentication;
- require employees or applicants to authorize the employer to advertise on their personal social media account, or compel them to add the employer or an employment agency to a list of contacts;
- compel an employee or applicant to access a personal social media account in the employer's presence in a manner allowing the employer to view the contents;
- take, or threaten to take, any action to discharge, discipline, or otherwise penalize any employee for refusing to do any of the above-described actions; or
- fail or refuse to hire an applicant based on the applicant's refusal to do any of the above-described actions (Or. Rev. Stat. § 659A.330(1)).

Employers may require employees to disclose any username or password for accessing an account provided by or to be used on behalf of the employer (Or. Rev. Stat. § 659A.320(2)). Employers may not be held liable for failing to request or require employees or applicants to disclose information about their personal social media accounts (Or. Rev. Stat. § 659A.330(3)).

Nothing in the law prohibits employers from conducting investigations, without requiring an employee to provide a username or password, for the purpose of ensuring compliance with applicable laws or prohibitions against work-related employee misconduct involving a personal online account, conducting such an investigation in which username or password information is not requested but an employee is required to share content reported to the employer that is necessary for the employer to make a factual determination, or complying with state and federal law and rules of self-regulatory organizations (Or. Rev. Stat. § 659A.330(4)). In addition, employers may access information available to the public that is accessible through an online account (Or. Rev. Stat. § 659A.330(5)). If an employer inadvertently received a username or password of an employee through the use of an electronic device used for monitoring usage of the employer's network or employer-provided devices, the employer is not liable for having the information but may not use it to access the employee's personal social media account (Or. Rev. Stat. § 659A.330(6)).

Inquiries on criminal convictions: Under provisions regarding the establishment of procedures regarding

criminal record information by the Department of State Police, if such information is sought by an employer for employment purposes, the employer must first have advised the employee or applicant that such information might be sought and must state on making the request that the individual has been advised, together with the manner in which he was notified (Or. Rev. Stat. § 181A.230(2)(b)).

Oregon also has a “ban-the-box” provision that makes it an unlawful practice for an employer to exclude an applicant from an initial interview solely because of a past criminal conviction (Or. Rev. Stat. § 659A.360(1)). Employers commit an unlawful exclusion when they require an applicant to disclose a criminal conviction on an employment application, require an applicant to disclose such a conviction prior to an initial interview, or require an applicant to disclose such a conviction prior to a conditional offer of employment if no interview is conducted (Or. Rev. Stat. § 659A.360(2)). Aside from the above described conditions, Oregon employers are not prevented from considering an applicant's conviction history when making an employment decision (Or. Rev. Stat. § 659A.360(3)). The ban-the-box provisions do not apply if federal, state, or local law requires consideration of an applicant's criminal history, or to employers in law enforcement and criminal justice or employers seeking nonemployee volunteers (Or. Rev. Stat. § 659A.360(4)). Aggrieved employees or applicants may file a complaint with the Bureau of Labor and Industries (see Section II.C.).

Finally, if an employee's juvenile record has been expunged, an employer may not rely on such record for the purposes of making an employment decision, except when the employer demonstrates a bona fide occupational qualification reasonably necessary to the normal operation of the employer's business (Or. Rev. Stat. § 659.030(1)(a)). A person aggrieved by a violation of this provision may bring a civil action (see Section I.G.50.).

Employer inquiries into credit history of applicants and employees: In general, it is an unlawful employment practice for an employer to obtain or use for employment purposes information contained in the credit history of an applicant or employee (Or. Rev. Stat. § 659A.320(1)). This prohibition does not apply to employers who are federally insured banks or credit unions, employers required by state or federal law to use individual credit histories for employment purposes, and specified applications for public safety officers (Or. Rev. Stat. § 659A.320(2)(a)-(c)). In addition, employers may obtain and use information in a credit history if the information is substantially job-related and the employer's reasons for the use of such information are disclosed to the employee or applicant in writing (Or. Rev. Stat. § 659A.320(2)(d)).

Aggrieved employees or applicants may file a complaint with the Bureau of Labor and Industries under Or. Rev. Stat. § 659A.820 (see Section II.C.) or may bring a civil action under Or. Rev. Stat. § 659A.885 (see Section I.G.50.) (Or. Rev. Stat. § 659A.320(3)).

Prohibited testing: It is an unlawful employment practice for an employer to subject any employee to a breathalyzer test, polygraph examination, psychological stress test, genetic test, or brain wave test, as those terms are defined by law (Or. Rev. Stat. § 659A.300(1)-(2)). However, this provision does not prohibit the administration of a polygraph test, if the individual consents to it, in a proceeding in which the employee is a party or witness (Or. Rev. Stat. § 659A.300(3)). Additionally, a breathalyzer test may be conducted if the individual consents to the test or when the employer has reasonable grounds to believe that the individual is under the influence of intoxicating liquor. In the latter instance, the employer may not require the employee to pay for the test (Or. Rev. Stat. § 659A.300(4)). Finally, a genetic test may be administered when an individual or a representative grants informed consent as specified by law and the test is used solely to determine a bona fide occupational qualification (Or. Rev. Stat. § 659A.300(5)).

Persons aggrieved by a violation of this provision may bring a civil action under Or. Rev. Stat. § 659A.885 (see Section I.G.50.).

Genetic information and testing: In addition to the prohibition on genetic tests outlined above, it is an unlawful employment practice for an employer to seek to obtain, or to obtain or use, genetic information of an employee or prospective employee or a blood relative thereof to distinguish between or discriminate against or restrict any right or benefit otherwise due or available to him (Or. Rev. Stat. § 659A.303).

Employment references: An employer who discloses information about a former employee's job performance to another prospective employer on request of the employee or prospective employer is presumed to be acting in good faith and is immune from civil liability for any disclosure unless a lack of good faith is shown by a preponderance of the evidence. In addition, no civil action for defamation may be maintained against an employer by a terminated employee based on a claim that in seeking subsequent employment the former employee will be forced to reveal the reasons given by the employer for the termination (Or. Rev. Stat. § 30.178).

Consumer Identity Theft Protection Act: Employers that own or license data that includes “personal information” as defined under the Oregon Consumer Identity Theft Protection Act (CITPA) are subject to the provisions of the CITPA governing data breach notifications (see Section I.C.80.), security freezes (see Section I.D.40.), data security (see Section I.C.60.), data disposal (see Section I.C.70.), and prohibitions on the display of social security numbers (see Section I.D.100.).

I.E.70. **Insurance** —

Insurance information and privacy protection provisions: Oregon law establishes standards for the collection, use, and disclosure of personal information gathered in connection with insurance transactions by insurers, insurance producers, and insurance support organizations (Or. Rev. Stat. § 746.605). Insurers also are required by regulation to establish and implement an information security program (Or. Admin. R. 836-081-0111). These law and regulatory provisions are outlined in detail below.

Scope and primary definitions: The obligations imposed by the law apply to insurers, producers, and support organizations that, in the case of life and health insurance, collect, receive, or maintain personal information, in connection with insurance transactions, that pertains to Oregon residents, or engage in such transactions with applicants, individuals, or policyholders who are Oregon residents (Or. Rev. Stat. § 746.610(1)(A)), and in the case of other kinds of insurance, collect, receive, or maintain personal information in connection with insurance transactions involving policies or certificates issued in Oregon, or engage in insurance transactions involving policies or certificates issued in Oregon (Or. Rev. Stat. § 746.610(1)(b)). The provisions do not apply to personal information collected from public records for title insurance purposes (Or. Rev. Stat. § 746.610(4)).

“Health information” is defined as oral or written information in any form that is created or received by a covered entity, public health authority, life insurer, school, university, or health care provider that is not a covered entity and that relates to the past, present, or future physical or mental condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual (Or. Rev. Stat. § 746.600(15)). A “covered entity” is a health insurer, health care provider that transmits health information in electronic form to carry out financial or administrative activities in connection with a covered transaction, or a health care clearinghouse (Or. Rev. Stat. § 746.600(8)).

“Individually identifiable health information” means oral or written health information that is created or received by a covered entity or by a health care provider that is not a covered entity that is identifiable to an individual, or for which there is a reasonable basis to believe it can be used to identify the individual, that relates to the past, present, or future physical or mental condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual (Or. Rev.

Stat. § 746.600(19)). “Personal financial information” includes information that is identifiable with an individual, gathered in connection with an insurance transaction, from which judgment can be made about an individual's character, habits, avocations, finances, occupations, general reputation, credit or other personal characteristics, or an individual's name, address, and policy number or similar access code (Or. Rev. Stat. § 746.600(31)(a)), but does not include information a licensee has reason to believe is lawfully made available to the general public from federal, state, or local government records, widely distributed media, or disclosures to the public required by federal, state, or local law (Or. Rev. Stat. § 746.600(31)(b)). “Protected health information” means individually identifiable health information transmitted or maintained in any form of electronic or other medium by a covered entity but does not include education records covered by federal Family Educational Rights and Privacy Act (FERPA) provisions, records described in Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule provisions, or employment records held by a covered entity in its role as an employer (Or. Rev. Stat. § 746.600(38)).

“Personal information” includes personal financial information, individually identifiable health information, and protected health information as outlined above (Or. Rev. Stat. § 746.600(32)).

Initial and annual notices: Licensees must provide an initial notice of personal information practices to a customer no later than when a customer relationship is established, but such notice may be delayed by a reasonable time after this date if the customer relationship is not established at the customer's election or if providing notice as of that date would substantially delay the customer's transaction. Notice to a consumer other than a customer must be provided before the licensee discloses any personal information pursuant to requirements of the law (Or. Rev. Stat. § 746.620(1)).

Licensees must provide notice accurately reflecting its privacy policy and practices to every customer at least annually (Or. Rev. Stat. § 746.620(2)). The initial or annual notice must be in writing, clear, and conspicuous. It may be delivered electronically if the recipient agrees and must include the categories of personal information that the licensee collects and discloses, the categories of affiliates and nonaffiliated third parties to whom the licensee discloses personal information, the categories of personal information of former customers that the licensee discloses and the parties to whom they are disclosed, a separate description of the categories actually disclosed if a disclosure has been made, and explanations of a customer's rights to authorize disclosure or to access and correct personal information, among other items (Or. Rev. Stat. § 746.620(3)).

If a licensee discloses personal information as authorized under an exception to a prohibition on disclosure, it is not required to list the exceptions on a privacy notice. It must state only that the licensee makes disclosures to other affiliated or nonaffiliated parties as authorized by law (Or. Rev. Stat. § 746.620(4)). In lieu of the notice outlined above, the licensee may provide abbreviated notice under specified circumstances (Or. Rev. Stat. § 746.620(5)). The Director of the Department of Consumer and Business Services has the authority to issue regulations establishing specific requirements regarding notices (Or. Rev. Stat. § 746.620(6)-(7)) and has done so at Or. Admin. R. 836-080-0511 through Or. Admin. R. 836-080-0531.

Marketing and research surveys: An insurer or insurance producer must clearly identify any questions that are designed to obtain personal information solely for marketing or research purposes (Or. Rev. Stat. § 746.625). The regulations impose further restrictions on licensees with respect to sharing account number information for marketing purposes (Or. Admin. R. 836-080-0546).

Disclosure authorization requirements: An authorization form used by a licensee or insurance support organization must contain all of the following:

- the identity of the subject;

- a general description of the categories of personal information to be disclosed;
- general descriptions of the parties to whom the licensee discloses personal information, the purpose of disclosure, and how the information may be used;
- the signature of the subject or a legally empowered representative; and
- notice of the length of time for which the authorization is valid, that the individual may revoke it at any time, and the procedure for revocation (Or. Rev. Stat. § 746.630(1)).

Authorizations may not be valid for more than 24 months (Or. Rev. Stat. § 746.630(2)). The individual may revoke an authorization at any time, subject to the rights of an individual who acted in reliance on an authorization prior to notice of its revocation (Or. Rev. Stat. § 746.630(3)). Licensees must maintain the authorization in the record of the subject (Or. Rev. Stat. § 746.630(4)). The regulations specify that a request for authorization and an authorization form may be delivered to a consumer or customer as part of an initial notice if the request and authorization form are clear and conspicuous (Or. Admin. R. 836-080-0551).

Limitations and conditions on disclosure: A licensee or insurance support organization may not disclose any personal or privileged information about an individual collected or received in connection with an insurance transaction unless the disclosure is with the written authorization of the individual and, if the authorization is submitted by another licensee or insurance support organization, it meets the authorization requirements outlined above, or, if the authorization is submitted by a person other than a licensee or insurance support organization, it is dated, signed by the individual, and obtained one year or less prior to the date disclosure is sought (Or. Rev. Stat. § 746.665(1)(a)).

Additional disclosures are permitted in a variety of circumstances, including to a person other than a licensee or insurance support organization to perform a business, professional, or insurance function of the disclosing entity or to provide information for determining eligibility or detecting or preventing criminal activity or fraud; to a licensee, insurance support organization, or self-insurer when reasonably necessary to detect or prevent criminal activity or fraud or when necessary for the licensee or organization to perform its function in connection with an insurance transaction; to a heath care provider for purposes of verifying coverage or benefits, informing an individual of a medical problem, or conducting an audit; to insurance regulators and law enforcement authorities; as otherwise permitted by law or required by court order, search warrant, or subpoena; or for specified research purposes (Or. Rev. Stat. § 746.665(1)(b)-(i)). Disclosures also are permitted pursuant to a sale of the business of a licensee, or to a nonaffiliated third party solely in connection with the marketing of a product or service, or to an affiliated party for such purposes, subject to specified requirements (Or. Rev. Stat. § 746.665(j)-(l)). [Note: the regulations specify the form and content of opt-out notices associated with respect to disclosures made specifically for marketing purposes; see Or. Admin. R. 836-080-0541]. Finally, the law allows for disclosures by consumer reporting agencies, to group policyholders, to professional peer review organizations, to government authorities, and to policyholders and certificate holders under specified conditions (Or. Rev. Stat. § 746.665(1)(m)-(q)).

Personal or privileged information also may be acquired by a group practice prepayment health care service contractor and may be transferred among providers contracting with the contractor for purposes of administering the plans offered by the contractor, provided that the contractor may not disclose information for other purposes except as allowed by law (Or. Rev. Stat. § 746.665(2)).

Access and correction: An insurer, insurance producer, or insurance support organization that receives a written request from an individual, accompanied by appropriate identification, for access to recorded personal

information about the individual that is reasonably described, locatable, and retrievable must, within 30 business days of receiving the request:

- inform the individual of the nature and substance of the recorded personal information in writing, by telephone, or by other oral communication, at the discretion of the insurer;
- permit the individual to see and copy the information in person or to obtain a copy by mail, whichever the individual prefers, or provide an accurate translation in writing and in plain language if the information is encoded;
- disclose the identity of other persons to whom the insurer has disclosed the information in the past two years, or if such information is not recorded, the names of insurers, insurance producers, and other persons to whom such information is usually disclosed; and
- provide the individual with a summary of procedures by which he may request correction, amendment, or deletion of the information (Or. Rev. Stat. § 746.640(1)).

If the source of personal information is an institutional source, the insurer must identify the source (Or. Rev. Stat. § 746.640(2)). If an individual requests individually identifiable health information supplied by a health care provider, the insurer must provide the information, including the identity of the health care provider, either to the individual or a health care provider designated by the individual, whichever the insurer prefers. If the insurer elects to disclose to a health care provider, it must notify the individual at the time of disclosure (Or. Rev. Stat. § 746.640(3)). Insurers may charge a reasonable fee for providing copies unless the information is provided as a result of an adverse underwriting decision (Or. Rev. Stat. § 746.640(4)).

Within 30 business days of receiving a request from an individual to correct, amend, or delete any recorded personal information in its possession, the insurer, insurance producer, or insurance support organization must either correct, amend, or delete the disputed information, or notify the individual of its refusal to make the correction, amendment, or deletion, the reasons for the refusal, and the individual's right to file a statement (Or. Rev. Stat. § 746.645(1)). In the event of a correction, amendment, or deletion, the insurer must notify the individual in writing and furnish the correction, amendment, or deletion to each person designated by the individual who may have received the personal information within the past two years, to each insurance support organization whose primary source of personal information is insurers if the organization has been systematically receiving information from the insurer for the past seven years, unless the organization no longer maintains personal information about the individual, and to each insurance support organization that furnished the subject information (Or. Rev. Stat. § 746.645(2)).

An individual disagreeing with a refusal to correct, amend, or delete recorded information may file with the insurer, insurance producer, or insurance support organization a concise statement setting forth what the individual thinks is correct, relevant, or fair information, and a concise statement of the reason why the individual disagrees with the refusal to correct, amend, or delete (Or. Rev. Stat. § 746.645(3)). If the individual files either or both statements, the insurer, insurance producer, or insurance support organization must file the statements with the disputed information and provide a means by which anyone reviewing the file will be aware of the statement and have access to them. Additionally, in any subsequent disclosure, the insurer, insurance producer, or insurance support organization must clearly identify the matter or matters in dispute and provide the statements. Finally, the insurer, insurance producer, or insurance support organization must furnish the statements in the same manner they are required to provide notice to individuals and natural persons of a correction as outlined above (Or. Rev. Stat. § 746.645(4)).

Specific provisions regarding health insurers: The provisions outlined above regarding initial and annual privacy notices, authorization for disclosure of information, access to information, correction of information, and limits on disclosure do not apply to health insurers (Or. Rev. Stat. § 746.609). Instead, health insurers are subject to specific provisions governing permissible uses and disclosures. In general, a health insurer may use or disclose personal information of an individual in a manner that is consistent with an authorization provided by the individual or his personal representative (Or. Rev. Stat. § 746.607(1)). A health insurer may use or disclose protected health information without such authorization for the insurer's own treatment, payment, or health care operations, or as otherwise permitted or required by state or federal law or court order (Or. Rev. Stat. § 746.607(2)). Disclosures of protected health information without authorization also are permitted, subject to federal and state regulatory requirements, to another covered entity for health care operations of that entity, provided that each entity had or has a relationship with the subject individual, the protected health information pertains to the relationship, and the disclosure is for purposes of specified health care operations or health care fraud and abuse detection or compliance (Or. Rev. Stat. § 746.607(3)(a)), or to another covered entity or health care provider for specified treatment or payment purposes (Or. Rev. Stat. § 746.607(3)(b)-(c)). A health insurer may use or disclose personal financial information to perform a business, professional, or insurance function, subject to regulatory authorization requirements, or without obtaining authorization as otherwise permitted by federal or state law or court order (Or. Rev. Stat. § 746.607(4)).

The law permits health insurers to charge reasonable, cost-based fees for copying personal information requested by an individual, including postage and the costs of preparing an explanation or summary of personal information if requested (Or. Rev. Stat. § 746.607(5)). Health insurers also must provide adequate notice of the uses and disclosures of personal information that may be made and of the individual's rights and the health insurer's duties with respect to personal information (Or. Rev. Stat. § 746.607(6)). Finally, a health insurer must permit an individual or personal representative to request access to inspect or obtain a copy of personal financial information or protected health information maintained by the insurer, and must permit requests for corrections, amendments, or deletions of personal information (Or. Rev. Stat. § 746.607(7)).

A health insurer may retain genetic information of an individual without authorization if the retention is for treatment, payment, or health care operations of the insurer (Or. Rev. Stat. § 746.632(1)). In addition, such information may be disclosed without authorization if the health insurer discloses it to other covered entities as outlined above (Or. Rev. Stat. § 746.632(2)).

The law requires the Director of the Department of Consumer and Business Services to adopt rules implementing the use and disclosure requirements applicable to health insurers (Or. Rev. Stat. § 746.608). These rules are promulgated at Or. Admin. R. 836-080-0615 through Or. Admin. R. 836-080-0700 and expand on and clarify the notice, use, and disclosure provisions discussed above. These rules contain provisions similar to those outlined above for licensees regarding notices, authorizations, opt-in notices, and permitted disclosures.

Enforcement: The Director of the Department of Consumer and Business Services may investigate violations of any of the above requirements (Or. Rev. Stat. § 746.670). In addition, any person whose right to access or correct personal information is violated may file an action in circuit court for appropriate equitable relief, and licensees who violate the provisions of the law regarding use or disclosure of information may be liable for actual damages (see Section I.G.10.).

Implementation of information security program: The regulations require licensees to implement a comprehensive written information security program that includes administrative, technical, and physical safeguards for the protection of customer information. The safeguards must be appropriate to the size and complexity of the licensee and the scope of its activities (Or. Admin. R. 836-081-0111)). The program must

ensure the security and confidentiality of customer information, protect against anticipated threats to the security or integrity of the information, and protect against unauthorized access or use of information that could result in substantial harm or inconvenience for the customer (Or. Admin. R. 836-081-0116). Examples of methods of development and implementation are set forth (Or. Admin. R. 836-081-0121). A violation of the requirements is an unfair trade practice under Oregon insurance law (Or. Admin. R. 836-081-0126).

Consumer Identity Theft Protection Act: For purposes of the Oregon Consumer Identity Theft Protection Act (CITPA), a consumer's health insurance policy number or subscriber identification number, in combination with any other unique identifier that a health insurer uses to identify the consumer, is defined as “personal information” when used in combination with a person's name, or when used not in combination with a person's name if encryption, redaction, or other methods have not rendered the information unusable, and the information would enable a person to commit identity fraud against a consumer (Or. Rev. Stat. § 646A.602(11)(a)(F) and Or. Rev. Stat. § 646A.602(11)(b)). Accordingly, such information, and any other information included in the definition of “personal information” under the CITPA, is subject to CITPA requirements regarding data breach notifications (see Section I.C.80.), security freezes (see Section I.D.40.), data security (see Section I.C.60.), data disposal (see Section I.C.70.), and prohibitions on the display of social security numbers (see Section I.D.100.).

I.E.80. **Retail & Consumer Products** —

Consumer Identity Theft Protection Act: Businesses engaged in the retail and consumer products sector that own or license data that includes “personal information” as defined under the Oregon Consumer Identity Theft Protection Act (CITPA) are subject to the provisions of the CITPA governing data breach notifications (see Section I.C.80.), security freezes (see Section I.D.40.), data security (see Section I.C.60.), data disposal (see Section I.C.70.), and prohibitions on the display of social security numbers (see Section I.D.100.).

I.E.90. **Social Media** —

Privacy of employee and student social media account information: In general, it is an unlawful employment practice for an employer to require employees or applicants to provide access to their personal social media accounts or to take punitive action against employees, or refuse to hire applicants, based on their refusal to provide such access. For a comprehensive discussion of these requirements, see Section I.E.60.

Similar restrictions apply to educational institutions with respect to social media accounts of students and prospective students (see Section I.E.20.).

Consumer Identity Theft Protection Act: Businesses engaged in the social media sector that own or license data that includes “personal information” as defined under the Oregon Consumer Identity Theft Protection Act (CITPA) are subject to the provisions of the CITPA governing data breach notifications (see Section I.C.80.), security freezes (see Section I.D.40.), data security (see Section I.C.60.), data disposal (see Section I.C.70.), and prohibitions on the display of social security numbers (see Section I.D.100.).

I.E.100. **Tech & Telecom** —

Consumer Identity Theft Protection Act: Businesses engaged in the tech and telecommunications sector that own or license data that includes “personal information” as defined under the Oregon Consumer Identity Theft Protection Act (CITPA) are subject to the provisions of the CITPA governing data breach notifications (see Section I.C.80.), security freezes (see Section I.D.40.), data security (see Section I.C.60.), data disposal (see Section I.C.70.), and prohibitions on the display of social security numbers (see Section I.D.100.).

Security of Connected Devices: Or Rev. Stat. § ORS 646A.813(1)(c) requires manufacturers of Internet-connected devices to equip their devices with "reasonable security features," which are defined as "methods to protect a connected device, and any information or disclosure that are appropriate for the nature and function of the connected device and for the type of information the connected device may collect, store or transmit (H.B. 4155)".

Although the law does not provide any definitive standard of what constitutes "reasonable security features," the law does provide that a reasonable security feature *may* consist of: (1) a means for authentication from outside a local area network, including: (a) a preprogrammed password that is unique for each connected device; or (b) a requirement that a user generate a new means of authentication before gaining access to the connected device for the first time; or (2) compliance with requirements of federal law or federal regulations that apply to security measures for connected devices (Or Rev. Stat. § ORS 646A.813(2)).

The law also provides that it does *not* do any of the following: (1) require a provider of an electronic store, gateway, marketplace, or other means for purchasing or downloading software or firmware to verify or enforce compliance with the law; (2) require a person to prevent a consumer from having or obtaining full control over a connected device, including the ability to modify the connected device or any software or firmware installed on the connected device; (3) limit the authority of a law enforcement officer or law enforcement agency to obtain information from a manufacturer as provided by law or authorized in an order from a court of competent jurisdiction; or (4) impose a duty on a manufacturer to provide reasonable security features for software, firmware, or peripheral devices that another manufacturer makes and that a consumer installs in or adds to the connected device (Or Rev. Stat. § ORS 646A.813(3)).

Net Neutrality: Public bodies may not contract with broadband Internet service providers who engage in specified activities such as paid prioritization or content blocking (H.B. 4155).

I.E.110. **Other Sectors** —

Our research has revealed no specific Oregon law provisions applicable to other business sectors.

I.F. **Electronic Surveillance** —

In general, procedures for the permissible interception of communications in Oregon are governed by criminal procedure law relating primarily to interceptions by law enforcement officials as permitted by court order or under other specified circumstances (see Or. Rev. Stat. § 133.721 to Or. Rev. Stat. § 133.739). Any person whose wire, electronic, or oral communication was intercepted, disclosed, or used in violation of these provisions has a civil cause of action against any person who willfully intercepts, discloses, or uses the communication or procures another to do so and may recover damages (see Section I.G.50.).

Under Oregon criminal law provisions, unless a person is in compliance with the communication interception requirements outlined above (specifically, Or. Rev. Stat. § 133.724 and Or. Rev. Stat. § 133.726), a person may not obtain or attempt to obtain the whole or any part of a telecommunication or a radio communication to which the person is not a participant, by any means, unless consent is given by at least one participant (Or. Rev. Stat. § 165.540(1)(a)). Additional restrictions apply to tampering with equipment over which messages are transmitted; to obtaining any part of a conversation if not all participants are specifically informed that the conversation is being obtained; to obtaining a conversation, telecommunication, or radio communication while knowing or having good reason to believe that the conversation or communication was obtained in an illegal manner; or to using or divulging the contents of a conversation or communication obtained in violation (Or. Rev. Stat. § 165.540(1)(b)-(e)).

A number of exceptions apply to the prohibitions outlined above, including interceptions performed for the purposes

of construction or maintenance by telecommunications providers; subscribers performing the otherwise prohibited acts in their homes; broadcasts transmitted for use of the general public; communications involving specified criminal activity; communications that are part of public meetings, educational activities, or private meetings if all involved know or should have known a recording was being made; and citizen's band or government communication system transmissions (Or. Rev. Stat. § 165.540(2)-(7)).

A person who violates the prohibition on obtaining the contents of a communication, or an employee, agent, or officer of a telecommunications provider who obtains information and subsequently discloses it for any purpose other than construction or maintenance purposes, is guilty of a class A misdemeanor (Or. Rev. Stat. § 165.540(8)).

A separate criminal law provision specifies that any person who willfully intercepts, attempts to intercept, or procures another to intercept or attempt to intercept any wire or oral communication where such person is not a party to the communication and where none of the parties to the communication has given consent to the interception is guilty of a class A misdemeanor (Or. Rev. Stat. § 165.543(1)). Accordingly, Oregon is a “one-party consent” state.

I.G. **Private Causes of Action**

I.G.10. **Consumer Protection** —

Disclosures of customer information to state or local agencies by financial institutions: A customer who suffers any ascertainable loss as a result of a willful violation of provisions prohibiting financial institutions from disclosing financial information to state or local agencies unless an exception applies may bring an action to recover actual damages or $1,000, whichever is greater (Or. Rev. Stat. § 192.606(1)). A similar action for a negligent violation may be brought to recover actual damages (Or. Rev. Stat. § 192.606(2)). A court may award reasonable attorney fees to the prevailing party, but such fees may not be awarded to the state or a political subdivision of the state (Or. Rev. Stat. § 192.606(3)). An action must be commenced within two years after the date of the violation (Or. Rev. Stat. § 192.606(4)).

Social security number disclosure by Department of Transportation: A person aggrieved by a violation involving the impermissible disclosure of a social security number (SSN) by the Department of Transportation or a redisclosure of an SSN by another agency (see Section I.D.100.) may bring a civil action against the person in violation and may recover actual damages or $2,500, whichever is greater, plus attorney fees and costs (Or. Rev. Stat. § 802.195(8)).

Disclosures of social security numbers by public universities and community colleges: A student who suffers an ascertainable loss of money, personal property, or real property as a result of a violation of provisions prohibiting the disclosure of SSNs by public universities and community colleges (see Section I.E.20.) may bring an action to recover the student's actual damages. The court also may award reasonable attorney fees to a prevailing party in such an action (Or. Rev. Stat. § 326.591).

Improper access to student social media accounts by educational institutions: A student aggrieved by a violation of provisions prohibiting educational institutions from requiring access to his personal social media accounts (see Section I.E.20.) may bring a civil action for equitable relief, damages (subject to limitations on liability for specified public bodies and officers), or both. Damages will be $200 or actual damages, whichever is greater, and the court may award other relief as appropriate (Or. Rev. Stat. § 326.554(1)). An action must be filed within one year of filing a grievance with the governing body of an educational institution and may not be filed unless such a grievance has been filed within 180 days of the alleged violation, among other procedural requirements (Or. Rev. Stat. § 326.554(2)-(6)). The court must award reasonable attorney fees to a prevailing

plaintiff and may award such fees to a prevailing defendant if, in the court's judgment, there was not objectively reasonable basis for the claim or for the appeal of an adverse decision of a trial court (Or. Rev. Stat. § 326.554(7)).

Disclosure of personal information by insurers: A licensee or insurance support organization that discloses information in violation of requirements restricting such disclosures, or a health insurer who violates provisions regarding disclosure specifically applicable to it (see Section I.E.70.), is liable for damages sustained by the individual about whom the information relates. However, individuals are not entitled to a monetary award exceeding actual damages (Or. Rev. Stat. § 746.680(2)). The court may award attorney fees to a prevailing party (Or. Rev. Stat. § 746.680(3)). An action must be brought within two years of the date the alleged violation is or should have been discovered (Or. Rev. Stat. § 746.680(3)).

I.G.20. **Identity Theft** —

In general: A person commits identity theft if the person, with the intent to deceive or defraud, obtains, possesses, transfers, creates, utters, or converts to the person's own use the personal identification of another person. The crime of identity theft is a class C felony (Or. Rev. Stat. § 165.800(1)-(2)). Persons under age 21 using the personal identification to purchase alcohol, tobacco products, or inhalant delivery systems or to misrepresent the person's age to obtain access to an age-restricted place or benefit have an affirmative defense to a violation (Or. Rev. Stat. § 165.800(3)). “Personal identification” is defined as any written document or electronic data that provides, or purports to provide, a variety of information, including name, address, telephone number, driving privileges, social security number (SSN) or tax ID number, depositor account numbers, and e-mail names and signatures, among others (Or. Rev. Stat. § 165.800(4)(b)).

A person commits aggravated identity theft if he violates the above prohibitions under the following circumstances:

- in 10 or more incidents within a 180-day period;
- where the person has a previous conviction for aggravated identity theft;
- the losses incurred in a single or aggregate transaction are $10,000 or more within a 180-day period; or
- the violator has in his custody 10 or more pieces of personal identification from 10 or more different persons (Or. Rev. Stat. § 165.803(1)).

Aggravated identity theft is a class B felony (Or. Rev. Stat. § 165.803(2)).

Breach notifications: For information regarding requirements governing security breach notifications under the Oregon Consumer Identity Theft Protection Act, see Section I.C.80.

Data security: For information regarding data security requirements imposed on businesses under the Oregon Consumer Identity Theft Protection Act, see Section I.C.60.

Social security numbers: For information regarding requirements governing the display of SSNs by specified persons under the Oregon Consumer Identity Theft Protection Act, see Section I.D.100.

I.G.30. **Invasion of Privacy** —

Private cause of action: A plaintiff has a cause of action for invasion of personal privacy if he can show any

of the following:

- The defendant knowingly made or recorded a photograph, motion picture, videotape, or other visual recording of the plaintiff in a state of nudity without the consent of the plaintiff and in an area where the plaintiff had a reasonable expectation of personal privacy;

- The defendant was in a location to observe the plaintiff, for purposes of sexual arousal or gratification, in a state of nudity without the consent of the plaintiff and in an area where the plaintiff had a reasonable expectation of personal privacy;

- For purposes of sexual arousal or gratification, the defendant knowingly made or recorded a photograph, motion picture, videotape, or other visual recording of an intimate area of the plaintiff, or viewed such an area, without the plaintiff's consent;

- Without the plaintiff's consent, the defendant disseminated a photograph, motion picture, videotape, or other visual recording of the plaintiff in a state of nudity, and the defendant knew that the plaintiff was in a place and circumstances where the plaintiff had a reasonable expectation of personal privacy (Or. Rev. Stat. § 30.865(1)).

A plaintiff who prevails in an action for invasion of physical privacy is entitled to receive compensatory damages and reasonable attorney fees (Or. Rev. Stat. § 30.865(2)). An action must be commenced within two years after the conduct occurred (Or. Rev. Stat. § 30.865(3)).

An exception to the violation of knowingly making a visual recording of an individual in a state of nudity or disseminating such a recording is available if the subject is under age 12 and the person who makes or disseminates the recording is the father, mother, sibling, grandparent, aunt, uncle, or first cousin, by blood, adoption, or marriage, of the subject, and the recording is made for a purpose other than sexual arousal or gratification (Or. Rev. Stat. § 30.865(5)).

Criminal provisions: A person commits the crime of invasion of personal privacy in the second degree if, for the purpose of sexual arousal or gratification, the person is in a location to observe another person in a state of nudity without his consent, and where the other person has a reasonable expectation of privacy, or the person knowingly makes or records a photograph, motion picture, videotape, or other visual recording of another person's intimate area without his consent and the person being recorded has a reasonable expectation of privacy concerning the intimate area (Or. Rev. Stat. § 163.700(1)). Invasion of personal privacy in the second degree is a class A misdemeanor (Or. Rev. Stat. § 163.700(3)).

A person commits the crime of invasion of personal privacy in the first degree if the person knowingly makes or records a photograph, motion picture, videotape, or other visual recording of another person in a state of nudity without his consent and the person being recorded is in a place in which he has a reasonable expectation of privacy (Or. Rev. Stat. § 163.701(1)(a)). In addition, a person committing an action constituting invasion of personal privacy in the second degree who, at the time of the offense, has a conviction for invasion of personal privacy in any degree, public indecency, private indecency, or a sex crime, or an equivalent offense in another jurisdiction, is guilty of invasion of personal privacy in the first degree (Or. Rev. Stat. § 163.701(1)(b)). Invasion of personal privacy is a class C felony and is classified as crime category 6 for purposes of Oregon sentencing guidelines (Or. Rev. Stat. § 163.701(2)). In addition, a court may designate invasion of personal privacy in the first degree as a sex crime if the court determines that the circumstances of the offense require the offender to register and report as a sex offender (Or. Rev. Stat. § 163.701(3)).

Exceptions to the provisions outlined above apply to legitimate medical procedures performed by or under the

supervision of licensed medical personnel, and any activity related to bona fide law enforcement or corrections activity or necessary to the proper functioning of the criminal justice system (Or. Rev. Stat. § 163.702(1)). In addition, the provisions related to an invasion of privacy in the first degree regarding visual recordings do not apply to recordings of a subject under age 12 if the recording is taken by the father, mother, sibling, grandparent, aunt, uncle, or first cousin, by blood, adoption, or marriage, of the subject, and the recording is made for a purpose other than sexual arousal or gratification (Or. Rev. Stat. § 163.702(2)).

Anti-Doxxing. On June 15, 2021, Oregon passed a new “anti-doxxing” law criminalizing the dissemination of personal information online with the intent of stalking, harassing, or otherwise injuring another person (HB 3047). The law defines personally identifying information as:

- a person's home address, personal email address, personal phone number or social security number;
- contact information for the person's employer;
- contact information for a family member of the person;
- photographs of the individual's children; or
- identification of the school that the person's children attend.

Plaintiffs may recover economic and noneconomic damages, punitive damages, injunctive relief, and attorney's fees.

I.G.40. **Computer Hacking** —

A person commits computer crime under Oregon law when the person knowingly accesses, attempts to access, uses, or attempts to use any computer, computer system, computer network, or any part thereof to devise or execute a scheme or artifice to defraud; obtain money, property, or services by means of false or fraudulent pretenses, representations, or promises; or commit theft, including, but not limited to, theft of proprietary information or intimate images (Or. Rev. Stat. § 164.377(2)). It is also a computer crime to knowingly and without authorization alter, damage, or destroy any computer, computer system, computer network, or any computer software or specific component thereof, or to knowingly and without authorization use, access, or attempt to access such a computer, network, system, or software (Or. Rev. Stat. § 164.377(3)-(4)).

A computer crime violation involving knowing access or use to defraud, obtain money, or commit theft is a class C felony. A violation involving use, access, or attempted access knowingly or without authorization is generally a class A misdemeanor (Or. Rev. Stat. § 164.377(5)(a)). However, any violation of the computer crime law involving a computer, network, program, software, or data owned or operated by the Oregon State Lottery or another person under contract with the lottery is a class C felony (Or. Rev. Stat. § 164.377(5)(b)).

I.G.50. **Other Causes of Action** —

Genetic information: A person aggrieved by a violation of laws governing the collection, maintenance, and disclosure of genetic information and DNA samples (see Section I.E.50.) may bring a civil action.

For a violation involving an individual's rights to privacy in such information or the maintenance, retention, or destruction of such information, or of provisions governing rules adopted by the Oregon Health Authority, the court must award the greater of actual damages or the following amounts: $100 for an inadvertent violation not arising out of the negligence of the defendant, $500 for a negligent violation, $10,000 for a knowing or reckless

violation, $15,000 for a knowing violation based on fraudulent misrepresentations, or $25,000 for a knowing violation committed with the intent to sell, transfer, or use for commercial advantage, personal gain, or malicious harm (Or. Rev. Stat. § 192.541(2)).

For a violation involving a failure to obtain informed consent from an individual prior to collecting genetic information or for unlawfully disclosing such information, the court must award the greater of actual damages or the following amounts: $1,000 for an inadvertent violation not arising out of the negligence of the defendant, $5,000 for a negligent violation, $100,000 for a knowing or reckless violation, $150,000 for a knowing violation based on fraudulent misrepresentations, or $250,000 for a knowing violation committed with the intent to sell, transfer, or use for commercial advantage, personal gain or malicious harm (Or. Rev. Stat. § 192.541(3)).

The damages described above apply to each violation by a defendant (Or. Rev. Stat. § 192.541(8)).

The defendant has an affirmative defense if he corrected the violation through the destruction of illegally retained or obtained samples or information or took other corrective action if the destruction or action was completed within 120 days after the defendant knew or should have known the violation occurred (Or. Rev. Stat. § 192.541(4)). The court may award equitable relief and attorney fees as prescribed by law (Or. Rev. Stat. § 192.541(5)-(6)). An action must be commenced within three years after the date the plaintiff knew, or should have known, of the violation, but in no case later than 10 years after the date of the violation (Or. Rev. Stat. § 192.541(7)).

Disclosures by providers of public health services: An individual or his representative may commence an action for equitable relief regarding requirements related to the disclosure of written accounts of treatment by a health care service provider acting as a public provider (see Section I.E.50.) in the circuit court where the individual resides or where the written accounts are stored. In such an action, the court must order payment or reasonable attorney fees at trial and on appeal, as well as actual disbursements to the prevailing party (Or. Rev. Stat. § 179.507(1)). A similar action may be commenced for damages and to restrain future violations. If the violation is proven, the individual will recover the greater of actual damages or $500. On showing an intentional violation, the individual may receive punitive damages. The prevailing party receives attorney fees and costs (Or. Rev. Stat. § 179.507(2)).

Disclosure of cancer registry information: In general, no action for damages for the disclosure of confidential or privileged information arising from a violation of provisions governing information submitted to Oregon's cancer and tumor registry system (see Section I.E.50.) may be maintained against any person acting in good faith in such reporting (Or. Rev. Stat. § 432.550(1)). However, this provision may not be construed to apply to the unauthorized disclosure of such information due to gross negligence or willful misconduct (Or. Rev. Stat. § 432.550(3)).

Employer inquiries into credit history of applicants and employees: Employees or applicants aggrieved by a violation of provisions prohibiting employers from inquiring into their credit histories (see Section I.E.60.) may bring a civil action in circuit court under Or. Rev. Stat. § 659A.885 (Or. Rev. Stat. § 659A.320(3)). In such an action, the court may order injunctive relief and any other appropriate relief, including reinstatement of an employee with or without back pay (Or. Rev. Stat. § 659A.885(1)).

Employer reliance on expunged juvenile record: A person aggrieved by a violation of the provisions of employment discrimination law prohibiting the use of an expunged juvenile record in an employment decision (see Section I.E.60.) may bring a civil action in which a court may order injunctive relief and any other appropriate relief, including reinstatement of an employee with or without back pay (Or. Rev. Stat. § 659A.885(1)-(2)). In addition to this relief, in an action making such a claim, the court may award

compensatory damages or $200, whichever is greater, and punitive damages (Or. Rev. Stat. § 659A.885(3)(a)). In addition, the action may be tried by jury at the request of any party, appeals may be taken to the appellate court pursuant to standards specified by law, and any attorney fee agreement is subject to court approval (Or. Rev. Stat. § 659A.885(3)(b)-(d)).

Electronic surveillance: A person whose wire, electronic, or oral communication was intercepted, disclosed, or used in violation of law (see Section I.F.) has a civil cause of action against any person who willfully intercepts, discloses, or uses the communication or procures another to do so and may recover actual damages, but not less than damages computed at the rate of $100 per day for each violation or $1,000, whichever is greater, and punitive damages (Or. Rev. Stat. § 133.739(1)). Good faith reliance on a court order or legislative authorization is an absolute defense to an action (Or. Rev. Stat. § 133.739(2). The court may award reasonable attorney fees to a prevailing party, unless the prevailing party is a defendant and the action was maintained as a class action under Oregon Rules of Civil Procedure (Or. Rev. Stat. § 133.739(4)-(5)).

Disclosure of educational records: A person claiming to be aggrieved by the reckless disclosure of personally identifiable information from a student's educational record as prohibited by standards issued by the State Board of Education or the governing board of a public university may file an action for equitable relief or damages, or both. The court may order other relief as it deems appropriate (Or. Rev. Stat. § 30.864(1)). Such an action must be filed within two years of the alleged unlawful disclosure (Or. Rev. Stat. § 30.864(2)). A prevailing party may be awarded costs, disbursements, and reasonable attorney fees (Or. Rev. Stat. § 30.864(3)).

Invasion of personal privacy: A private cause of action is available for plaintiffs who allege an invasion of their personal privacy; for more information, see Section I.G.30.

I.H. **Criminal Liability** —

Genetic information: A person commits the crime of unlawfully obtaining, retaining, or disclosing genetic information if the person knowingly, recklessly, or with criminal negligence obtains, retains, or discloses information in violation of Oregon's genetic privacy law (see Section I.E.50.). This crime is a class A misdemeanor (Or. Rev. Stat. § 192.543)).

Communicable disease reporting: Public health authorities may not disclose the name and address of, or otherwise disclose the identity of, any person reported as having a disease, the reporting of which is required by law, although several exceptions apply, as when necessary for administration of public health law or in cases where a person may have been exposed to a communicable disease (Or. Rev. Stat. § 433.008). A violation is a class A misdemeanor (Or. Rev. Stat. § 433.990(1)).

Social security number disclosure by Department of Transportation: A violation of provisions involving the impermissible disclosure of a social security number (SSN) by the Department of Transportation or a redisclosure of an SSN by another agency (see Section I.D.100.) is a class A misdemeanor (Or. Rev. Stat. § 802.195(7)).

Electronic surveillance: See Section I.F.

Invasion of personal privacy: See Section I.G.30.

Computer hacking: See Section I.G.40.

Revenge porn: A person commits the crime of unlawful dissemination of an intimate image if the following elements are present:

• The person, with intent to harass, humiliate, or injure another person, knowingly causes to be disclosed through an Internet website an identifiable image of the other person whose intimate parts are visible or who is engaged in sexual conduct;

• The person knows or reasonably should have known that the other person does not consent to the disclosure;

• The other person is harassed, humiliated, or injured by the disclosure, and

• A reasonable person would be harassed, humiliated, or injured by the disclosure (Or. Rev. Stat. § 163.472(1)).

In general, unlawful dissemination of an intimate image is a class A misdemeanor, unless the person has a prior conviction for the offense, in which case it is a class C felony (Or. Rev. Stat. § 163.472(2)). The offense does not apply to activities by law enforcement agencies investigating and prosecuting crimes; legitimate medical, scientific, or educational activities; specified legal proceedings; the reporting of unlawful conduct to a law enforcement agency; disclosures that serve a lawful public interest; and disclosures of images that depict another person voluntarily displaying intimate parts in a public area or that were created for a commercial purpose with the consent of the other person (Or. Rev. Stat. § 163.472(4)(a)-(f)). Additionally, the crime does not apply to a provider of an interactive computer service for an image of intimate parts provided by an information content provider (Or. Rev. Stat. § 163.472(4)(g)).

II. **REGULATORY AUTHORITIES AND ENFORCEMENT**

II.A. **Attorney General** —

The Attorney General has enforcement authority over a variety of state privacy provisions, including do-not-call provisions (see Section I.E.10.), credit card information violations (see Section I.D.30.), genetic information privacy laws (see Section I.E.50.), and disclosures of social security numbers by the Department of Transportation (see Section I.D.100.), among others. Although the Attorney General provides for data breach reporting on its consumer protection website, Oregon law technically vests enforcement authority for data breach laws, as well as other components of the Oregon Consumer Identity Theft Protection Act (CITPA), in the Director of the Department of Consumer and Business Services. See Section I.C.80. (breach notification), Section I.D.40. (security freezes), Section I.C.60. (data security requirements), Section I.C.70. (data disposal requirements), and Section I.D.100. (prohibitions on the display of social security numbers).

II.B. **Other Regulators** —

The Oregon Bureau of Labor and Industries enforces privacy and data security provisions related to employment, including the ban on requiring or using credit histories and violations of the state's “ban-the-box” law (see Section I.E.60.).

The Department of Administrative Services has the authority to enforce provisions governing privacy and data security applicable to state agencies under the Oregon Consumer Identity Theft Protection Act (CITPA). See Section I.C.80. (breach notification), Section I.D.40. (security freezes), Section I.C.60. (data security requirements), Section I.C.70. (data disposal requirements), and Section I.D.100. (prohibitions on the display of social security numbers), and other data security provisions specifically applicable to state agencies (see Section I.C.60.).

The Oregon Health Authority is authorized to impose civil penalties on persons failing to comply with requirements governing reporting of information to the state's cancer registry (see Section I.E.50.).

II.C. **Sanctions & Fines** —

Consumer Identity Theft Protection Act: The Director of the Department of Consumer and Business Services has the authority to enforce provisions of the Oregon Consumer Identity Theft Protection Act (CITPA) regarding data breach notification (see Section I.C.80.), security freezes (see Section I.D.40.), data security (see Section I.C.60.), data disposal (see Section I.C.70.), and prohibitions on the display of social security numbers (see Section I.D.100.). The Director has the authority to conduct investigations and to compel obedience with lawful subpoenas and other requests for information via court order (Or. Rev. Stat. § 646A.624(1)-(2)). The Director also may issue a cease-and-desist order against a violator or may require the violator to pay compensation to consumers injured by the violation, but compensation is available only on a finding that enforcement of the rights of a consumer would be so burdensome or expensive as to be impractical (Or. Rev. Stat. § 646A.624(3)).

In addition to any other penalties provided by law, a person violating the provisions of the CITPA is subject to a penalty of not more than $1,000 per violation. Every violation is a separate offense, and for continuing violations, each day's continuance is a separate violation. The maximum penalty for any occurrence may not exceed $500, 000 (Or. Rev. Stat. § 646A.624(4)(a)-(b)). Civil penalties are imposed as provided in the state's Administrative Procedures Act at Or. Rev. Stat. § 183.745 (Or. Rev. Stat. § 646A.624(4)(c)).

Limitations on information in credit card receipts: The Attorney General or a district attorney may bring an action to restrain and prevent violations of provisions regarding limits on information that may be included on credit card receipts (see Section I.D.30.). The Attorney General or district attorney may seek an injunction or a civil penalty from a person who violates an injunctive order (Or. Rev. Stat. § 646A.230(1)). A person who violates such an order is subject to a civil penalty of not more than $1,000 per violation. In addition, in an action brought by a prosecuting attorney, the court may award the prevailing party reasonable attorney fees at trial and on appeal (Or. Rev. Stat. § 646A.230(2)).

Ban-the-box law: Individuals who are aggrieved by an employer's violation of provisions prohibiting it from seeking information on criminal convictions on an employment application (the “ban-the-box” law; see Section I.E.60.) may seek redress from the Commissioner of the Bureau of Labor and Industries, including filing a complaint, seeking a potential settlement, or seeking imposition of civil penalties, as provided by Or. Rev. Stat. § 659A.820 through Or. Rev. Stat. § 659A.865 (Or. Rev. Stat. § 659A.362).

Employer inquiries into credit history of applicants and employees: Employees or applicants aggrieved by a violation of provisions prohibiting employers from inquiring into their credit histories (see Section I.E.6.) may file a complaint with the Commissioner of the Bureau of Labor and Industries under Or. Rev. Stat. § 659A.820 (Or. Rev. Stat. § 659A.320(3)).

Genetic information: The Attorney General or a district attorney may bring an action against a person who violates provisions of Oregon's genetic information privacy laws (see Section I.E.50.). The same remedies available pursuant to a private cause of action brought under Or. Rev. Stat. § 192.541 (see Section I.G.50.) are available to the Attorney General or district attorney, together with the costs of litigation (Or. Rev. Stat. § 192.545(1)). In addition, the Attorney General is authorized to intervene in a private cause of action if it determines that the action is of general public importance, and in such a case, is entitled to the relief outlined above (Or. Rev. Stat. § 192.545(2)).

Cancer registry reporting: Any person who fails to comply with requirements regarding the reporting of information to the Oregon cancer and tumor registry system (see Section I.E.50.) is subject to a civil penalty imposed by the Oregon Health Authority. The penalty is imposed for each day compliance is refused. For a health care facility, the penalty is equal to $50 for the first 30 days and $500 per day afterwards, and for a health care

practitioner, the penalty is $50 per day (Or. Rev. Stat. § 432.900(1)).

Social security number disclosure by Department of Transportation: The Attorney General or a district attorney may obtain appropriate relief to enforce provisions involving the impermissible disclosure of a social security number (SSN) by the Department of Transportation or a redisclosure of an SSN by another agency (see Section I.D.100.), together with attorney fees and costs (Or. Rev. Stat. § 802.195(9)).

II.D. **Representative Enforcement Actions** —

In 2013, Oregon's Department of Consumer and Business Services fined a regional health system after a patient found medical records discarded in an unlocked recycling container. The department's Division of Finance and Corporate Securities assessed a civil penalty of $5,000 against Samaritan Health Services Inc. “for publicly posting, displaying or otherwise making available to the public, files bearing consumer names and unredacted Social Security numbers in violation of [the Oregon Consumer Identity Theft Protection Act]” See the Order. The department agreed to suspend $4,000 of the penalty if Samaritan complied with the terms of the decree and commits no new violations of the act for five years.

II.E. **State Resources** —

The Attorney General provides a variety of resources for businesses and consumers on its website, including information on data breaches, identity theft, and do-not-call provisions. Notably, those resources include a searchable database of all breaches reported to the Attorney General. In addition, the Department of Justice has issued a Spotlight on Privacy that touches on a number of topics, including consumer safeguards, student privacy, and data security. Finally, the Attorney General provides an online complaint form for consumers to use if they believe that a business is violating their privacy in any manner.

The Oregon Cybersecurity Advisory Council provides a resource page listing federal and state resources available to state government regarding cyberthreat prevention and recovery practices.

The Department of Administrative Services has issued a best practices checklist outlining state agency practices to be considered to comply with the Oregon Consumer Identity Theft Protection Act (CITPA). In addition, the Department has promulgated Statewide Policy No. 107-004-052 on information security policies for state agencies and Statewide Policy No. 107-004-120 on information security incident response requirements applicable to such agencies.

The Division of Financial Regulation provides an overview on steps that businesses should consider to comply adequately with CITPA provisions.

The Bureau of Labor and Industries has provided documentation for use by employers with respect to the conduct of criminal background checks on applicants for employment.

III. **RISK ENVIRONMENT** —

Introduction

Like most other states in the country, Oregon does not currently have in place any comprehensive privacy and data protection law, such as the California Consumer Privacy Act of 2018 (“CCPA”) or the Virginia Consumer Data Protection Act (“VCDPA”). Oregon does, however, have a number of sector-specific laws and common law torts that are designed to protect Oregon residents’ privacy and data protection rights. The common law torts available in Oregon pertaining to privacy are: (1) intrusion upon solitude or seclusion; (2) public disclosure of private facts; (3) false light privacy; and (4)

appropriation of name or likeness.

Also like other states, Oregon recently updated its data breach notification law in 2019, originally known as the Oregon Consumer Identity Theft Protection Act. Now known as the Oregon Consumer Information Protection Act as a result of the recent amendments, the current version of Oregon's breach notice law entails a broader definition of security breach and also imposes additional requirements on vendors and service providers.

Oregon is, however, on the forefront of Internet of Things ("IoT") security laws, and is only one of two states (along with California) to have enacted a law specifically focused on the security of connected devices. That law, "Security Requirements for Internet-Connected Devices," ORS 646A.813, went into effect on January 1, 2020.

Attorney General Approach to Privacy

Consumer privacy is a key issue for the Oregon Department of Justice ("DOJ") and Attorney General Ellen F. Rosenblum. AG Rosenblum has stated her commitment to making the online marketplace safer and more straightforward for Oregonians as one of her top priorities in her role as AG. In 2017, AG Rosenblum supported the Oregon legislature's passage of a bill designed to hold companies accountable for their online privacy policies. As a result of bill's passage, Oregon's Unlawful Trade Practices Act (originally passed in the 1970s) now applies to the privacy terms consumers agree to prior to downloading an app or other online tools. In 2015, AG Rosenblum was part of a coalition of 38 states that opposed the sale of consumer data in connection with RadioShack's proposed bankruptcy sale to General Wireless. The action taken by AG Rosenblum and the other state AGs resulted in a settlement agreement that ensured that the majority of RadioShack's consumer data would be destroyed. The settlement also required General Wireless to give Radio Shack customers the opportunity to opt out of the sale of their email addresses and other information.

No significant enforcement actions have been taken by AG Rosenblum in the last 12 months.

Other Notable Issues/Information

Oregon Senator Ron Wyden has been one of the most active lawmakers in Washington D.C. on the privacy and data security front, and has made pushing for comprehensive privacy and data protection legislation a top priority of his while serving in the United States Senate. In 2018, Senator Wyden introduced the Consumer Data Protection Act, which would have provided sweeping legislation that empowered consumers to control their personal information, created transparency into how companies use and share their data, and imposed fines on executives that misused consumers' data.

In 2019, Senator Wyden introduced the Mind Your Own Business Act of 2019 (S 2637), which—similar to the Consumer Data Protection Act—would have mandated transparency about how companies share, sell, and use consumer data. In addition, the bill would have also created stringent penalties—including harsh fines and prison terms—for corporate executives that misuse consumers' data and lie about those practices to the government. The bill failed during the 116th Congress.

Most recently, in April 2021 Senator Wyden introduced the Protecting Americans' Data From Foreign Surveillance Act, which would create new safeguards relating to the export of sensitive personal information to foreign countries if doing so could harm United States national security. While Oregon does not have a biometric privacy law of its own, federal courts in Oregon have made it easier for consumers to bring biometric privacy class action lawsuits against businesses under the Illinois Biometric Information Privacy Act ("BIPA"). The Ninth Circuit Court of Appeals in *Patel v. Facebook*, Inc., 932 F.3d 1264 (9th Cir. 2019) held that *any* BIPA violation—even a mere technical violation—amounts to a violation of plaintiffs' substantive privacy rights and, thus, constitutes a cognizable, concrete injury-in-fact sufficient to confer Article III standing to sue in federal court. In doing so, the Ninth Circuit became the first federal appellate court to

hold that a mere technical BIPA violation injures an individual's concrete right to privacy and, in turn, presents a concrete injury-in-fact for Article III standing. This decision has played a large role in incentivizing plaintiffs seeking to recover statutory damages under BIPA—which has led to a flood of bet-the-company litigation under Illinois' biometric privacy law—as a result of lowering the Article III standing hurdle that poses a roadblock in many other types of class action litigation. The *Patel* court also upheld the certification of a class of Illinois Facebook users, which ultimately led to the landmark $650 million settlement that was reached to resolve the *Patel* litigation against Facebook.

IV. **EMERGING ISSUES AND OUTLOOK**

IV.A. **Recent Legislation** —

Contact Tracing Privacy Law. Under legislation (HB 3284) that took effect on June 15, 2021, private entities may not collect, use or disclose personal health data about a person's exposure to or infection by Covid-19 without the users' consent. Such data must be deleted 65 days after it has been collected. The law does not apply to healthcare providers, the Oregon Health Authority, or public health agencies who are already covered by separate health information privacy statutes.

Data Breach and Scope of Personal Information. Under legislation that took effect on Jan. 1, 2020, third-party vendors must notify covered entities as soon as is practicable but not later than 10 days after discovering a data breach. If the breach involves personal information of more than 250 consumers the state attorney general must be notified (Or. Rev. Stat. § 646A.604(2)(a)-(c)). SB 624 also expands the definition of "personal information" to include a user name or other means of identifying a consumer for the purpose of permitting access to the consumer's account, together with any other method necessary to authenticate the user name or means of identification (Or. Rev. Stat. § 646A.602(12)(a)).

IV.B. **Current Session Legislation (2019-2020)** —

Click here to view recent state specific privacy and data security legislation. This search is automatically updated to display active bills as they move through the legislative process.

IV.C. **Other Issues** —

Equifax Breach. On July 22, 2019, the Federal Trade Commission (FTC) announced that Equifax will pay at least $575 million and up to $700 million as part of a settlement with the FTC, the Consumer Financial Protection Bureau (CFPB) and 48 states, plus the District of Columbia and Puerto Rico. The settlement resolves allegations that the company failed to adequately protect consumers' data, which ultimately led to the 2017 data breach affecting at least 147 million consumers.

Under the settlement agreement, Equifax will contribute $300 million to a fund created to provide credit monitoring for all consumers affected by the breach and provide an additional $125 million to the fund if the initial amount is insufficient to compensate affected consumers. The fund will also be used to compensate and reimburse consumers who bought credit monitoring services from Equifax and paid other out-of-pocket expenses resulting from the breach. Affected individuals are eligible to receive up to $20,000 for verifiable unreimbursed costs related to the breach. Further, the company will pay $175 million to the 48 states, District of Columbia, and Puerto Rico. CFPB will collect another $100 million in civil penalties. Beginning in 2020, Equifax will provide to all U.S. consumers six free credit reports per year for seven years – in addition to the one free report provided annually by Equifax and two national credit monitoring agencies, TransUnion and Experian.

The FTC's complaint against Equifax alleged that after being alerted in March 2017 to a critical security vulnerability in its consumer inquiry database, the company's security team ordered the system to be patched within 48 hours.

However, Equifax failed to ensure the order was executed and learned in July 2017 that the database was unpatched. As a result, for several months, hackers gained access to, and stole, consumers' personally identifiable information, including Social Security numbers, birth dates, credit card numbers, and other sensitive data.

The FTC alleged that Equifax failed to implement basic security measures, such as implementing a policy to ensure security vulnerabilities were patched, failing to install intrusion detection for legacy databases, and failing to encrypt Social Security numbers and other sensitive consumer data. Although the basic security measures were not taken, Equifax's privacy policy stated that it implemented reasonable safeguards to limit access to and protect consumer information. As such, the FTC's complaint alleged that Equifax violated the Gramm-Leach-Bliley Act's Safeguards Rule because "it did not design and implement safeguards to address foreseeable internal and external risks, regularly test or monitor the effectiveness of the safeguards, or evaluate and adjust the information security program in light of the results of testing and monitoring…." Additionally, the FTC alleged that Equifax's failure violated the FTC Act.

In addition to civil penalties and the monetary compensation to affected individuals, Equifax must also create and implement a comprehensive information security program, with a third-party assessment every two years.

Facebook/Cambridge Analytica. In March 2018, Oregon Attorney General Ellen F. Rosenblum joined other attorneys general in a letter sent to Facebook CEO Mark Zuckerberg, asking questions about data-sharing procedures that led to the alleged use of 50 million users' data without their consent by Cambridge Analytica. The National Association of Attorneys General seeks information about how the company will make privacy policies and terms of service clearer and more understandable; what controls the company has over data given to developers; what safeguards are in place to police these activities; and what kinds of user data the social media giant knew Cambridge Analytica was accessing and using, and when.

Facebook sent a detailed response to the National Association of Attorneys General on May 7, 2018, that outlines the company's policies and practices regarding user data, the facts related to the misuse of data, and the steps Facebook is taking to address the incident and prevent any recurrence.

Facebook-FTC Settlement. On July 24, 2019, the Federal Trade Commission (FTC) announced that Facebook will pay $5 billion and implement new privacy restrictions as part of a 20-year settlement agreement for alleged privacy violations. The settlement resolves the FTC's allegations that the company violated a 2012 FTC order and deceived Facebook users about their ability to control the privacy of their personal information. According to the FTC, the monetary fine "is one of the largest penalties ever assessed by the U.S. government for any violation," and is "almost 20 times greater than the largest privacy or data security penalty ever imposed worldwide." The FTC's 2012 order required Facebook to, among other things, give consumers clear notice and obtain express consent before sharing consumers' information, execute and maintain a privacy program to protect consumers' information, and obtain independent third-party privacy audits every other year. However, the FTC alleged in its 2019 complaint that Facebook violated the order because the company did not maintain a privacy program that protected the privacy of consumer's information, it used deceptive privacy settings and statements that users relied on to restrict sharing their information on Facebook, and it shared data of users' Facebook friends with third-party app developers regardless of the friends' privacy settings. Further, Facebook violated Section 5(a) of the FTC Act by failing to disclose that certain user information would be used for advertising. In addition to the $5 billion penalty, Facebook must create an independent privacy committee consisting of Facebook's board of directors, appointed by an independent nominating committee. Facebook must also designate compliance officers to be in charge of the company's new privacy program. The compliance officers, along with CEO Mark Zuckerberg, must submit quarterly and annual compliance certifications to the FTC stating the company is in compliance with the 2019 order. Among other requirements, the company must also implement broader oversight of third-party apps, provide users with clear notice that it uses facial recognition technology, and conduct a privacy review of all new or modified products,

services, or practices before implementation.

Coronavirus Contact Tracing Developments. In April 2020, Oregon launched a contact tracing program aimed at curbing the spread of the pandemic in the state. Under the voluntary program, a public health worker who is performing contact tracing will reach out to Covid-positive patients to urge them to isolate at home and ask them about recent activities and the identity of recent close contacts. The tracers then reach out to those who may have been exposed to the virus and request that they, too, go into quarantine for 14 days. To protect patient privacy, contacts are only informed that they may have been in close contact with a person diagnosed with Covid-19. They are not told the identity of the patient. The governor hopes to add an additional 600 trained tracers to the program.