Utah Code Ann. § 13-44-202

Current through May 1, 2024 of the 2024 General Session.

Utah Code Annotated > Title 13 Commerce and Trade (Chs. 1 — 74) > Chapter 44 Protection of Personal Information Act (Pts. 1 — 3) > Part 2 Protection of Personal Information (§§ 13-44-201 — 13-44-202)

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.

(c) If an investigation under Subsection (1)(a) reveals that the misuse of personal information relating to 500 or more Utah residents, for identity theft or fraud purposes, has occurred or is reasonably likely to occur, the person shall, in addition to the notification required in Subsection (1)(b), provide notification to:

(i) the Office of the Attorney General; and

(ii) the Utah Cyber Center created in Section 63A-16-1102.

(d) If an investigation under Subsection (1)(a) reveals that the misuse of personal information relating to 1,000 or more Utah residents, for identity theft or fraud purposes, has occurred or is reasonably likely to occur, the person shall, in addition to the notification required in Subsections (1)(b) and (c), provide notification to each consumer reporting agency that compiles and maintains files on consumers on a nationwide basis, as defined in 15 U.S.C. Sec. 1681a.

(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)(b) 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 Subsection (1)(b) 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 the notification requirement in Subsection (1)(b) 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) The following information may be deemed confidential and classified as a protected record under Subsections 63G-2-305 (1) and (2) if the requirements of Subsection 63G-2-309 (1)(a)(i) are met:

(i) a notification submitted under Subsection (1)(c), including supporting information provided under Subsection (6)(b); and

(ii) information produced by the Office of the Attorney General or the Utah Cyber Center in providing coordination or assistance to the person providing notification under Subsection (1)(c).

(b) A person providing notification under Subsection (1)(c) to the Office of the Attorney General or the Utah Cyber Center of a breach of system security shall include the following information in the notification, to the extent the information is known or available at the time the person provides the notification:

(i) the date the breach of system security occurred;

(ii) the date the breach of system security was discovered;

(iii) the total number of people affected by the breach of system security, including the total number of Utah residents affected;

(iv) the type of personal information involved in the breach of system security; and

(v) a short description of the breach of system security that occurred.

(7) A waiver of this section is contrary to public policy and is void and unenforceable.

History

C. 1953, 13-42-202, enacted by L. 2006, ch. 343, § 4; recompiled as § 13-44-202; 2009, ch. 388, § 61; 2019 ch. 348, § 4, effective May 14, 2019; 2023 ch. 496, § 1, effective May 3, 2023; 2024 ch. 426, § 1, effective May 1, 2024.

End of Document