

SB 583A
SECTION-BY-SECTION ANALYSIS

SECTION 1 Title. This act is entitled the Oregon Consumer Identity Theft Protection Act.

SECTION 2 Definitions. Defines terms used in the act: Breach of security, Consumer, Consumer report, Consumer reporting agency, Debt, Encryption, Extension of Credit, Identity theft, Identity theft declaration, Person, Personal information, Redacted, and Security freeze.

Other than the definition for Person, these definitions are mostly consistent with similar definitions in other jurisdictions that have laws covering the topics in this Act. The definition of Person includes public bodies, making this Act applicable to state, local and special government bodies. Not all laws concerning identity theft in other states are applicable to government.

SECTION 3 Notification of breach of security. Requires any person that owns, maintains or otherwise possesses personal information used in the person's business, vocation, occupation or volunteer activities to notify Oregon residents when a breach of computerized data is discovered, unless after investigation or consultation with law enforcement, the breach has not and will not likely result in harm. Notification must be made in the most expedient time possible, but may be delayed at the written request of law enforcement conducting a criminal investigation. Notice may be given by mail, e-mail, telephone, or substitute notice, which consists of conspicuous posting on the person's web page and notice to major statewide TV and newspaper media. Substitute notice is permitted only if the cost of notification will exceed \$250,000, more than 350,000 Oregon residents must be notified, or the person has insufficient contact information. Information to be included in the notice is prescribed. Complying with notification requirements established under a federal or state law or by the person's primary or functional federal regulator fulfills these notification requirements.

Of the 38 states with a notification law, 32 states require notification only if the breach involves computerized data, thus this Act follows the majority of states. The description of when notification is required ranges widely, from notify upon any breach, to notify unless the breach has not and will not likely result in a significant risk of identity theft. The notification procedures in this section are similar to, but not identical with, provisions in the majority of the 37 states.

SECTION 4 Security freeze election. Any Oregon resident may elect to place a freeze on their credit report. To place the freeze, the consumer must send a written request to a consumer reporting agency, or may use a secure electronic website if made available by the consumer reporting agency. If the consumer is a victim of identity theft, or has reported theft of personal information to law enforcement, the request may include a copy of the police report, incident report or identity theft declaration. The consumer must provide proper identification and any fee authorized in Section 6. Except as provided in Section 8, if a security freeze is in place, information from the consumer report may not be released without the consumer's authorization, but the credit reporting agency may advise a third party that a freeze is in effect.

Of the 39 states with a freeze law, 33 states permit all consumers to place a freeze on their credit report, thus this Act follows the majority of the states. The process to place the freeze is consistent with that in the other states.

SECTION 5 Security freeze procedures. The consumer reporting agency must place the freeze within 5 business days of the consumer's request, and within 10 business days of placing the security freeze, the agency must send a written confirmation to the consumer. With the confirmation, the consumer reporting agency must provide a personal identification number (PIN) or password to be used by the consumer to later temporarily lift or remove the freeze, and must describe those temporary lift and removal processes. To temporarily lift or remove the freeze, the consumer must provide proper identification, the PIN or password, the temporary lift period of time, if applicable, and any fee authorized in Section 6. The consumer reporting agency must temporarily lift or remove the freeze within 3 business days of receiving the request. No later than 12/31/08, the Director of the Department of Consumer and Business Services (DCBS) must inform designated persons in the legislature concerning the minimum time necessary to place, temporarily lift or remove a freeze using current technology.

The time frames and processes in this section are consistent with the procedures set in the other states' laws. Several states have legislated that a temporary lift be accomplished within 15 minutes of the consumer's electronic or telephone request, but have set a delayed date for this requirement. Rather than incorporating something similar in this section, the Director of DCBS is to report to the legislature by the end of 2008, allowing an amendment of this Act in the next general legislative session to implement timing for temporarily lifting the freeze that the credit reporting agencies can reasonably accommodate.

SECTION 6 Security freeze fees. No fee may be charged to an identity theft victim, or to a consumer who has reported to law enforcement the theft of personal information, provided the consumer submits to the consumer reporting agency a copy of a valid police report, incident report, or identity theft declaration. A fee not to exceed \$10 may be charged to any other consumer to place, temporarily lift, or remove a freeze, or to replace a lost PIN or password.

Almost all of the 32 states with a freeze law prohibit fees being charged to identity theft victims and some states prohibit charging fees to seniors who have reached a specific age. For other consumers, maximum permitted fees range from \$0 to \$20. The \$10 maximum fees permitted in this section are consistent with the majority of the states.

SECTION 7 Security freeze temporary lift or removal restrictions. A consumer reporting agency may temporarily lift a freeze only when requested by the consumer. A freeze may be removed only at the consumer's request or if the consumer reporting agency determines the credit report was frozen due to a material misrepresentation of fact by the consumer. The consumer must be given at least 5 business days' notice of removal of the freeze by the consumer reporting agency for misrepresentation.

This section is consistent with provisions in other states.

SECTION 8 Security freeze exclusions. Even while the credit report is frozen, information from the report may be used by or for the 10 persons or entities listed in this section. The list includes creditors with whom the consumer already has an account, persons operating under court order or federal law including the Fair Credit Reporting Act, persons the consumer has authorized to access the credit report, as authorized by law for insurance purposes, or for screening an applicant for a residential dwelling unit.

All states with a freeze law include a section similar to this, although the persons included in the lists are not consistent from one state to the next.

SECTION 9 Applications while freeze in effect. A third party may treat as incomplete any application for credit or any other use, when the third party cannot access the consumer's frozen credit report.

This provision is contained in the freeze laws of the majority of other states. Treating an application as incomplete is the preferred alternative to denying the application. Denying an application requires specific actions be performed, including providing the reason for denial, and may negatively impact the applicant's credit report.

SECTION 10 Changing information in a frozen credit report, entities not required to freeze credit reports. A consumer reporting agency may not change the consumer's name, date of birth, Social Security number or address in a frozen credit report, unless written confirmation of the change is sent within 30 days of the change to the consumer. For an address change, confirmation must be sent to both the new and former addresses.

A reseller of credit information that does not maintain its own database, a check services or fraud prevention services company dealing with questions on checks or other payment methods, and a company issuing reports for a new deposit account are not required to place a freeze on a credit report. The reseller must honor a freeze placed on a consumer report by another consumer reporting agency.

These provisions are consistent with similar provisions found in other states' freeze laws, and allow for uniformity.

SECTION 11 Social Security number restrictions. All persons are prohibited from disclosing a consumer's Social Security number by printing it on cards or documents, publicly posting it or publicly displaying it. These restrictions do not apply to use of the Social Security number for internal verification purposes, to records required by federal law or state law including court rules to include Social Security numbers or to be provided to the public, to court or Secretary of State records on file before the effective date of this bill, or to court or Secretary of State records received after the effective date of this Act, if the filer could have protected the Social Security number from disclosure.

Approximately 15 other states have a broad law similar to this, although several of them specifically exclude government from the law. The list of who is excluded from the restrictions varies widely. In addition, other states have limited laws prohibiting use of Social Security numbers for specified purposes, such as on fishing and hunting licenses.

SECTION 12 Data safeguarding requirement. Any person that owns, maintains or possesses personal information used in the course of the person's business, vocation, occupation or volunteer activities must develop, implement and maintain reasonable procedures to safeguard that data, including when disposing of the data. Administrative, technical and physical components of complying with the safeguarding requirement are described, while allowing an owner of a small business discretion to determine what is appropriate safeguarding for his or her particular business. Persons that comply with a state or federal law providing similar or higher requirements, including the Gramm-Leach-Bliley and Health Insurance Portability and Accountability Acts, are deemed to be in compliance with these safeguarding requirements.

The data safeguarding requirements apply to both paper and computerized data, making this section broader than the section on notification for breach of security of computerized data.

Most depository and non-depository financial institutions are already subject to safeguarding requirements issued by federal regulators, such as banking regulators, the Securities and Exchange Commission and the Federal Trade Commission. In addition, most of the insurance industry is subject to safeguarding requirements adopted by the federal Department of Health and Human Services and the Oregon Insurance Commissioner.

Other states have enacted laws concerning disposal of personal information, and other states have enacted laws concerning safeguarding of data, but few states' laws address safeguarding of data both while maintaining and using the data, and when disposing of the data, as this Act does.

SECTION 13 Enforcement. The Director of the DCBS is authorized to conduct investigations, issue cease and desist orders, require a person who has violated this Act to pay restitution to harmed Oregon residents under certain circumstances, and assess civil penalties. The civil penalties are set at \$1,000 per violation, and in the case of a continuing violation each day's continuance is a separate violation, but the maximum penalty for any occurrence may not exceed \$500,000.

Assigning enforcement authority to a state agency other than the Attorney General is unique among all states with identity theft legislation. All other states permit a private right of action, or enforcement by the Attorney General, usually as a violation of trade practices laws, or a combination of the two remedies.

Penalties vary widely, with some states setting different amounts for violations of their respective notification, freeze, data security and/or Social Security number violations. Penalty amounts range from \$100 per violation to \$10,000 per violation. The highest aggregate penalty found was \$750,000.

SECTION 14 Rulemaking. The Director of DCBS is authorized to adopt rules to carry out the purposes of this Act.

SECTION 15 Funding. To implement this Act, the Director of DCBS is authorized to allocate as deemed appropriate moneys derived pursuant to programs currently administered within the Department's Insurance Division and Division of Finance and Corporate Securities.

SECTION 16 Safeguarding delayed operative date. The safeguarding requirements become operative on January 1, 2008.

SECTION 17 Emergency clause. An emergency is declared, and this Act takes effect October 1, 2007.