122nd MAINE LEGISLATURE

FIRST SPECIAL SESSION-2005

Legislative Document **No. 1671**

H.P. 1180 House of Representatives, May 12, 2005

An Act To Protect Maine Citizens from Identity Theft

(AFTER DEADLINE)

Approved for introduction by a majority of the Legislative Council pursuant to Joint Rule 205.

Reference to the Committee on Business, Research and Economic Development suggested and ordered printed.

Millicent M. MacFarland

MILLICENT M. MacFARLAND
Clerk

Presented by Representative PELLETIER-SIMPSON of Auburn.
Cosponsored by Senator HOBBINS of York and
Representatives: BRAUTIGAM of Falmouth, CANAVAN of Waterville, FAIRCLOTH of Bangor, Senator: SULLIVAN of York.

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. Business. "Business" means a person, including a corporation, doing business in the State.

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

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

A. Social security number;

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

C. Account number or credit or debit card number in combination with any required security code, access code or password that would permit access to an individual's account or financial records as defined in Title 9-B, section 161.

4. Reasonable notification procedures. "Reasonable notification procedures," with respect to a security breach, means procedures that:

A. Use a security program reasonably designed to block unauthorized transactions before they are charged to a customer's account;

B. Provide for notice to be given to a subject person by the owner or licensee of a database or an agent of the owner or licensee after the security program required under

paragraph A indicates that the security breach has resulted in fraud or unauthorized transactions, but do not necessarily require notice in other circumstances; and

C. Are subject to examination for compliance with the requirements of this chapter by one or more federal functional regulators, as defined in the federal Gramm-Leach-Bliley Act, 15 United States Code, Section 6809(2), or by the Department of Professional and Financial Regulation, Office of Consumer Credit Regulation with respect to the operation of the security program and the notification procedures.

5. Security breach. "Security breach" means the compromise of the security, confidentiality or integrity of computerized data that results in unauthorized acquisition of and access to personal information maintained by a business or that creates a reasonable basis for the conclusion that such acquisition has occurred. "Security breach" does not include the good faith acquisition of personal information by an employee or agent of a business for the purposes of that business if the personal information is not used or subject to further unauthorized disclosure.

6. Subject person. "Subject person" means a resident of this State whose personal information is stored by a business that has suffered a security breach resulting in the disclosure or possible disclosure of the resident's personal information.

7. Substitute notice. "Substitute notice" means:

A. An e-mail notice, if the business has the e-mail addresses of its customers;

B. A conspicuous posting of the notice on a publicly accessible website of the business; or

C. Publication in major media, including newspapers of general circulation.

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

§1348. Database security

1. Disclosure of security breach to subject person. A business that owns or licenses electronic data containing personal information, following the discovery of a security breach, shall notify the subject person whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

2. Notification to owner or licensee. A business in possession of electronic data containing personal information that the business does not own or license shall notify the owner or licensee of the personal information if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person through a security breach.

3. Timeliness of notification. Except as provided in subsection 4, notification required pursuant to subsections 1 and 2 must be made as expediently as possible and without unreasonable delay following:

A. The discovery by the business of a security breach; and

B. Any measures necessary to determine the scope of the security breach, prevent further disclosures and restore the reasonable integrity of the system.

4. Delay of notification for law enforcement purposes. Notwithstanding subsections 1 and 2, if a law enforcement agency determines that the notification required under this section would impede a criminal investigation, notification may be delayed until that law enforcement agency determines that the notification will no longer compromise the investigation.

5. Methods of notice. A business is considered to be in compliance with this section if the business provides the subject person with:

A. Written notice by regular, first-class mail; or

B. Substitute notice, if:

(1) The business demonstrates to the Director of the Office of Consumer Credit Regulation within the Department of Professional and Financial Regulation that the cost of providing direct notice would exceed $250,000;

(2) The number of subject persons to be notified exceeds 500,000; or

(3) The business does not have sufficient contact information to notify the subject persons.

6. Alternative notification procedures. Notwithstanding the requirements of subsections 1 and 2, a business is in compliance with the requirements of this chapter if the business maintains its own reasonable notification procedures as part of a security policy for personal information and notifies subject

persons in accordance with that security policy in the event of a security breach.

§1349. Enforcement; penalties

1. Enforcement. The Department of Professional and Financial Regulation, Office of Consumer Credit Regulation is responsible for enforcement of this chapter.

2. Civil violation. A business that violates this chapter commits a civil violation and is subject to the following:

A. A fine of not more than $5,000 per violation, up to a maximum of $25,000 per each day the business is in violation of this chapter;

B. Equitable relief; or

C. Enjoinment from further violations of this chapter.

3. Other rights and remedies. In addition to a civil penalty assessed or relief provided pursuant to subsection 2, a subject person injured by a violation of this chapter may bring a civil action against the business to recover damages.

4. 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.

SUMMARY

This bill requires an entity engaged in business in Maine that is in possession of electronic data containing personal information to disclose any unauthorized acquisition or suspected unauthorized acquisition of that personal information to a person whose personal information may have been acquired.