Chapter 44
Protection of Personal Information Act

Part 1
General Provisions

13-44-101 Title.

This chapter is known as the "Protection of Personal Information Act."

Amended by Chapter 61, 2009 General Session

13-44-102 Definitions.

As used in this chapter:

(1)
(a) "Breach of system security" means an unauthorized acquisition of computerized data maintained by a person that compromises the security, confidentiality, or integrity of personal information.
(b) "Breach of system security" does not include the acquisition of personal information by an employee or agent of the person possessing unencrypted computerized data unless the personal information is used for an unlawful purpose or disclosed in an unauthorized manner.

(2) "Consumer" means a natural person.

(3)
(a) "Personal information" means a person's first name or first initial and last name, combined with any one or more of the following data elements relating to that person when either the name or date element is unencrypted or not protected by another method that renders the data unreadable or unusable:
(i) Social Security number;
(ii)
(A) financial account number, or credit or debit card number; and
(B) any required security code, access code, or password that would permit access to the person's account; or
(iii) driver license number or state identification card number.
(b) "Personal information" does not include information regardless of its source, contained in federal, state, or local government records or in widely distributed media that are lawfully made available to the general public.

(4) "Record" includes materials maintained in any form, including paper and electronic.

Enacted by Chapter 343, 2006 General Session

Part 2
Protection of Personal Information

13-44-201 Protection of personal information.

(1) Any person who conducts business in the state and maintains personal information shall implement and maintain reasonable procedures to:

(a) prevent unlawful use or disclosure of personal information collected or maintained in the regular course of business; and
(b) destroy, or arrange for the destruction of, records containing personal information that are not to be retained by the person.
(2) The destruction of records under Subsection (1)(b) shall be by:
(a) shredding;
(b) erasing; or
(c) otherwise modifying the personal information to make the information indecipherable.
(3) This section does not apply to a financial institution as defined by 15 U.S.C. Section 6809.

Enacted by Chapter 343, 2006 General Session

13-44-202 Personal information -- Disclosure of system security breach.

(1)
(a) A person who owns or licenses computerized data that includes personal information concerning a Utah resident shall, when the person becomes aware of a breach of system security, conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused for identity theft or fraud purposes.
(b) If an investigation under Subsection (1)(a) reveals that the misuse of personal information for identity theft or fraud purposes has occurred, or is reasonably likely to occur, the person shall provide notification to each affected Utah resident.
(2) A person required to provide notification under Subsection (1) shall provide the notification in the most expedient time possible without unreasonable delay:
(a) considering legitimate investigative needs of law enforcement, as provided in Subsection (4)(a);
(b) after determining the scope of the breach of system security; and
(c) after restoring the reasonable integrity of the system.
(3)
(a) A person who maintains computerized data that includes personal information that the person does not own or license shall notify and cooperate with the owner or licensee of the information of any breach of system security immediately following the person's discovery of the breach if misuse of the personal information occurs or is reasonably likely to occur.
(b) Cooperation under Subsection (3)(a) includes sharing information relevant to the breach with the owner or licensee of the information.
(4)
(a) Notwithstanding Subsection (2), a person may delay providing notification under Subsection (1) at the request of a law enforcement agency that determines that notification may impede a criminal investigation.
(b) A person who delays providing notification under Subsection (4)(a) shall provide notification in good faith without unreasonable delay in the most expedient time possible after the law enforcement agency informs the person that notification will no longer impede the criminal investigation.
(5)
(a) A notification required by this section may be provided:
(i) in writing by first-class mail to the most recent address the person has for the resident;

(ii) electronically, if the person's primary method of communication with the resident is by electronic means, or if provided in accordance with the consumer disclosure provisions of 15 U.S.C. Section 7001;
(iii) by telephone, including through the use of automatic dialing technology not prohibited by other law; or
(iv) by publishing notice of the breach of system security:
(A) in a newspaper of general circulation; and
(B) as required in Section 45-1-101.
(b) If a person maintains the person's own notification procedures as part of an information security policy for the treatment of personal information the person is considered to be in compliance with this chapter's notification requirements if the procedures are otherwise consistent with this chapter's timing requirements and the person notifies each affected Utah resident in accordance with the person's information security policy in the event of a breach.
(c) A person who is regulated by state or federal law and maintains procedures for a breach of system security under applicable law established by the primary state or federal regulator is considered to be in compliance with this part if the person notifies each affected Utah resident in accordance with the other applicable law in the event of a breach.
(6) A waiver of this section is contrary to public policy and is void and unenforceable.

Amended by Chapter 388, 2009 General Session

Part 3
Enforcement

13-44-301 Enforcement.
(1) The attorney general may enforce this chapter's provisions.
(2)
(a) Nothing in this chapter creates a private right of action.
(b) Nothing in this chapter affects any private right of action existing under other law, including contract or tort.
(3) A person who violates this chapter's provisions is subject to a civil fine of:
(a) no greater than $2,500 for a violation or series of violations concerning a specific consumer; and
(b) no greater than $100,000 in the aggregate for related violations concerning more than one consumer.
(4) In addition to the penalties provided in Subsection (3), the attorney general may seek injunctive relief to prevent future violations of this chapter in:
(a) the district court located in Salt Lake City; or
(b) the district court for the district in which resides a consumer who is affected by the violation.
(5) In enforcing this chapter, the attorney general may:
(a) investigate the actions of any person alleged to violate Section 13-44-201 or 13-44-202;
(b) subpoena a witness;
(c) subpoena a document or other evidence;
(d) require the production of books, papers, contracts, records, or other information relevant to an investigation; and

(e) conduct an adjudication in accordance with Title 63G, Chapter 4, Administrative Procedures Act, to enforce a civil provision under this chapter.

(6) A subpoena issued under Subsection (5) may be served by certified mail.

(7) A person's failure to respond to a request or subpoena from the attorney general under Subsection (5)(b), (c), or (d) is a violation of this chapter.

(8)

(a) The attorney general may inspect and copy all records related to the business conducted by the person alleged to have violated this chapter, including records located outside the state.

(b) For records located outside of the state, the person who is found to have violated this chapter shall pay the attorney general's expenses to inspect the records, including travel costs.

(c) Upon notification from the attorney general of the attorney general's intent to inspect records located outside of the state, the person who is found to have violated this chapter shall pay the attorney general $500, or a higher amount if $500 is estimated to be insufficient, to cover the attorney general's expenses to inspect the records.

(d) The attorney general shall deposit any amounts received under this Subsection (8) in the Attorney General Litigation Fund established in Section 76-10-3114.

(e) To the extent an amount paid to the attorney general by a person who is found to have violated this chapter is not expended by the attorney general, the amount shall be refunded to the person who is found to have violated this chapter.

(f) The Division of Corporations and Commercial Code or any other relevant entity shall revoke any authorization to do business in this state of a person who fails to pay any amount required under this Subsection (8).

Amended by Chapter 187, 2013 General Session