THE SENATE
TWENTY-THIRD LEGISLATURE, 2006
STATE OF HAWAII

S.B. NO. 2290 S.D. 2

A BILL FOR AN ACT

RELATING TO PROTECTION FROM SECURITY BREACHES.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF HAWAII:

SECTION 1. The Hawaii Revised Statutes is amended by adding to title 26 a new chapter to be appropriately designated and to read as follows:

"CHAPTER

NOTIFICATION OF SECURITY BREACHES

§ -1 Purpose. The privacy and financial security of individuals is increasingly at risk due to the widespread collection of personal information by the private sector and government agencies. Numerous sources include personal information that forms the source material for identity thieves.

Identity theft is one of the fastest growing crimes committed throughout the United States, including Hawaii. Criminals who steal personal information, such as social security numbers, use the information to open credit card accounts, write bad checks, buy cars, and commit other financial crimes with other people's identities.

The purpose of this chapter is to alleviate the growing plague of identity theft by requiring businesses and government

agencies that maintain records containing resident individuals' personal information to notify an individual whenever the individual's personal information has been compromised by unauthorized disclosure.

§ -2 Definitions. As used in this chapter:

"Business" means a sole proprietorship, partnership, corporation, association, or other group, however organized and whether or not organized to operate at a profit. The term includes a financial institution organized, chartered, or holding a license or authorization certificate under the laws of this State, any other state, the United States, or any other country, or the parent or the subsidiary of any such financial institution. The term also includes an entity whose business is records destruction.

"Government agency" means any department, division, board, commission, public corporation, or other agency or instrumentality of the State or of any county.

"Encryption" means the use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without use of a confidential process or key.

"Personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

(1) Social security number;

(2) Driver's license number or Hawaii identification card number; or

(3) Account number, credit or debit card number, access code, or password that would permit access to an individual's financial account.

For purposes of this section, "personal information" shall not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

"Records" means any material on which written, drawn, spoken, visual, or electromagnetic information is recorded or preserved, regardless of physical form or characteristics.

"Redacted" means the rendering of data so that it is unreadable or is truncated so that no more than the last four digits of the identification number are accessible as part of the data.

"Security breach" means an incident of unauthorized access to and acquisition of unencrypted or unredacted records or data containing personal information where illegal use of the personal information has occurred or is reasonably likely to occur or that creates a material risk of harm to a person. Any incident of unauthorized access to and acquisition of encrypted records or data containing personal information along with the confidential process or key shall constitute a security breach. Good faith acquisition of personal information by an employee or agent of the business for a legitimate purpose is not a security breach, provided that the personal information is not used for a purpose other than a lawful purpose of the business and is not subject to further unauthorized disclosure.

§ -3 Protection from security breaches. (a) Any business that owns or licenses personal information of residents of Hawaii, any business that conducts business in Hawaii that owns or licenses personal information in any form (whether computerized, paper, or otherwise), or any government agency that collects personal information for specific government purposes shall provide notice to the affected person that there has been a security breach following discovery or notification of the breach. The disclosure notification shall be made

without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection (c) of this section, and consistent with any measures necessary to determine sufficient contact information, determine the scope of the breach, and restore the reasonable integrity, security, and confidentiality of the data system.

(b) Any business located in Hawaii or any business that conducts business in Hawaii that maintains or possesses records or data containing personal information of residents of Hawaii that the business does not own or license, or any government agency that maintains or possesses records or data containing personal information of residents of Hawaii shall notify the owner or licensee of the information of any security breach immediately following discovery of the breach, consistent with the legitimate needs of law enforcement as provided in subsection (c).

(c) The notice required by this chapter shall be delayed if a law enforcement agency informs the business or government agency that notification may impede a criminal investigation or jeopardize national security and requests a delay; provided that such request is made in writing, or the business or government agency documents the request contemporaneously in writing,

including the name of the law enforcement officer making the request and the officer's law enforcement agency engaged in the investigation. The notice required by this chapter shall be provided without unreasonable delay after the law enforcement agency communicates to the business or government agency its determination that notice will no longer impede the investigation or jeopardize national security.

(d) The notice shall be clear and conspicuous. The notice shall include a description of the following:

(1) The incident in general terms;

(2) The type of personal information that was subject to the unauthorized access and acquisition;

(3) The general acts of the business or government agency to protect the personal information from further unauthorized access;

(4) A telephone number that the person may call for further information and assistance, if one exists; and

(5) Advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports.

(e) For purposes of this section, notice to affected persons may be provided by one of the following methods:

(1) Written notice to the last available address the business or government agency has on record;

(2) Electronic notice, for those persons for whom a business or government agency has a valid email address and who have agreed to receive communications electronically if the notice provided is consistent with the provisions regarding electronic records and signatures for notices legally required to be in writing set forth in 15 U.S.C. section 7001;

(3) Telephonic notice provided that contact is made directly with the affected persons; and

(4) Substitute notice, if the business or government agency demonstrates that the cost of providing notice would exceed $250,000 or that the affected class of subject persons to be notified exceeds 500,000, or if the business or government agency does not have sufficient contact information or consent to satisfy paragraph (1), (2), or (3), for only those affected persons without sufficient contact information or consent, or if the business or government agency is unable to identify particular affected persons, for

only those unidentifiable affected persons.

Substitute notice shall consist of all the following:

(A) Email notice when the business or government agency has an electronic mail address for the subject persons;

(B) Conspicuous posting of the notice on the website page of the business or government agency, if one is maintained; and

(C) Notification to major statewide media.

(f) In the event a business provides notice to more than 1,000 persons at one time pursuant to this section, the business shall notify in writing, without unreasonable delay, the State of Hawaii's office of consumer protection and all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C. section 1681a(p), of the timing, distribution, and content of the notice.

(g) Any waiver of the provisions of this chapter is contrary to public policy and is void and unenforceable.

(h) The following shall be deemed to be in compliance with this chapter:

(1) A financial institution that is subject to the Federal Interagency Guidance Response Programs for

Unauthorized Access to Consumer Information and Customer Notice, issued on March 7, 2005, by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision, or subject to 12 C.F.R. Part 748, and any revisions, additions, or substitutions relating to said interagency guidance; and

(2) Any health plan or healthcare provider that is subject to and in compliance with the standards for privacy or individually identifiable health information and the security standards for the protection of electronic health information of the Health Insurance Portability and Accountability Act of 1996.

(i) Any business who violates or attempts to violate any provision of this chapter shall be deemed to have engaged in an unfair or deceptive act or practice in the conduct of trade or commerce within the meaning of section 480-2. The attorney general or the director of the office of consumer protection may bring an action based upon unfair or deceptive acts or practices declared unlawful by this section. No such action may be brought against a government agency.

(j) In addition to any penalty provided for in subsection (i), any business who violates any provision of this chapter is liable to the injured party in an amount equal to the sum of any actual damages sustained by the injured party as a result of the violation, or damages not less than $500, whichever is greater. The court, in any action brought under this section, may award reasonable attorneys' fees to the prevailing party. No such action may be brought against a government agency."

SECTION 2. This Act shall take effect on January 1, 2007.

SB2290, SD2

Report Title:
Identity Theft; Prevention

Description:
Requires businesses that experience a security breach to notify affected people of the breach. (SD2)