DEPARTMENT OF CONSUMER & BUSINESS SERVICES

NEWS RELEASE

Director's Office, 350 Winter St. NE, Room 200, Salem, Oregon 97301-3878

For immediate release:
December 14, 2007

For more information:
Diane Childs, 503-947-7423

New Identity Theft Law has Jan. 1 Deadline

Business, Government Must Safeguard Sensitive Data

(Salem) — A key piece of Oregon's new identity theft law takes effect Jan. 1, 2008. By that date, Oregon businesses, organizations, and government agencies must have a plan in place to protect the sensitive data they collect, keep, and share, according to a law passed by the 2007 Legislature.

The Oregon Consumer Identity Theft Protection Act (SB 583) also requires businesses and government agencies to protect sensitive information and Social Security numbers, and to notify customers if there is a security breach involving computer files. The latter two requirements have been in effect since Oct. 1.

The plan required by the new law must contain reasonable protections to ensure that personal identifying information doesn't fall into the wrong hands. Plans will vary depending on the nature, size, and scope of the business. Personal identifying information is defined, by law, as a person's name in combination with either a Social Security number, passport number, Oregon-issued driver's license or identification card number, or a financial account, credit card or debit card number along with a security code, password, or access code.

"Protecting personal information can be as easy as placing paper documents, CDs, and even laptops that contain that data in a locked file cabinet," said David Tatman, administrator for the division of Finance and Corporate Securities (DFCS), part of the department of Consumer and Business Services (DCBS).

Other simple, yet effective, steps include encrypting – which means making sensitive computer data unreadable – and installing effective password protections on computers and servers.

"Laptops containing personal information account for about one-fourth of all security breaches in the United States," Tatman said. "These lapses in security could have been prevented if the owner of the information had made it completely unusable to the identity thieves."

A data safeguarding plan also should include procedures for disposing sensitive information after it is no longer needed. Proper disposal means shredding or burning it if the information is paper, or destroying or erasing electronic files and folders.

Identity theft is prevalent in Oregon. According to the Federal Trade Commission, the state is ranked the 13th worst, per capita, in this crime. Identity theft victims may incur damaged credit records, unauthorized charges on credit cards, and unauthorized withdrawals from bank accounts.

In addition to the new requirements for businesses, the law gives consumers the right to place a "freeze" on their credit file to prevent identity theft. For more information on the credit freeze and the new requirements for businesses, visit www.dfcs.oregon.gov and click on Identity Theft.

The Division of Finance and Corporate Securities has developed educational materials and is available to make presentations for businesses to better understand their rights and responsibilities under the new law. To contact the division by phone, call 503-378-4140, or toll-free at 1 (866) 814-9710.

###