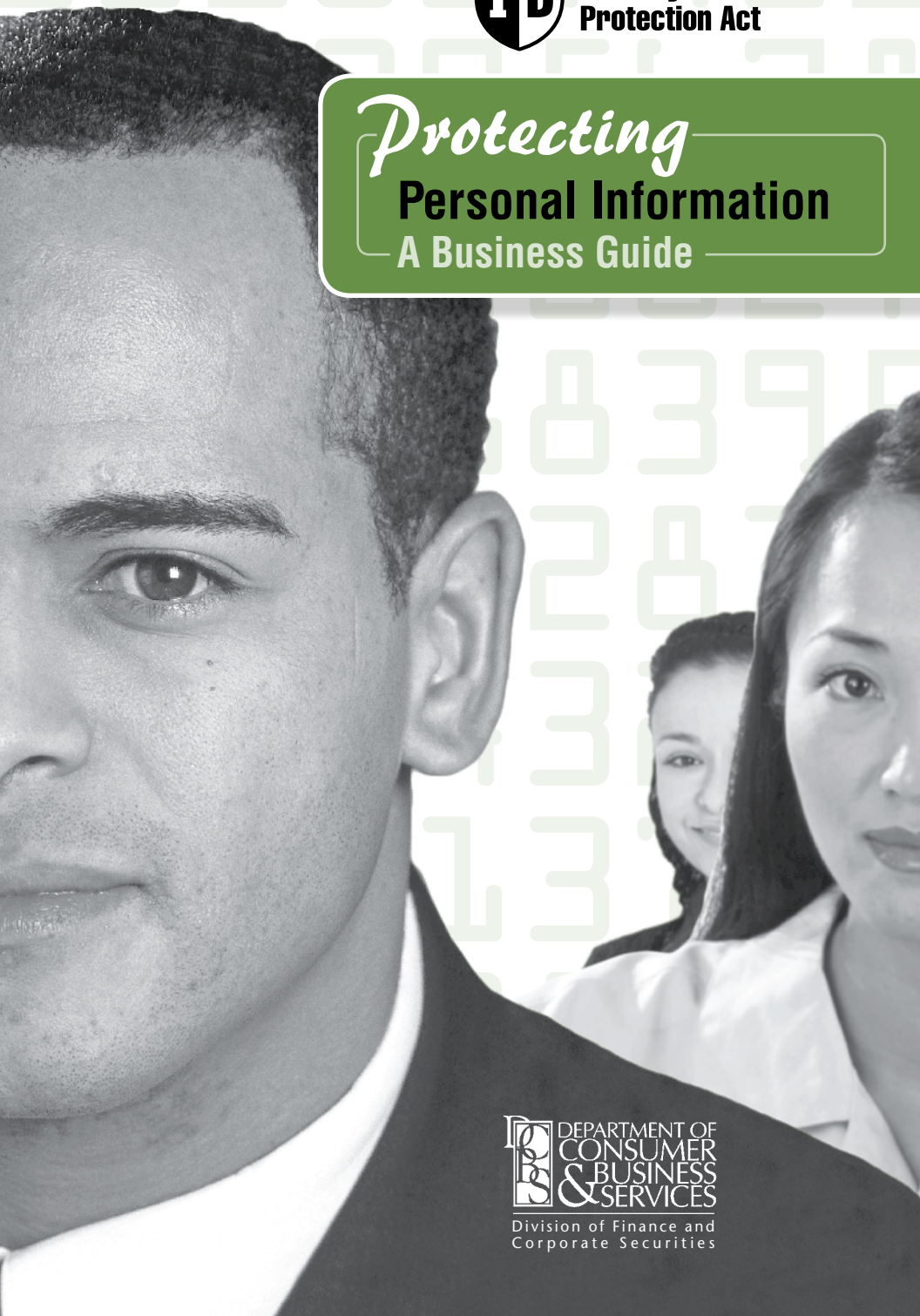
OREGON
Identity Theft Protection Act

Protecting Personal Information

A Business Guide



DEPARTMENT OF CONSUMER & BUSINESS SERVICES
Division of Finance and Corporate Securities

Oregon Identity Theft Protection Act

Collecting and sharing personal data is essential to all types of businesses, organizations, and government entities — small and large. Most organizations, whether public or private, gather consumers' personal identifying information such as names, addresses, credit card and Social Security numbers either manually or electronically (or both) to conduct transactions and better target their products and services.

However, if this information lands in the wrong hands it can be exploited by those who commit identity theft. Identity theft can cause economic havoc to both business and the public. According to the Federal Trade Commission, this crime costs U.S. businesses nearly $48 billion every year. Oregon is ranked the 13th worst in the nation for identity theft. Identity theft can be particularly detrimental to businesses that are small with limited resources.

Oregon has a new law — the Identity Theft Protection Act — that will give you clear direction and expectations to ensure the safety of sensitive data. And Oregon consumers will have more tools to protect themselves against identity theft by having the ability to place a security freeze on their credit file.

⚠ *Your Responsibility...*

You can assess and minimize the risks to your business and to consumers by following the requirements contained in the Oregon Identity Theft Protection Act passed in 2007. The law contains standards to shield Social Security numbers, notify consumers in case of a security breach, and safeguard personal identifying information.

Recognizing that Oregon has a large percentage of small businesses, the components of the law can be adapted and implemented whether you have five employees or 500 employees.

The Department of Consumer and Business Services is charged with enforcing these new laws as well as providing educational materials.

Protect Social Security Numbers

A Social Security number is a person's most unique means of identification because it never changes. Unlike other identifying information, a SSN has a significant role in linking records that contain sensitive information. This unique factor is what makes a SSN so valuable to those who commit identity theft. Both the broad use of this identifier and its value have contributed to the growth of identity theft and credit fraud.

⚠ *Your Responsibility...*

The Oregon Identity Theft Protection Act prohibits individuals, government agencies, organizations, or businesses from printing Social Security numbers on any material that is mailed, unless the recipient has requested it. 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 Web site.

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 SSNs as an account identifier should use another means to identify the consumer's account.

Notify Consumers

The faster a consumer knows their personal identification information has been breached, the more opportunities they have to take precautions to ensure their information is not being used fraudulently.

Personal information includes a consumer's name in combination with a Social Security number, Oregon driver's license or Oregon identification card number, or a financial, credit, or debit card number along with a security code or password that would allow someone to access a consumer's financial account

⚠ *Your Responsibility...*

Those who maintain personal information are required to notify their customers if computer files containing that personal information have been subject to a security breach as soon as possible in one of the following manners:

- 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 consumer

A person or company that maintains or possesses personal identifying information on behalf of another is required to immediately notify that owner or licensee of a security breach.

Notification to consumers may be delayed if a law enforcement agency determines that it will impede a criminal investigation.

If an investigation into the breach or consultation with a federal, state or local law enforcement agency determines there is no reasonable likelihood of harm to consumers, or if the personal information was encrypted or made unreadable, notification is not required.

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 follow Oregon's notification requirements.

Substitute notice

If you demonstrate that the cost of notifying would exceed $250,000, that the number of those who need to be contacted is over 350,000, or if you don't have the means to sufficiently contact consumers, substitute notice may be given. Substitute notice consists of:

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

Notifying consumer reporting agencies

In the event that the security breach affects more than 1,000 consumers, the responsible person or organization must report the timing, distribution, and content of the notice given to the affected consumers to the three credit reporting agencies (TransUnion, Equifax, Experian), without unreasonable delay.

Protect Data

Consumers appreciate your products and the service you provide. They also will appreciate the measures you have in place that effectively protect their personal identifying 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 the information. Safeguarding also means properly disposing of information.

The following steps will assist you in implementing an information security program that will help minimize breach risks.

Assess

Take inventory of all information you have on computers and files by type and location. This also includes how your business receives personal information through Web sites, from contractors, and others. Be sure you know what sensitive information is stored on laptops, employees' home computers, flash drives, cell phones, and personal digital assistants (PDAs).

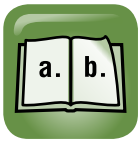
As part of the assessment, take a look at the effectiveness of existing security safeguards to see if there are any foreseeable internal or external risks with your network or the software used.

Protect

Lost or stolen paper documents containing personal identifying information make you vulnerable to a security breach. The best defense in securing paper documents, as well as CDs, floppy disks, zip drives, tapes, and backups, 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. And ensure that sensitive information stored on laptops is encrypted. Use a firewall software to protect your computer system from attacks.

Reduce

If you don't have a need for certain personal identifying information, don't keep it. And don't collect sensitive consumer information, such as a Social Security number, if it's not a legitimate business need. If this information does serve a need, design a record 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 identifying information is, know how important it is to safeguard it, and know your security program practices and procedures. Personal information includes a consumer's name in combination with a Social Security number, Oregon driver's license or Oregon identification card number, or a financial, credit, or debit card number along with a security code or password that would allow someone to access a consumer's financial account. 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. In addition, look at any risk to your information storage whether it is a locking file cabinet or electronic system. This will help in quickly responding 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.

Destroy

Protect against any unauthorized access or use of the personal identifying information you maintain and no longer need by properly destroying it. Hard copy records with sensitive information should be shred, burned, or pulverized. Any electronic records should be erased in such a way that they cannot be read or reconstructed.

The Oregon Legislature recently passed a law to encourage the recycling of electronic devices including desktop and laptop computers. Because you are responsible for safeguarding any personal identifying information that may be on an electronic device, you should first properly dispose of any electronic records that contain personal identifying information by erasing or destroying the hard drive or reach an agreement with the company collecting the equipment that it will properly dispose of the information before recycling.

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.
- Assess risks in information processing, 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 identifying information.

Small Business Requirements

Small businesses, defined as 200 or fewer employees in manufacturing or 50 or fewer employees in other types of business, comply with the safeguard requirements if their information security and disposal program contains the administrative, technical, and physical safeguards and disposal measures appropriate to the business' size and complexity as well as the nature, scope of its activities, and the sensitivity of the personal information it collects.

Additional Resources

Federal Trade Commission
www.ftc.gov/infosecurity

Department of Homeland Security's National Strategy to Secure Cyberspace
www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf

OnGuard Online
www.OnGuardOnline.gov

Security Freeze – An Option for Consumers

The Oregon Identity Theft Protection Act also provides consumers with a proactive way to guard their personal identifying information: a security freeze. Placing a security freeze on your credit file is an effective deterrent against identity theft.

All Oregonians may place a security freeze on their credit file maintained by a credit reporting agency such as Equifax, Experian, or TransUnion. Once activated, someone who has fraudulently obtained your personal identifying information would not be able to gain access to your credit file. The freeze also prevents lenders and others from gaining access to your credit report for review.

Important note: Keep in mind that a security freeze will not prevent an identity thief from misusing existing credit cards and credit accounts.

Before you decide to apply an optional freeze to your credit files, consider whether you intend to make a purchase that would require a look at your credit history. For example, if you plan to buy a cell phone and service, the company will need to access your credit files to finalize the sale.

Obtaining a Security Freeze

To place a freeze, you must write to each of the three credit agencies. By law the agencies will freeze your file within five business days after receiving your request.

Cost

There is no fee if a person is a victim of identity theft or has reported the theft of their personal identifying information to a law enforcement agency. To prove this you must submit a valid copy of a police incident report or a Federal Trade Commission Identity Theft Complaint Form.

If you are not an identity theft victim, you still may place a security freeze but you may have to pay a fee. Each credit reporting agency may charge a fee of no more than $10. Therefore if you place a freeze with all three agencies, you will pay a total of $30.

Important note: One security freeze does not cover everyone in a household. Spouses or partners must freeze their credit files separately.

Access to Your File under a Freeze

Even if you have a security freeze, some government agencies, law enforcement and courts, and private companies can still access your credit files. These include companies you are doing business with; companies to which you owe money; and collection agencies.

"Thawing" the Freeze

Consumers who place a freeze on their credit report can temporarily or permanently remove the freeze or "thaw" their file to apply for new credit. To do so, follow the procedures in the confirmation letter each credit reporting agency sent when you first placed your security freeze. A fee of no more than $10 will be charged by each agency to lift the freeze. Credit reporting agencies must lift a freeze within three business days after receiving your request.

For more details on the procedures for placing and lifting a security freeze and to see sample security freeze request letters, go to www.dfcs.oregon.gov and click on Identity Theft.

Contact:
503-378-4140
866-814-9710
www.dfcs.oregon.gov
Click on Identity Theft

440-4117 (2/08/COM)