

1 security numbers, use the information to open credit card
2 accounts, write bad checks, buy cars, and commit other financial
3 crimes with other people's identities.

4 The purpose of this chapter is to alleviate the growing
5 plague of identity theft by requiring businesses that maintain
6 records containing resident individuals' personal information,
7 and to notify an individual, whenever the individual's personal
8 information has been compromised by unauthorized disclosure.

9 § -2 **Definitions.** As used in this chapter:

10 "Business" means a sole proprietorship, partnership,
11 corporation, association, or other group, however organized and
12 whether or not organized to operate at a profit. The term
13 includes a financial institution organized, chartered, or
14 holding a license or authorization certificate under the laws of
15 this State, any other state, the United States, or any other
16 country, or the parent or the subsidiary of any such financial
17 institution. The term also includes an entity whose business is
18 records destruction. The term shall not include any government
19 or governmental subdivision or agency.

20 "Encryption" means the use of an algorithmic process to
21 transform data into a form in which the data is rendered

1 unreadable or unusable without use of a confidential process or
2 key.

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

- 7 (1) Social security number.
- 8 (2) Driver's license number or Hawaii identification card
9 number.
- 10 (3) Account number, credit or debit card number, access
11 code, or password that would permit access to an
12 individual's financial account.

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

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

20 "Security breach" means an incident of unauthorized access
21 to and acquisition of unencrypted or unredacted records or data
22 containing personal information where illegal use of the

1 personal information has occurred or is reasonably likely to
2 occur or that creates a material risk of harm to a person. Any
3 incident of unauthorized access to and acquisition of encrypted
4 records or data containing personal information along with the
5 confidential process or key shall constitute a security breach.
6 Good faith acquisition of personal information by an employee or
7 agent of the business for a legitimate purpose is not a security
8 breach, provided that the personal information is not used for a
9 purpose other than a lawful purpose of the business and is not
10 subject to further unauthorized disclosure.

11 § -3 **Protection from security breaches.** (a) Any
12 business that owns or licenses personal information of residents
13 of Hawaii or any business that conducts business in Hawaii that
14 owns or licenses personal information in any form (whether
15 computerized, paper, or otherwise) shall provide notice to the
16 affected person that there has been a security breach following
17 discovery or notification of the breach. The disclosure
18 notification shall be made without unreasonable delay,
19 consistent with the legitimate needs of law enforcement, as
20 provided in subsection (c) of this section, and consistent with
21 any measures necessary to determine sufficient contact
22 information, determine the scope of the breach, and restore the

1 reasonable integrity, security, and confidentiality of the data
2 system.

3 (b) Any business that maintains or possesses records or
4 data containing personal information of residents of Hawaii that
5 the business does not own or license, or any business that
6 conducts business in Hawaii that maintains or possesses records
7 or data containing personal information that the business does
8 not own or license shall notify the owner or licensee of the
9 information of any security breach immediately following
10 discovery of the breach, consistent with the legitimate needs of
11 law enforcement as provided in subsection (c).

12 (c) The notice required by this chapter shall be delayed
13 if a law enforcement agency informs the business that
14 notification may impede a criminal investigation or jeopardize
15 national security, provided that such request is made in writing
16 or the business documents such request contemporaneously in
17 writing, including the name of the law enforcement officer
18 making the request and the officer's law enforcement agency
19 engaged in the investigation. The notice required by this
20 section shall be provided without unreasonable delay after the
21 law enforcement agency communicates to the business its

1 determination that notice will no longer impede the
2 investigation or jeopardize national security.

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

5 (1) The incident in general terms;

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

8 (3) The general acts of the business to protect the
9 personal information from further unauthorized access;

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

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

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

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

19 (2) Electronic notice, for those persons for whom it has a
20 valid email address and who have agreed to receive
21 communications electronically if the notice provided
22 is consistent with the provisions regarding electronic



1 records and signatures for notices legally required to
2 be in writing set forth in 15 U.S.C. section 7001;

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

5 (4) Substitute notice, if the business demonstrates that
6 the cost of providing notice would exceed \$250,000 or
7 that the affected class of subject persons to be
8 notified exceeds 500,000, or if the business does not
9 have sufficient contact information or consent to
10 satisfy paragraph (1), (2), or (3), for only those
11 affected persons without sufficient contact
12 information or consent, or if the business is unable
13 to identify particular affected persons, for only
14 those unidentifiable affected persons. Substitute
15 notice shall consist of all the following:

16 (A) Email notice when the business has an electronic
17 mail address for the subject persons;

18 (B) Conspicuous posting of the notice on the website
19 page of the business, if one is maintained; and

20 (C) Notification to major statewide media.

21 (f) In the event a business provides notice to more than
22 1,000 persons at one time pursuant to this section, the business



1 shall notify in writing, without unreasonable delay, the State
2 of Hawaii's office of consumer protection and all consumer
3 reporting agencies that compile and maintain files on consumers
4 on a nationwide basis, as defined in 15 U.S.C. section 1681a(p),
5 of the timing, distribution, and content of the notice.

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

8 (h) A financial institution that is subject to and in
9 compliance with the Federal Interagency Guidance Response
10 Programs for Unauthorized Access to Consumer Information and
11 Customer Notice, issued on March 7, 2005, by the Board of
12 Governors of the Federal Reserve System, the Federal Deposit
13 Insurance Corporation, the Office of the Comptroller of the
14 Currency, and the Office of Thrift Supervision, and any
15 revisions, additions, or substitutions relating to said
16 interagency guidance, shall be deemed to be in compliance with
17 this chapter.

18 (i) Any person who violates or attempts to violate any
19 provision of this chapter shall be deemed to have engaged in an
20 unfair or deceptive act or practice in the conduct of trade or
21 commerce within the meaning of section 480-2. The attorney
22 general or the director of the office of consumer protection may



1 bring an action based upon unfair or deceptive acts or practices
2 declared unlawful by this section."

3 SECTION 3. This Act shall take effect on January 1, 2007.

SB2290, SD1

Report Title:

Identity Theft; Prevention

Description:

Requires businesses that experience a security breach to notify affected people of the breach. (SD1)

