

**CHAPTER 379**

**H.P. 1180 - L.D. 1671**

**An Act To Protect Maine Citizens from Identity Theft**

**Be it enacted by the People of the State of Maine as follows:**

**Sec. 1. 10 MRSA c. 210-B** is enacted to read:

**CHAPTER 210-B**

**NOTICE OF RISK TO PERSONAL DATA**

**§1346. Short title**

This chapter may be known and cited as "the Notice of Risk to Personal Data Act."

**§1347. Definitions**

As used in this chapter, unless the context otherwise indicates, the following terms have the following meanings.

1. **Breach of the security of the system.** "Breach of the security of the system" or "security breach" means unauthorized acquisition of an individual's computerized data that compromises the security, confidentiality or integrity of personal information of the individual maintained by an information broker. Good faith acquisition of personal information by an employee or agent of an information broker for the purposes of the information broker is not a breach of the security of the system if the personal information is not used for or subject to further unauthorized disclosure.

2. Encryption. "Encryption" means the disguising of data using generally accepted practices.

3. Information broker. "Information broker" means a person who, for monetary fees or dues, engages in whole or in part in the business of collecting, assembling, evaluating, compiling, reporting, transmitting, transferring or communicating information concerning individuals for the primary purpose of furnishing personal information to nonaffiliated 3rd parties. "Information broker" does not include a governmental agency whose records are maintained primarily for traffic safety, law enforcement or licensing purposes.

4. Notice. "Notice" means:

A. Written notice;

B. Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 United States Code, Section 7001; or

C. Substitute notice, if the information broker demonstrates that the cost of providing notice would exceed \$5,000, that the affected class of individuals to be notified exceeds 1,000 or that the information broker does not have sufficient contact information to provide written or electronic notice to those individuals. Substitute notice must consist of all of the following:

(1) E-mail notice, if the information broker has e-mail addresses for the individuals to be notified;

(2) Conspicuous posting of the notice on the information broker's publicly accessible website, if the information broker maintains one; and

(3) Notification to major statewide media.

5. Person. "Person" means an individual, partnership, corporation, limited liability company, trust, estate, cooperative, association or other entity. "Person" as used in this chapter may not be construed to require duplicative notice by more than one individual, corporation, trust, estate, cooperative, association or other entity involved in the same transaction.

6. Personal information. "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 or redacted:

A. Social security number;

B. Driver's license number or state identification card number;

C. Account number, credit card number or debit card number, if circumstances exist wherein such a number could be used without additional identifying information, access codes or passwords;

D. Account passwords or personal identification numbers or other access codes; or

E. Any of the data elements contained in paragraphs A to D when not in connection with the individual's first name, or first initial, and last name, if the information if compromised would be sufficient to permit a person to fraudulently assume or attempt to assume the identity of the person whose information was compromised.

"Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media.

7. System. "System" means a computerized data storage system containing personal information.

8. Unauthorized person. "Unauthorized person" means a person who does not have authority or permission of an information broker to access personal information maintained by the information broker or who obtains access to such information by fraud, misrepresentation, subterfuge or similar deceptive practices.

### §1348. Security breach notice requirements

1. Notification to residents. An information broker that maintains computerized data that includes personal information shall give notice of a breach of the security of the system following discovery or notification of the security breach to a resident of this State whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The notice must be made as expeditiously as possible and without unreasonable delay, consistent with the legitimate needs of law enforcement pursuant to subsection 3 or with measures

necessary to determine the scope of the security breach and restore the reasonable integrity, security and confidentiality of the data in the system.

**2. Notification to information broker.** A person that maintains, on behalf of an information broker, computerized data that includes personal information that the person does not own shall notify the information broker of a breach of the security of the system immediately following discovery if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

**3. Delay of notification for law enforcement purposes.** The notification required by this section may be delayed if a law enforcement agency determines that the notification will compromise a criminal investigation; the notification required by this section must be made after the law enforcement agency determines that it will not compromise the investigation.

**4. Notification to consumer reporting agencies.** If an information broker discovers a breach of the security of the system that requires notification to more than 1,000 persons at a single time, the information broker shall also notify, without unreasonable delay, consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 United States Code, Section 1681a(p).

**5. Notification to state regulators.** When notice of a breach of the security of the system is required under subsection 1, the information broker shall notify the appropriate state regulators within the Department of Professional and Financial Regulation, or if the information broker is not regulated by the department, the Attorney General.

#### **§1349. Enforcement; penalties**

**1. Enforcement.** The appropriate state regulators within the Department of Professional and Financial Regulation shall enforce this chapter for any information broker that is licensed or regulated by those regulators. The Attorney General shall enforce this chapter for all other information brokers.

**2. Civil violation.** An information broker that violates this chapter commits a civil violation and is subject to one or more of the following:

A. A fine of not more than \$500 per violation, up to a maximum of \$2,500 for each day the information broker is in violation of this chapter;

B. Equitable relief; or

C. Enjoinment from further violations of this chapter.

3. Cumulative effect. The rights and remedies available under this section are cumulative and do not affect or prevent rights and remedies available under federal or state law.

**Sec. 2. Data security and security breach study; report.** The Department of Professional and Financial Regulation, in conjunction with the Attorney General, other financial regulatory agencies, business representatives, other interested parties that store electronic consumer data and consumer representatives, shall conduct a study regarding data security and security breach requirements. The study must include, but is not limited to, current electronic data security plans used by businesses; the value, practicality and costs of imposing additional requirements, including notification requirements, on businesses; California law governing security breach and notification requirements; and the right to private cause of action for a person injured by a violation of security breach notification law. The Department of Professional and Financial Regulation shall report its findings, including any proposed legislation, to the Joint Standing Committee on Insurance and Financial Services, by February 1, 2006. Following receipt and review of the report required under this section and the report required under section 3, the Joint Standing Committee on Insurance and Financial Services may report out a bill related to the reports to the Second Regular Session of the 122nd Legislature.

**Sec. 3. Security of information maintained by State Government; report.** No later than February 1, 2006, the Chief Information Officer within the Department of Administrative and Financial Services shall report to the Joint Standing Committee on Insurance and Financial Services regarding the State's current and planned-for policies, strategies and systems to protect the privacy and security of electronic personal information maintained by State Government.

**Sec. 4. Effective date.** That section of this Act that enacts the Maine Revised Statutes, Title 10, chapter 210-B takes effect January 31, 2006.