Maine Revised Statutes
Title 10 – Commerce and Trade
Part 3 – Regulation of Trade
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 a person. Good faith acquisition of personal information by an employee or agent of 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.

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 person maintaining personal information 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 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 person has e-mail addresses for the individuals to be notified;

2) Conspicuous posting of the notice on the person's publicly accessible website, if the person 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, 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 the purposes of this chapter, “person” does not include an agency of the State Government.

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 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 information from 3rd-party claims databases maintained by property and casualty insurers or 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 a person maintaining personal information to access personal information maintained by the person or who obtains access to such information by fraud, misrepresentation, subterfuge or similar deceptive practices.

§ 1348. Security breach notice requirements

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.

2. NOTIFICATION TO PERSON MAINTAINING PERSONAL INFORMATION. A 3rd-party entity that maintains, on behalf of a person, computerized data that includes personal information that the 3rd-party entity does not own shall notify the 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.

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 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 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). Notification must include the date of the breach, an estimate of the number of persons affected by the breach, if known, and the actual or anticipated date that persons were or will be notified of the breach.

5. NOTIFICATION TO STATE REGULATORS. When notice of a breach of the security of the system is required under subsection 1, the person shall notify the appropriate state regulators within the Department of Professional and Financial Regulation, or if the person 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 person that is licensed or regulated by those regulators. The Attorney General shall enforce this chapter for all other persons.

2. CIVIL VIOLATION. 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 person is in violation of this chapter, except that this paragraph does not apply to State Government, the University of Maine System, the Maine Community College System or Maine Maritime Academy;

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.

4. EXCEPTIONS. A person that complies with the security breach notification requirements of rules, regulations, procedures or guidelines established pursuant to federal law or the law of this State is deemed to be in compliance with the requirements of this chapter as long as the law, rules, regulations or guidelines provide for notification procedures at least as protective as the notification requirements of this chapter.

§ 1350-A. Rules; education and compliance. The following provisions govern rules and education and compliance.

1. RULES. With respect to persons under the jurisdiction of the regulatory agencies of the Department of Professional and Financial Regulation, the appropriate state regulators within that department may adopt rules as necessary for the administration and

implementation of this chapter. With respect to all other persons, the Attorney General may adopt rules as necessary for the administration and implementation of this chapter. Rules adopted pursuant to this subsection are routine technical rules as defined in Title 5, chapter 375, subchapter 2-A.

2. EDUCATION AND COMPLIANCE. The appropriate state regulators within the Department of Professional and Financial Regulation shall undertake reasonable efforts to inform persons under the department's jurisdiction of their responsibilities under this chapter. With respect to all other persons, the Attorney General shall undertake reasonable efforts to inform such persons of their responsibilities under this chapter.