OREGON

Identity Theft Protection Act

Protecting Personal Information

A BUSINESS GUIDE

DEPARTMENT OF CONSUMER & BUSINESS SERVICES

Division of Financial Regulation

Oregon Identity Theft Protection Act

Collecting, sharing, and keeping personal data is essential to businesses, organizations, and government agencies. Cyber attacks have become increasingly common and sophisticated, so it's not just essential to have a plan to protect your customers and employees, it's the law.

Oregon's Consumer Identity Theft Protection Act and related rules will give you clear direction and expectations to ensure the safety of sensitive data.

In Oregon, personal information includes a consumer's first name – or first initial and last name – in combination with the consumer's:

- Social Security number
- Driver license number or state ID card number issued by the Department of Transportation
- Passport number or other U.S.-issued identification number
- Financial account, credit, or debit card number, in combination with any required security or access code, or password that would allow access to the financial account

- Physical characteristics data used to authenticate identification during a financial transaction such as fingerprint, retina, or iris image
- Health insurance policy number or health insurance subscriber identification number in combination with any other unique identifier used by health insurers
- Medical history, mental or physical condition, or medical diagnosis or treatment by a health care professional

⚠ Your responsibility...

You can assess and minimize the risks to your business and to consumers by following the requirements contained in the Oregon Consumer Identity Theft Protection Act. The law contains standards to safeguard personal information, shield Social Security numbers, and notify consumers in case of a security breach.

The Department of Consumer and Business Services and the Oregon Department of Justice enforce these laws and provide educational materials.

Protect data

Consumers appreciate your products and the service you provide. They also will appreciate the measures you have in place to effectively protect their personal information.

⚠ Your responsibility...

The Oregon Identity Theft Protection Act requires you to develop, implement, and maintain reasonable safeguards to ensure the security, confidentiality, and integrity of personal information. Safeguarding also means properly disposing of information.

The following steps will help you to implement an information security program that will help minimize breach risks.

Assess

Take inventory of all personal information you have on computers and files by type and location. This also includes information your business receives through websites and from contractors and others. Be sure you know what sensitive information is stored on electronic devices such as tablets, laptops, employees' home computers, flash drives, and cell phones.

As part of the assessment, test the effectiveness of your existing security safeguards to see if there are any foreseeable internal or external risks with your network or the software used.

Protect

Lost or stolen paper documents containing personal information make you vulnerable to a security breach. The best defense in securing paper documents, as well as hard disks, CDs, DVDs, flash drives, tapes, and other storage media, is locking them in a file cabinet or placing them in a locked room with limited access. Develop a plan for your employees, outlining procedures to securely store sensitive information, including if or how devices can be taken off the premises. Encrypt sensitive information stored on laptops. Use a firewall to protect your computer system from attacks.

Reduce

If you don't have a need for personal information, don't collect it and don't keep it. If you do need it for a legitimate business purpose, design a records retention plan that outlines what information must be kept, how to secure it, how long to keep it, and how to dispose of it securely once you no longer need it.

Train

Make sure employees know what personal information is, how important it is to safeguard it, and your security program practices and procedures. Likewise, train your employees on notification procedures in the event of a security breach.

To help spread the word, designate one or more employees to coordinate the security program.

Detect

Regularly assess security risks by testing and monitoring key controls, systems, and procedures. Look at any risk to your information storage, whether it is a locking file cabinet or electronic system. This will help you respond quickly to any attacks or intrusions.

When selecting outside service providers, know their capabilities in maintaining appropriate safeguards and require these safeguards in your contract with them.

Prepare

Create a plan for dealing with a security breach if one should occur. Swift action is crucial for complying with federal and state laws, and failing to develop a breach response plan ahead of time will almost certainly result in missteps. The plan should include, for example, procedures for involving the necessary service providers and professionals to evaluate and contain the breach, investigating the breach, preserving evidence, reporting the breach to regulators and law enforcement, notifying affected customers, and addressing the breach in the media.

Given the prevalence of security breaches affecting electronic information, many insurance companies are now offering "cyber insurance." Explore this insurance option and understand what coverage will and won't do for you.

Destroy

Properly destroy records with personal information to protect against any unauthorized access or use. Shred, burn, or pulverize hard-copy records, and erase any electronic records to make them unreadable and prevent anyone from reconstructing them.

Oregon's E-Cycles program encourages everyone to recycle electronic devices, including computers, monitors, keyboards, and mice. However, before recycling, make sure all personal information on the devices is erased permanently or destroyed.

More details on securing data

According to the Oregon Identity Theft Protection Act, a security program includes the following:

Administrative safeguards

- Designate one or more employees to coordinate the security program.
- Identify reasonably foreseeable internal and external risks.

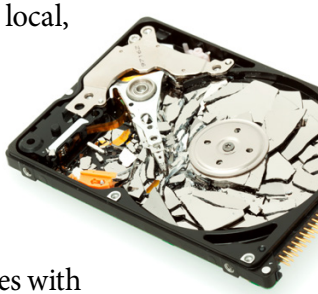
- Assess the sufficiency of safeguards in place to control the identified risks.
- Train and manage employees in the security program practices and procedures.
- Select service providers capable of maintaining appropriate safeguards, and require those safeguards by contract.
- Adjust the security program in light of business changes or new circumstances.

Technical safeguards

- Assess risks in network and software design, information processing and transmission, and storage.
- Detect, prevent, and respond to attacks or system failures.
- Regularly test and monitor the effectiveness of key controls, systems, and procedures.

Physical safeguards

- Assess risks of information storage and disposal.
- Detect, prevent, and respond to intrusions.
- Protect against unauthorized access to or use of personal information during or after the collection, transportation, and destruction or disposal of the information.
- Dispose of personal information after it is no longer needed for business purposes or as required by local, state, or federal law by burning, pulverizing, shredding, or modifying a physical record and by destroying electronic media so that the information cannot be read or reconstructed.



Note: Any individual, business, government agency, or organization that is subject to and complies with data safeguard regulations or guidance adopted under the Gramm-Leach-Bliley Act or the Health Insurance Portability and Accountability Act (HIPAA) does not need to develop additional

processes. However, you must follow Oregon's requirements to protect your employees' personal information, such as Social Security numbers or financial data as HIPAA does not cover this information.

Protect Social Security numbers

A Social Security number is a person's most unique means of identification because it never changes. It also is used to link to records that contain other sensitive information. These factors make the Social Security number valuable to those who commit identity theft, and absolutely crucial to protect from disclosure.

⚠ Your responsibility...

The Oregon Identity Theft Protection Act prohibits anyone (individuals, government agencies, organizations, or businesses) from printing Social Security numbers on any material that is mailed when the recipient has not requested it, unless redacted. This does not apply to records or documents required by state or federal law such as W2s, 1099s, or similar documents. The law also prohibits printing a Social Security number on a card used to access products or services, or publicly posting or displaying a Social Security number, such as on a website. Exceptions include records required by state or federal law; that are used for internal verification or administrative processes; or that are used to enforce a judgment or court order.
Other exceptions include:

- Rules adopted by the courts
- Copies of records possessed by a court, the State Court Administrator, or the Secretary of State

Businesses or organizations that use Social Security numbers as an account identifier should use another means to identify their customers' accounts.

Notify consumers

The faster consumers know their personal identification information has been breached, the faster they can take safeguarding precautions.

⚠ Your responsibility...

A person that owns, maintains, or licenses personal information used in the course of business, vocation, occupation, or volunteer activities, must notify their customers as soon as possible that there has been a data security breach. Notification can be made in one of the following ways:

- Written notification.
- Electronic notice, if this is the customary means of communication between you and your customers.
- Telephone notice provided that you make direct contact with the affected customer.

A person or company that maintains or possesses personal information on behalf of another must immediately notify that owner or licensor of a security breach.

If there are more than 250 consumers affected by the security breach, you must notify the Oregon Attorney General at https://justice.oregon.gov/consumer/DataBreach/Home/Submit or 877-877-9392 (toll-free).

You may delay notification if a law enforcement agency determines that it will impede a criminal investigation.

Notification is not required if either of the following are true:

- An investigation or consultation with a federal, state, or local law enforcement agency leads you to determine that there is no reasonable likelihood of harm to consumers. You must document this determination in writing and maintain the documentation for at least five years.
- The personal information was encrypted or made unreadable.

Any individual, business, government agency, or organization that is subject to and complies with the notification regulations or guidance adopted under the Gramm-Leach-Bliley Act meets Oregon's notification requirements. However, if the breach involves your employees, you must comply with Oregon's notification requirements.

Substitute notice

If you can show that the cost of notifying consumers will exceed $250,000, or those needing to be contacted is more than 350,000, or if you don't have sufficient contact information to notify affected consumers, you may follow both of these substitute notice requirements:

- Conspicuous posting of the notice or a link to the notice on your website if you maintain one.
- Notifying major statewide Oregon television and newspaper media.

Notifying consumer reporting agencies

If the security breach affects more than 1,000 consumers, you must report the timing, distribution, and content to the three credit reporting agencies (TransUnion, Equifax, and Experian), without unreasonable delay.

TransUnion

Phone: 800-971-4307 (toll-free)

Experian

Phone: 714-830-5442

Equifax

Phone: 866-510-4211 (voice mail only) (toll-free)
Email: businessrecordsecurity@equifax.com
Mail: Equifax Fraud Assistance, Attn: Security Breach
PO Box 740245, Atlanta, GA 30374

Additional resources

Oregon Identity Theft Protection Act – Oregon Revised Statute 646A.600
https://www.oregonlegislature.gov/bills_laws/ors/ors646A.html
(Scroll to **Identity Theft Prevention**.)

Oregon Administrative Rule – Identity Theft
http://arcweb.sos.state.or.us/pages/rules/oars_400/oar_441/441_646.html
(Scroll to **Identity Theft OAR Chapter 441, Div. 646, Section 0010 through 0040**.)

Federal Trade Commission
www.ftc.gov/infosecurity

OnGuard Online
www.OnGuardOnline.gov

Contact:
503-378-4140
866-814-9710
dfr.oregon.gov

440-4117 (7/17/COM)