



AN ACT REQUIRING STATE AGENCIES TO PROTECT CERTAIN PERSONAL INFORMATION; REQUIRING STATE AGENCIES TO DEVELOP PROCEDURES TO PROTECT SOCIAL SECURITY NUMBERS; AND PROVIDING A NOTIFICATION PROCEDURE FOR STATE AGENCIES OR THIRD PARTIES REGARDING A BREACH SUSPECTED OF COMPROMISING CERTAIN PERSONAL INFORMATION.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF MONTANA:

**Section 1. Definitions.** For the purposes of [sections 1 through 4], the following definitions apply:

(1) "Breach of the security of a data system" or "breach" means unauthorized acquisition of computerized data that:

(a) materially compromises the security, confidentiality, or integrity of the personal information maintained by a state agency or by a third party on behalf of the state agency; and

(b) causes or is reasonably believed to cause loss or injury to a person.

(2) "Individual" means a human being.

(3) "Person" means an individual, a partnership, a corporation, an association, or a public organization of any character.

(4) (a) "Personal information" means a first name or first initial and last name in combination with any one or more of the following data elements when the name and the data elements are not encrypted:

(i) a social security number or tax identification number;

(ii) a driver's license number, an identification number issued pursuant to 61-12-501, a tribal identification number or enrollment number, or a similar identification number issued by any state, the District of Columbia, the Commonwealth of Puerto Rico, Guam, the Virgin Islands, or American Samoa; or

(iii) an account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to a person's financial account.

(b) The term does not include publicly available information that is lawfully made available to the general public from federal, state, local, or tribal government records.

(5) "Redaction" means the alteration of personal information contained within data to make all or a significant part of the data unreadable. The term includes truncation, which means that no more than the last four digits of an identification number are accessible as part of the data.

(6) (a) "State agency" means an agency, authority, board, bureau, college, commission, committee, council, department, hospital, institution, office, university, or other instrumentality of the legislative or executive branch of state government. The term includes an employee of a state agency acting within the course and scope of employment.

(b) The term does not include an entity of the judicial branch.

(7) "Third party" means:

(a) a person with a contractual obligation to perform a function for a state agency; or

(b) a state agency with a contractual or other obligation to perform a function for another state agency.

**Section 2. Protection of social security numbers -- compliance.** (1) Each state agency that maintains the social security number of an individual shall develop procedures to protect the social security number while enabling the state agency to use the social security number as necessary for the performance of its duties under federal or state law.

(2) The procedures must include measures to:

(a) eliminate the unnecessary use of social security numbers;

(b) identify the person or state agency authorized to have access to a social security number;

(c) restrict access to social security numbers by unauthorized persons or state agencies;

(d) identify circumstances when redaction of social security numbers is appropriate;

(e) dispose of documents that contain social security numbers in a manner consistent with other record retention requirements applicable to the state agency;

(f) eliminate the unnecessary storage of social security numbers on portable devices; and

(g) protect data containing social security numbers if that data is on a portable device.

(3) Except as provided in [section 3], each state agency in existence on [the effective date of this act] shall complete the requirements of this section by September 1, 2012. A state agency that is created after [the effective date of this act] shall complete the requirements of this section within 1 year of its creation.

**Section 3. Extensions.** The chief information officer provided for in 2-17-511 may grant an extension to any state agency subject to the provisions of the Montana Information Technology Act provided for in Title 2, chapter 17, part 5. The chief information officer shall inform the information technology board, the office of budget and program planning, and the legislative finance committee of all extensions that are granted and of the rationale for granting the extensions. The chief information officer shall maintain written documentation that identifies the terms and conditions of each extension and the rationale for the extension.

**Section 4. Notification of breach of security of data system.** (1) (a) Upon discovery or notification of a breach of the security of a data system, a state agency that maintains computerized data containing personal information in the data system shall make reasonable efforts to notify any person whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person.

(b) The notification must be made without unreasonable delay, consistent with the legitimate needs of law enforcement as provided in subsection (3) or with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the data system.

(2) (a) A third party that receives personal information from a state agency and maintains that information in a computerized data system in order to perform a state agency function shall:

(i) notify the state agency immediately following discovery of the breach of the security of a data system if the personal information is reasonably believed to have been acquired by an unauthorized person; and

(ii) make reasonable efforts upon discovery or notification of a breach of the security of a data system to notify any person whose unencrypted personal information is reasonably believed to have been acquired by an unauthorized person as part of the breach of the security of a data system. This notification must be provided in the same manner as the notification required in subsection (1).

(b) A state agency notified of a breach by a third party has no independent duty to provide notification of the breach if the third party has provided notification of the breach in the manner required by subsection (2)(a) but shall provide notification if the third party fails to do so in a reasonable time and may recover from the third party its reasonable costs for providing the notice.

(3) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation and requests a delay of notification. The notification required by this section must be made after the law enforcement agency determines that the notification will not

compromise the investigation.

(4) All state agencies and third parties to whom personal information is disclosed by a state agency shall develop and maintain:

- (a) an information security policy designed to safeguard personal information; and
- (b) breach notification procedures that provide reasonable notice to individuals as provided in subsections (1) and (2).

**Section 5. Codification instruction.** [Sections 1 through 4] are intended to be codified as an integral part of Title 2, and the provisions of Title 2 apply to [sections 1 through 4].

- END -

I hereby certify that the within bill,  
HB 0155, originated in the House.

---

Chief Clerk of the House

---

Speaker of the House

Signed this \_\_\_\_\_ day  
of \_\_\_\_\_, 2009.

---

President of the Senate

Signed this \_\_\_\_\_ day  
of \_\_\_\_\_, 2009.

HOUSE BILL NO. 155

INTRODUCED BY J. POMNICHOWSKI

BY REQUEST OF THE DEPARTMENT OF ADMINISTRATION

AN ACT REQUIRING STATE AGENCIES TO PROTECT CERTAIN PERSONAL INFORMATION; REQUIRING STATE AGENCIES TO DEVELOP PROCEDURES TO PROTECT SOCIAL SECURITY NUMBERS; AND PROVIDING A NOTIFICATION PROCEDURE FOR STATE AGENCIES OR THIRD PARTIES REGARDING A BREACH SUSPECTED OF COMPROMISING CERTAIN PERSONAL INFORMATION.