Division of Finance and Corporate Securities (DFCS)

Frequently Asked Questions

Q: What is the Identity Theft Protection Act?

A: The Act is a new law, passed by the 2007 Oregon legislature, that requires businesses, organizations, government agencies, and individuals that collect and maintain personal identifying information to ensure the security of that information.

Q: What is "personal identifying information?"

A: A person's name in combination with a Social Security number, Oregon driver's license number or Oregon identification card number, passport number, financial, credit or debit card numbers along with security or access codes or password that would provide access to a financial account.

Q: What does the law require?

A: The law contains three components that will help protect sensitive information:

Notification of a Security Breach. Anyone (business, organization, government agency, or individual) that maintains personal information of Oregon consumers will be required to notify his or her customers if computer files containing that personal information have been subject to a security breach. You need to notify as soon as possible unless law enforcement determines it would impede a criminal investigation. *Effective date: October 1, 2007*

Protection of Social Security numbers. Those who keep Social Security numbers are prohibited from printing Social Security numbers on cards or documents that are mailed, unless the consumer has requested information that requires an SSN, or publicly displaying or posting a Social Security number. This doesn't apply to the use of SSNs for internal verification purposes. The law allows an exception for records that are required by law to be made available to the public. *Effective date: October 1, 2007*

Safeguarding Data. If you collect personal identifying information, you must develop, implement and maintain reasonable safeguards to protect the security and confidentiality of the information. This also includes the proper

disposal of information. *Effective date: January 1, 2008*

Q: How does a business have to notify consumers in case of a security breach?

A: In the majority of cases you can notify by writing to your customers, however the law allows notification through electronic means if this is the primary manner of communication between you and your customers. Telephone notification may be used provided that you directly contact each customer.

Q: Can I just notify people through the media or post it on my Web site?

A: If the cost of notification is more than $250,000 or the number of individuals to be contacted is more than 350,000, you may notify through major Oregon television and newspaper media and conspicuously post a notice and a link to the notice on your Web site if you maintain one.

Q. My organization is subject to and complies with the Gramm-Leach-Bliley Act. Do I need to follow Oregon's requirements for breach notification?

A. If a business, organization or government agency is subject to and complies with notification regulations or guidance adopted under the Gramm-Leach-Bliley Act, it does not need to develop a further process. However, if the breach involves the personal identifying information of your employees, you must follow Oregon's notification requirements.

Q: If we have a security breach involving our employees' personal identifying information and some employees live outside of Oregon, do we still follow Oregon law to notify them?

A: For the employees living in Oregon, you would follow Oregon law in notification procedures. However, for those employees living outside of Oregon, you would follow the employee's home state notification law, if there is one. Of course, you can always notify your employee even if the home state would not require notification.

Q: What do I need to do to comply with the data safeguard component?

A: In general you must protect the security, confidentiality and integrity of the personal information you maintain including the disposal of information that is no longer needed by developing and implementing an information security plan.

According to the Identity Theft Protection Act, a security plan includes:

- **Administrative** safeguards such as identifying what personal information you keep and how to keep it safe, training employees in security program practices and procedures, and ensuring that contracted service providers are capable of supplying and maintaining systems that protect sensitive information.
- **Technical** safeguards such as assessing risks in network and software design, and detecting, preventing and responding to attacks or system failures;
- **Physical** safeguards such as protecting against unauthorized access to or use of personal identifying information, and disposing of information that is no longer needed by way of shredding, burning or erasing electronic data that is unreadable or cannot be reconstructed.

Click here for specific data safeguards.

Q. Is it true that if I follow the data safeguard regulations in the Health Insurance Portability and Accountability Act (HIPAA), I don't need to do develop further safeguards?

A. If your business or organization, including government, is subject to and complies with regulations or guidance adopted under HIPAA, you don't need to create a further process. The same is true if you also are subject to and comply with regulations adopted under the federal Gramm-Leach-Bliley Act in regard to protecting sensitive information. However, you must follow Oregon's requirements in safeguarding the personal identifying information of your employees.