An Act To Amend the Notice of Risk to Personal Data Act

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

Sec. 1. 5 MRSA §1973, sub-§7 is enacted to read:

7. Security standards for computerized data including personal information. The Chief Information Officer shall establish written standards for the security of computerized data, including personal information, maintained by state agencies and departments, including standards for notification to a resident of this State when an agency or department becomes aware of a breach of security with regard to personal information and if a reasonable investigation reveals that personal information has been misused or a reasonable possibility exists that personal information will be misused.

Sec. 2. 10 MRSA §1347, sub-§1, as enacted by PL 2005, c. 379, §1 and affected by §4, is amended to read:

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~~a person. Good faith acquisition of personal information by an employee or agent of ~~an information broker for the purposes of the information broker~~a person on behalf of the person is not a breach of the security of the system if the personal information is not used for or subject to further unauthorized disclosure.

Sec. 3. 10 MRSA §1347, sub-§4, ¶C, as enacted by PL 2005, c. 379, §1 and affected by §4, is amended to read:

C. Substitute notice, if the person maintaining personal 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 person maintaining personal 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~~person has e-mail addresses for the individuals to be notified;

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

(3) Notification to major statewide media.

Sec. 4. 10 MRSA §1347, sub-§5, as enacted by PL 2005, c. 379, §1 and affected by §4, is amended to read:

5. Person. "Person" means an individual, partnership, corporation, limited liability company, trust, estate, cooperative, association or other entity, including the University of Maine System, the Maine Community College System and private colleges and universities. "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. For purposes of this chapter, "person" does not include an agency of State Government.

Sec. 5. 10 MRSA §1347, sub-§8, as enacted by PL 2005, c. 379, §1 and affected by §4, is amended to read:

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

Sec. 6. 10 MRSA §1348, sub-§1, as enacted by PL 2005, c. 379, §1 and affected by §4, is repealed and the following enacted in its place:

1. Notification to residents. The following provisions apply to notification to residents by information brokers and other persons.

A. If an information broker that maintains computerized data that includes personal information becomes aware of a breach of the security of the system, the information broker shall conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused and 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 has been, or is reasonably believed to have been, acquired by an unauthorized person.

B. If any other person who maintains computerized data that includes personal information becomes aware of a breach of the security of the system, the person shall conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused and 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 if misuse of the personal information has occurred or if it is reasonably possible that misuse will occur.

The notices required under paragraphs A and B must be made as expediently 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.

Sec. 7. 10 MRSA §1348, sub-§2, as enacted by PL 2005, c. 379, §1 and affected by §4, is amended to read:

2. Notification to person maintaining personal information. A ~~person~~3rd-party entity that maintains, on behalf of ~~an information broker~~a person, computerized data that includes personal information that the ~~person~~3rd-party entity does not own shall notify the ~~information broker~~person

maintaining personal information 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.

Sec. 8. 10 MRSA §1348, sub-§4, as enacted by PL 2005, c. 379, §1 and affected by §4, is amended to read:

4. Notification to consumer reporting agencies. If ~~an information broker~~a person 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~~person 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).

Sec. 9. 10 MRSA §1348, sub-§5, as enacted by PL 2005, c. 379, §1 and affected by §4, is amended to read:

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

Sec. 10. 10 MRSA §1349, sub-§1, as enacted by PL 2005, c. 379, §1 and affected by §4, is amended to read:

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

Sec. 11. 10 MRSA §1349, sub-§2, as enacted by PL 2005, c. 379, §1 and affected by §4, is amended to read:

2. Civil violation. ~~An information broker~~A person 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~~person is in violation of this chapter;

B. Equitable relief; or

C. Enjoinment from further violations of this chapter.

Sec. 12. 10 MRSA §1350 is enacted to read:

§ 1350. Private remedy

A person may bring a civil action and recover actual damages together with costs and reasonable attorney's fees if the person is injured by any of the following actions taken by a person subject to the provisions of this chapter:

1. Failure to conduct investigation. After becoming aware of a security breach, a person subject to the provisions of this chapter fails to conduct in good faith a reasonable and prompt investigation as required by this chapter; or

2. Failure to notify. After becoming aware of a security breach, a person subject to the provisions of this chapter fails to provide the notification as required by this chapter.

Sec. 13. 10 MRSA §1350-A is enacted to read:

§ 1350-A. Rulemaking

The appropriate state regulators within the Department of Professional and Financial Regulation may adopt rules as necessary for the administration and implementation of this chapter. Rules adopted pursuant to this section are routine technical rules as defined in Title 5, chapter 375, subchapter 2-A.

SUMMARY

This bill expands to other types of persons and businesses, including colleges and universities, the current requirement that information brokers notify consumers upon a security breach of the consumers' personal information. The bill also establishes a private cause of action for certain violations of the obligation to notify consumers.

The bill also requires the State's Chief Information Officer to develop standards and policies requiring notification by state agencies to Maine residents upon a security breach of personal information.