LEGISLATIVE GENERAL COUNSEL
₵ Approved for Filing: R. Strong ₵
₵ 02-22-22 8:23 AM ₵

CONSUMER DATA PRIVACY AMENDMENTS

2022 GENERAL SESSION

STATE OF UTAH

Chief Sponsor: Clare Collard

Senate Sponsor: _____

LONG TITLE

General Description:

This bill amends provisions related to the protection of personal information.

Highlighted Provisions:

This bill:

- defines terms;
- clarifies the applicability of existing provisions of the Protection of Personal Information Act to agencies;
- subjects agencies to certain personal information protection requirements; and
- authorizes the attorney general to use an injunction to enforce provisions related to agencies.

Money Appropriated in this Bill:

None

Other Special Clauses:

None

Utah Code Sections Affected:

AMENDS:

13-44-102, as last amended by Laws of Utah 2019, Chapter 348

13-44-201, as last amended by Laws of Utah 2019, Chapter 348

13-44-202, as last amended by Laws of Utah 2019, Chapter 348

13-44-301, as last amended by Laws of Utah 2019, Chapter 348

H.B. 457

ENACTS:

13-44-401, Utah Code Annotated 1953

13-44-402, Utah Code Annotated 1953

13-44-403, Utah Code Annotated 1953

Be it enacted by the Legislature of the state of Utah:

Section 1. Section **13-44-102** is amended to read:

13-44-102. Definitions.

As used in this chapter:

(1) "Agency" means each department, commission, board, council, agency, institution, corporation, fund, division, office, committee, authority, laboratory, library, unit, bureau, panel, or other administrative unit of the state.

(2) "Biometric data" means unique data generated from measurements or analysis of human body characteristics for the purpose of authenticating an individual when the individual accesses an online account.

[~~(1)~~] (3) (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)~~] (4) "Consumer" means a natural person.

[~~(3)~~] (5) "Financial institution" means the same as that term is defined in 15 U.S.C. Sec. 6809.

[~~(4)~~] (6) (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[~~.~~];

(iv) an identification number including:

(A) student;

(B) health insurance;

(C) military; and

(D) passport; or

(v) biometric data.

(b) "Personal information" includes a Utah consumer's username or email address, in combination with a password or security questions and answers, that would permit access to an online account.

[~~(b)~~] (c) "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.

[~~(5)~~] (7) "Record" includes materials maintained in any form, including paper and electronic.

Section 2. Section **13-44-201** is amended to read:

13-44-201. Protection of personal information.

(1) Any person who is not an agency 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.

Section 3. Section **13-44-202** is amended to read:

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) for residents of the state for whom notification in a manner described in Subsections (5)(a)(i) through (iii) is not feasible, 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.

(7) This section does not apply to a person who is an agency.

Section 4. Section **13-44-301** is amended to read:

13-44-301. Enforcement -- Confidentiality agreement -- Penalties.

(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 penalty 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, unless:

(i) the violations concern:

(A) 10,000 or more consumers who are residents of the state; and

(B) 10,000 or more consumers who are residents of other states; or

(ii) the person agrees to settle for a greater amount.

(4) (a) In addition to the penalties provided in Subsection (3), the attorney general may seek, in an action brought under this chapter:

(i) injunctive relief to prevent future violations of this chapter; and

(ii) attorney fees and costs.

(b) The attorney general shall bring an action under this chapter in:

(i) the district court located in Salt Lake City; or

(ii) the district court for the district in which resides a consumer who is affected by the violation.

(5) The attorney general shall deposit any amount received under Subsection (3), (4), or (10) into the Attorney General Litigation Fund created in Section 76-10-3114.

(6) 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;

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

(f) enter into a confidentiality agreement in accordance with Subsection (7).

(7) (a) If the attorney general has reasonable cause to believe that an individual is in possession, custody, or control of information that is relevant to enforcing this chapter, the attorney general may enter into a confidentiality agreement with the individual.

(b) In a civil action brought under this chapter, a court may issue a confidentiality order that incorporates the confidentiality agreement described in Subsection (7)(a).

(c) A confidentiality agreement entered into under Subsection (7)(a) or a

confidentiality order issued under Subsection (7)(b) may:

(i) address a procedure;

(ii) address testimony taken, a document produced, or material produced under this section;

(iii) provide whom may access testimony taken, a document produced, or material produced under this section;

(iv) provide for safeguarding testimony taken, a document produced, or material produced under this section; or

(v) require that the attorney general:

(A) return a document or material to an individual; or

(B) notwithstanding Section 63A-12-105 or a retention schedule created in accordance with Section 63G-2-604, destroy the document or material at a designated time.

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

(9) A person's failure to respond to a request or subpoena from the attorney general under Subsection (6)(b), (c), or (d) is a violation of this chapter.

(10) (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) 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.

(e) 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 (10).

(11) (a) Subject to Subsection (11)(c), the attorney general shall keep confidential a procedure agreed to, testimony taken, a document produced, or material produced under this section pursuant to a subpoena, confidentiality agreement, or confidentiality order, unless the individual who agreed to the procedure, provided testimony, produced the document, or produced material waives confidentiality in writing.

(b) Subject to Subsections (11)(c) and (11)(d), the attorney general may use, in an enforcement action taken under this section, testimony taken, a document produced, or material produced under this section to the extent the use is not restricted or prohibited by a confidentiality agreement or a confidentiality order.

(c) The attorney general may use, in an enforcement action taken under this section, testimony taken, a document produced, or material produced under this section that is restricted or prohibited from use by a confidentiality agreement or a confidentiality order if the individual who provided testimony or produced the document or material waives the restriction or prohibition in writing.

(d) The attorney general may disclose testimony taken, a document produced, or material produced under this section, without consent of the individual who provided the testimony or produced the document or material, or the consent of an individual being investigated, to:

(i) a grand jury; or

(ii) a federal or state law enforcement officer, if the person from whom the information was obtained is notified 20 days or greater before the day on which the information is disclosed, and the federal or state law enforcement officer certifies that the federal or state law enforcement officer will:

(A) maintain the confidentiality of the testimony, document, or material; and

(B) use the testimony, document, or material solely for an official law enforcement purpose.

(12) (a) An administrative action filed under this chapter shall be commenced no later than 10 years after the day on which the alleged breach of system security last occurred.

(b) A civil action under this chapter shall be commenced no later than five years after the day on which the alleged breach of system security last occurred.

(13) This section does not apply to a person who is an agency.

Section 5. Section **13-44-401** is enacted to read:

Part 4. Agency Protection of Personal Information

13-44-401. Agency protection of personal information.

(1) Any agency who maintains personal information shall implement and maintain reasonable procedures to:

(a) prevent unlawful use or disclosure of personal information the agency collects; and

(b) destroy, or arrange for the destruction of, records containing personal information that the agency is not retaining.

(2) The agency shall destroy the records under Subsection (1)(b) by:

(a) shredding;

(b) erasing; or

(c) otherwise modifying the personal information to make the personal information indecipherable.

Section 6. Section **13-44-402** is enacted to read:

13-44-402. Computerized data -- Disclosure of system security breach.

(1) (a) An agency who owns or licenses computerized data that includes personal information concerning a Utah resident shall, when the agency becomes aware of a breach of system security, conduct in good faith a reasonable and prompt investigation to determine the likelihood that the personal information concerning the Utah resident 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 agency shall provide notice to each affected Utah resident.

(2) An agency required to provide notice under Subsection (1) shall provide the notice 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) An agency who maintains computerized data that includes personal information that the agency 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 agency'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), an agency may delay providing notice under Subsection (1) at the request of a law enforcement agency that determines that notice may impede a criminal investigation.

(b) An agency who delays providing notice under Subsection (4)(a) shall provide notice in good faith without unreasonable delay in the most expedient time possible after the law enforcement agency informs the person that notice will no longer impede the criminal investigation.

(5) (a) An agency must provide notice:

(i) in writing by first-class mail to the most recent address the agency has for the Utah resident;

(ii) electronically, if the agency's primary method of communication with the Utah 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 law; or

(iv) for Utah residents for whom notification in a manner described in Subsections (5)(a)(i) through (iii) is not feasible, 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) An agency may adopt an agency's own notification procedures as part of an information security policy for the treatment of personal information if:

(i) the adopted procedures are consistent with this part's timing requirements; and

(ii) the agency notifies each affected Utah resident in accordance with the agency's information security policy in the event of a breach.

(c) An agency 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 in compliance with this part if the agency notifies each affected Utah resident in

accordance with the applicable state or federal law in the event of a breach.

(6) If an agency is required to notify more than 1,000 Utah residents in compliance with this section, the agency shall also notify, in good faith without unreasonable delay in the most expedient time possible:

(a) the attorney general; and

(b) all consumer reporting agencies that compile and maintain files on a nationwide basis, as defined in 15 U.S.C. Sec. 1681a(p), of the anticipated date of the notification to the residents and the approximate number of residents the agency will notify.

(7) A person may not waive an agency's requirement to comply with this section.

Section 7. Section **13-44-403** is enacted to read:

13-44-403. Attorney general enforcement.

The attorney general may bring an action for injunctive relief to enforce the provisions of this part.