1st Sub. S.B. 69
PROTECTION OF INFORMATION IN CONSUMER CREDIT DATABASES

SENATE FLOOR AMENDMENTS AMENDMENT 1 FEBRUARY 7, 2006 9:24 AM

Senator **Carlene M. Walker** proposes the following amendments:

1. *Page 2, Line 50 through Page 3, Line 64:*

(3) **(a)** "Personal information" means {~~:~~}

{~~(a)~~} a person's name {~~, address, or telephone number~~} combined with {~~the person's~~} **one or more of the following data elements relating to that person if the name or data element is unencrypted** :

(i) Social Security number;

(ii) (A) financial account, 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;

(iii) driver license number or other {~~government-issued~~} **comparable** identification number;

(iv) consumer report;

(v) employee number;

(vi) faculty or student identification number;

(vii) United States Armed Forces serial number; or

(viii) genetic or biometric information {~~; or~~} **.**

(b) **"Personal information" includes** any of the information listed in Subsections (3)(a)(i) through (viii) without the person's name {~~, address, or telephone number~~} if the information is sufficient to allow a person to obtain money, credit, or services through unauthorized use of the information.

(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.

2. *Page 3, Line 85 through Page 5, Line 125:*

13-42-202. Personal information -- Disclosure of system security breach.

{~~(1) (a) A person possessing personal information shall, upon becoming 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.~~

~~(b) If the investigation determines that the misuse of information about the resident of the state occurs or is highly likely to occur, the person shall disclose the breach to the resident.~~

~~(2) If a person is required to notify more than 10,000 residents of this state of a breach of system security under this section, the person shall also notify any consumer reporting~~

~~agency, as defined in 15 U.S.C. Section 1681a, that does business on a nationwide basis of the circumstances surrounding the required notification, including:~~

~~(a) when the notification is made;~~

~~(b) to whom the notification is made; and~~

~~(c) the extent of the breach of system security.~~

~~(3) (a) A person required to provide notification under Subsection (1) shall provide the notification as soon as possible after determining the scope of the breach of system security and restoring the integrity of the personal information in the person's possession.~~

~~(b) (i) Notwithstanding Subsection (3)(a), a person may delay providing a notification required by Subsection (1) at the request of a law enforcement agency that determines that notification could impede a criminal investigation.~~

~~(ii) A person who delays providing notification under Subsection (3)(b)(i) shall provide notice immediately after the law enforcement agency informs the person that notification will no longer impede the criminal investigation.~~ }

(1)(a) A person who owns or licenses computerized data that includes personal information about 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.

(b) If an investigation under Subsection (1)(a) reveals that the misuse of personal information has occurred, or is highly likely to occur, the person shall provide notification to each affected Utah resident as soon as possible.

(2) A person required to provide notification under Subsection (1) shall provide the notification as soon as possible:

(a) considering legitimate investigative needs of law enforcement;

(b) after determining the scope of the breach of system security; and

(c) after restoring the 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 highly 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 as soon as possible after the law enforcement agency informs the person that notification will no longer impede the criminal investigation.

{ ~~(4)~~ } (5) (a) A notification required by this section may be provided:

(i) in writing by first-class mail; or

(ii) electronically, if provided in accordance with the consumer disclosure provisions of 15 U.S.C. Section 7001.

(b) Notwithstanding Subsection {~~(4)~~} (5) (a), if the cost of providing notification will exceed $150,000, the number of affected persons exceeds 100,000, or the person does not have sufficient contact information for affected persons, the notice may be provided by:

(i) electronic mail, if the person has an electronic mail address for the affected person;

(ii) conspicuous posting on the person's Internet website; or

(iii) publishing and broadcasting notice in major, statewide media.

{~~(c) If a person possessing personal information maintains notification procedures substantially similar to those required by this section, that person need not provide the notification required by this section if the notification is nevertheless provided within the time period prescribed in this section.~~

~~(d) A person possessing personal information who is required by federal law to maintain procedures for a breach of system security is considered to be in compliance with this chapter if the person notifies state residents of a breach of system security in accordance with the federal procedures.~~} **(c) If a person maintains the person's own notification procedures as part of an information security policy for the treatment of personal information 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.**

(d) 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.

{~~(5)~~} (6) A waiver of this section is contrary to public policy and is void and unenforceable.