

CHAPTER 487

CONSUMER PROTECTION

§487J-1 Definitions. As used in this chapter:

"Business" means a sole proprietorship, partnership, limited partnership, corporation, limited liability company, association, or any other form of business entity. The term also 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.

"Personal information" has the same meaning as in section 487N-1.

"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. [L 2006, c 137, pt of §2; am L Sp 2008, c 10, §3]

§487J-2 Social security number protection. (a) Except as otherwise provided in subsection (b), a business or government agency may not do any of the following:

- (1) Intentionally communicate or otherwise make available to the general public an individual's entire social security number;
- (2) Intentionally print or imbed an individual's entire social security number on any card required for the individual to access products or services provided by the business or government agency;
- (3) Require an individual to transmit the individual's entire social security number over the Internet, unless the connection is secure or the social security number is encrypted. For purposes of this paragraph, "encrypted" means that an algorithmic process has been used to transform data into a form in which the data is rendered unreadable or unusable without the use of a confidential process or key;
- (4) Require an individual to use the individual's entire social security number to access an internet website, unless a password or unique personal identification number or other authentication device is also required to access the internet website; or
- (5) Print an individual's entire social security number on any materials that are mailed to the individual, unless the materials are employer-to-employee communications, or where specifically requested by the individual.

(b) Subsection (a) shall not apply to:

(1) The inclusion of a social security number in documents that are mailed and:

(A) Are specifically requested by the individual identified by the social security number;

(B) Required by state or federal law to be on the document to be mailed;

(C) Required as part of an application or enrollment process;

(D) Used to establish, amend, or terminate an account, contract, or policy; or

(E) Used to confirm the accuracy of the social security number for the purpose of obtaining a credit report pursuant to 15 U.S.C. section 1681(b).

A social security number that is permitted to be mailed under this paragraph may not be printed, in whole or in part, on a postcard or other mailer not requiring an envelope, or visible on the envelope or without the envelope having been opened;

(2) The opening of an account or the provision of or payment for a product or service authorized by an individual;

(3) The collection, use, or release of a social security number to investigate or prevent fraud; conduct background checks; conduct social or scientific research; collect a debt; obtain a credit report from or furnish data to a consumer reporting agency pursuant to the Fair Credit Reporting Act, 15 U.S.C. sections 1681 to 1681x, as amended; undertake a permissible purpose enumerated under the federal Gramm Leach Bliley Act, 15 U.S.C. sections 6801 to 6809, as amended; locate an individual who is missing or due a benefit, such as a pension, insurance, or unclaimed property benefit; or locate a lost relative;

(4) A business or government agency acting pursuant to a court order, warrant, subpoena, or when otherwise required by law;

(5) A business or government agency providing the social security number to a federal, state, or local government entity including a law enforcement agency or court, or their agents or assigns;

(6) The collection, use, or release of a social security number in the course of administering a claim, benefit, or procedure relating to an individual's employment, including an individual's termination from employment, retirement from employment, injuries suffered during the course of employment, and other related claims, benefits, or procedures;

(7) The collection, use, or release of a social security number as required by state or federal law;

- (8) The sharing of the social security number by business affiliates;
- (9) The use of a social security number for internal verification or administrative purposes;
- (10) A social security number that has been redacted; and
- (11) Documents or records that are recorded or required to be open to the public pursuant to the constitution or laws of the State or court rule or order.

(c) A business or government agency covered by this section shall make reasonable efforts to cooperate, through systems testing and other means, to ensure that the requirements of this chapter are complied with. [L 2006, c 137, pt of §2; am L 2008, c 19, §68]

[§487J-3] Penalties; civil action. (a) Any business that violates any provision of this chapter shall be subject to penalties of not more than \$2,500 for each violation. The attorney general or the executive director of the office of consumer protection may bring an action pursuant to this section. No such action may be brought against a government agency.

(b) In addition to any penalty provided for in subsection (a), any business that violates any provision of this chapter shall be 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. 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.

(c) The penalties provided in this section shall be cumulative to the remedies or penalties available under all other laws of this State. [L 2006, c 137, pt of §2]

[§487J-4] Reporting requirements. A government agency shall submit a written report to the legislature within twenty days after the discovery of a material occurrence of a social security number disclosure by the government agency that is prohibited by this chapter. The report shall contain information relating to the nature of the incident, the number of individuals affected by the incident, and any procedures that have been implemented to prevent the incident from reoccurring. In the event that a law enforcement agency informs the government agency that the report may impede a criminal investigation or jeopardize national security, the report to the legislature may be delayed until twenty days after the law enforcement agency has determined that the report will no longer impede the investigation or jeopardize national security. [L 2006, c 137, pt of §2]

CHAPTER 487N

[SECURITY BREACH OF PERSONAL INFORMATION]

Section

487N-1 Definitions

487N-2 Notice of security breach

487N-3 Penalties; civil action

487N-4 Reporting requirements

487N-5 Information privacy and security council;
established; duties; reports

487N-6 Personal information security; best practices;
websites

487N-7 Personal information system; government agencies;
annual report

Note

Personal information protection requirements. L Sp 2008, c 10, §§7 to 15.

Cross References

Personal information policy and oversight responsibilities for government agencies, see §487J-5.

§487N-1 Definitions. As used in this chapter, unless the context otherwise requires:

"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 the 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.

"Council" means the information privacy and security council established under section 487N-5.

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

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

"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.

"Personal information" does 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 and that creates a 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 constitutes 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. [L 2006, c 135, pt of §2; am L 2008, c 19, §69; am L Sp 2008, c 10, §5]

§487N-2 Notice of security breach. (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 section 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 section 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 mail notice, for those persons for whom a business or government agency has a valid electronic mail 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 \$100,000 or that the affected class of subject persons to be notified exceeds two hundred thousand, 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) Electronic mail 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 one thousand 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) The following businesses shall be deemed to be in compliance with this section:

(1) A financial institution that is subject to the federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice published in the Federal Register on March 29, 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 the 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.

(h) Any waiver of the provisions of this section is contrary to public policy and is void and unenforceable. [L 2006, c 135, pt of §2; am L 2008, c 19, §70]

[§487N-3] Penalties; civil action. (a) Any business that violates any provision of this chapter shall be subject to penalties of not more than \$2,500 for each violation. The attorney general or the executive director of the office of consumer protection may bring an action pursuant to this section. No such action may be brought against a government agency.

(b) In addition to any penalty provided for in subsection (a), any business that violates any provision of this chapter shall be 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. 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.

(c) The penalties provided in this section shall be cumulative to the remedies or penalties available under all other laws of this State. [L 2006, c 135, pt of §2]

[§487N-4] Reporting requirements. A government agency shall submit a written report to the legislature within twenty days after discovery of a security breach at the government agency that details information relating to the nature of the breach, the number of individuals affected by the breach, a copy of the notice of security breach that was issued, the number of individuals to whom the notice was sent, whether the notice was delayed due to law enforcement considerations, and any procedures that have been implemented to prevent the breach from reoccurring. In the event that a law enforcement agency informs the government agency that notification may impede a criminal investigation or jeopardize national security, the report to the legislature may be delayed until twenty days after the law enforcement agency has determined that notice will no longer impede the investigation or jeopardize national security. [L 2006, c 135, pt of §2]

[CHAPTER 487R]

DESTRUCTION OF PERSONAL INFORMATION RECORDS

Section

487R-1 Definitions

487R-2 Destruction of personal information records

487R-3 Penalties; civil action

487R-4 Reporting requirements

Note

Personal information protection requirements. L Sp 2008, c 10, §§7 to 15.

§487R-1 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. Except as provided in section 487R-2(e), the term includes a financial institution organized, chartered, or holding a license or authorization certificate under the laws of the 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.

"Disposal" means the discarding or abandonment of records containing personal information or the sale, donation, discarding, or transfer of any medium, including computer equipment or computer media, containing records of personal information, or other nonpaper media upon which records of personal information are stored, or other equipment for nonpaper storage of information.

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

"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.

"Personal information" shall not include publicly available information that is lawfully made available to the general public from federal, state, or local government records. "Encrypted", as used in this definition means the use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without the use of a confidential process or key.

"Records" means any material on which written, drawn, spoken, visual, or electromagnetic information is recorded or preserved, regardless of physical form or characteristics. [L 2006, c 136, pt of §2; am L 2008, c 19, §71]

§487R-2 Destruction of personal information records. (a) Any business or government agency that conducts business in Hawaii and any business or government agency that maintains or otherwise possesses personal information of a resident of Hawaii shall take reasonable measures to protect against unauthorized access to or use of the information in connection with or after its disposal.

(b) The reasonable measures shall include:

(1) Implementing and monitoring compliance with policies and procedures that require the burning, pulverizing, recycling, or shredding of papers containing personal information so that information cannot be practicably read or reconstructed;

(2) Implementing and monitoring compliance with policies and procedures that require the destruction or erasure of electronic media and other nonpaper media containing personal information so that the information cannot practicably be read or reconstructed; and

(3) Describing procedures relating to the adequate destruction or proper disposal of personal records as official policy in the writings of the business entity.

(c) A business or government agency may satisfy its obligation hereunder by exercising due diligence and entering into a written contract with, and thereafter monitoring compliance by, another party engaged in the business of records destruction to destroy personal information in a manner consistent with this section. Due diligence should ordinarily include one or more of the following:

(1) Reviewing an independent audit of the disposal business' operations or its compliance with this chapter;

(2) Obtaining information about the disposal business from several references or other reliable sources and requiring that the disposal business be certified by a recognized trade association or similar third party with a reputation for high standards of quality review; or

(3) Reviewing and evaluating the disposal business' information security policies or procedures, or taking other appropriate measures to determine the competency and integrity of the disposal business.

(d) A disposal business that conducts business in Hawaii or disposes of personal information of residents of Hawaii shall take reasonable measures to dispose of records containing personal information by implementing and monitoring compliance with policies and procedures that protect against unauthorized access to, or use of, personal information during or after the collection, transportation, and disposing of such information.

(e) This chapter shall not apply to any of the following:

(1) Any financial institution that is subject to 15 U.S.C. sections 6801 to 6809, as amended;

(2) Any health plan or healthcare provider that is subject to and in compliance with the standards for privacy of 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; or

(3) Any consumer reporting agency that is subject to and in compliance with the Fair Credit Reporting Act, 15 U.S.C. sections 1681 to 1681x. [L 2006, c 136, pt of §2; am L 2008, c 19, §72]

[\$487R-3] Penalties; civil action. (a) Any business that violates any provision of this chapter shall be subject to penalties of not more than \$2,500 for each violation. The attorney general or the executive director of the office of consumer protection may bring an action pursuant to this section. No such action may be brought against a government agency.

(b) In addition to any penalty provided for in subsection (a), any business that violates any provision of this chapter shall be 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. 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.

(c) The penalties provided in this section shall be cumulative to the remedies or penalties available under all other laws of this State. [L 2006, c 136, pt of §2]

