CHAPTER 487N
[SECURITY BREACH OF PERSONAL INFORMATION]

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]

Previous Vol11_Ch0476-0490 Next

§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]

Previous Vol11_Ch0476-0490 Next

[§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]

Previous Vol11_Ch0476-0490 Next

[§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]

Previous Vol11 Ch0476-0490 Next

[§487N-5] Information privacy and security council; established; duties; reports. (a) There is established an information privacy and security council within the department of accounting and general services for administrative purposes only. Members of the council shall be appointed no later than September 1, 2008, by the governor without regard to section 26-34 and shall be composed of the following representatives:

(1) Executive agencies that maintain extensive personal information in the conduct of their duties, including the department of education, the department of health, the department of human resources development, the department of human services, and the University of Hawaii, to be selected by the governor;

(2) The legislature, to be selected by the president of the senate and the speaker of the house of representatives;

(3) The judiciary, to be selected by the administrator of the courts; and

(4) The four counties, to be selected by the mayor of each county; provided that the mayor of each county shall determine the extent to which the county may or may not participate.

The comptroller shall serve as chair of the council.

(b) By January 1, 2009, the council shall submit to the legislature a report of the council's assessment and recommendations on initiatives to mitigate the negative impacts of identity theft incidents on individuals. The report shall emphasize assessing the merits of identity theft passport and identity theft registry initiatives that have been implemented in other states.

(c) No later than June 30, 2009, the council shall develop guidelines to be considered by government agencies in deciding whether, how, and when a government agency shall inform affected individuals of the loss, disclosure, or security breach of personal information that can contribute to identify theft. The guidelines shall provide a standardized, risk-based notification process in the instance of a security breach.

(d) The council shall review the individual annual reports submitted by government agencies, pursuant to section 487N-7 and submit a summary report to the legislature no later than twenty days prior to the convening of the regular session of 2010 and each year thereafter. The summary report shall include the council's findings, significant trends, and recommendations to protect personal information used by government agencies.

The initial report to the legislature also shall include proposed legislation to amend section 487N-2 or any other law that the council deems necessary to conform to the guidelines established under subsection (c).

(e) The comptroller may establish support positions for the information and communication services division, including but not limited to, legal support, information technology, human resources and

personnel, records management, and administrative support. [L Sp 2008, c 10, pt of §4]

Previous Vol11 Ch0476-0490 Next

[§487N-6] Personal information security; best practices; websites. (a) The council shall identify best practices to assist government agencies in improving security and privacy programs relating to personal information. No later than March 31, 2009, the council shall identify best practices relating to:

(1) Automated tools;

(2) Training;

(3) Processes; and

(4) Applicable standards.

(b) No later than July 31, 2009, the best practices identified by the council shall be posted on each government agency's website in a manner that is readily accessible by employees of the government agency. [L Sp 2008, c 10, pt of §4]

Previous Vol11 Ch0476-0490 Next

[§487N-7] Personal information system; government agencies; annual report. (a) Effective January 1, 2009, any government agency that maintains one or more personal information systems shall submit to the council an annual report on the existence and character of each personal information system added or eliminated since the agency's previous annual report. The annual report shall be submitted no later than September 30 of each year.

(b) The annual report shall include:

(1) The name or descriptive title of the personal information system and its location;

(2) The nature and purpose of the personal information system and the statutory or administrative authority for its establishment;

(3) The categories of individuals on whom personal information is maintained, including:

(A) The approximate number of all individuals on whom personal information is maintained; and

(B) The categories of personal information generally maintained in the system, including identification of records that are:

(i) Stored in computer accessible records; or

(ii) Maintained manually;

(4) All confidentiality requirements relating to:

(A) Personal information systems or parts thereof that are confidential pursuant to statute, rule, or contractual obligation; and

(B) Personal information systems maintained on an unrestricted basis;

(5) Detailed justification of the need for statutory or regulatory authority to maintain any personal information system or part thereof on a confidential basis for all personal information systems or parts thereof that are required by law or rule;

(6) The categories of sources of personal information;

(7) The agency's policies and practices regarding personal information storage, duration of retention of information, and elimination of information from the system;

(8) The uses made by the agency of personal information contained in any personal information system;

(9) The identity of agency personnel, by job classification, and other agencies, persons, or categories to whom disclosures of personal information are made or

to whom access to the personal information system may be granted, including the purposes of access and any restrictions on disclosure, access, and redisclosure;

(10) A list identifying all forms used by the agency in the collection of personal information; and

(11) The name, title, business address, and telephone number of the individual immediately responsible for complying with this section.

(c) For purposes of this section:

"Personal information system" means any manual or automated recordkeeping process that contains personal information and the name, personal number, or other identifying particulars of a data subject.

(d) Notwithstanding any other law to the contrary, this report shall be confidential and not disclosed publicly in any form or forum. [L Sp 2008, c 10, pt of §4]

Previous Vol11 Ch0476-0490 Next