

Senator Carlene M. Walker proposes the following substitute bill:

**PROTECTION OF INFORMATION IN
CONSUMER CREDIT DATABASES**

2006 GENERAL SESSION

STATE OF UTAH

Chief Sponsor: Carlene M. Walker

House Sponsor: David Clark

LONG TITLE

General Description:

This bill addresses the integrity of consumer credit databases.

Highlighted Provisions:

This bill:

- ▶ defines terms;
- ▶ requires a person maintaining personal information in connection with a business to implement procedures to protect personal information;
- ▶ requires destruction of certain records;
- ▶ requires disclosure of breaches of databases containing personal information; and
- ▶ provides for enforcement by the attorney general.

Monies Appropriated in this Bill:

This bill appropriates from the General Fund to the attorney general:

- ▶ as an ongoing appropriation subject to future budget constraints, \$178,800 for fiscal year 2006-07; and
- ▶ \$46,000 for fiscal year 2006-07 only.

Other Special Clauses:

None



26 **Utah Code Sections Affected:**

27 ENACTS:

28 **13-42-101**, Utah Code Annotated 1953

29 **13-42-102**, Utah Code Annotated 1953

30 **13-42-201**, Utah Code Annotated 1953

31 **13-42-202**, Utah Code Annotated 1953

32 **13-42-301**, Utah Code Annotated 1953



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

35 Section 1. Section **13-42-101** is enacted to read:

36 **CHAPTER 42. CONSUMER CREDIT PROTECTION ACT**

37 **Part 1. General Provisions**

38 **13-42-101. Title.**

39 This chapter is known as the "Consumer Credit Protection Act."

40 Section 2. Section **13-42-102** is enacted to read:

41 **13-42-102. Definitions.**

42 As used in this chapter:

43 (1) (a) "Breach of system security" means an unauthorized acquisition of unencrypted
44 computerized records maintained by a person that compromises the security or confidentiality
45 of personal information contained in the records.

46 (b) "Breach of system security" does not include the acquisition of personal
47 information by an employee or agent of the person possessing records unless the personal
48 information is used or disclosed in an unauthorized manner.

49 (2) "Consumer" means a natural person.

50 (3) ~~§~~ (a) ~~§~~ "Personal information" means ~~§~~ [:

51 ~~(a)] ~~§~~ a person's name ~~§~~ [; address, or telephone number] ~~§~~ combined with ~~§~~ [the~~
51a person's] one or more of the following data elements relating to that person if the name or data
51b element is unencrypted ~~§~~ :

52 (i) Social Security number;

53 (ii) (A) financial account, or credit or debit card, number; and

54 (B) any required security code, access code, or password that would permit access to
55 the person's account;

56 (iii) driver license number or other ~~§~~ [government-issued] comparable ~~§~~ identification
56a number;

57 (iv) consumer report;

58 (v) employee number;

59 (vi) faculty or student identification number;

60 (vii) United States Armed Forces serial number; or

61 (viii) genetic or biometric information; or

62 (b) ~~§~~→ **"Personal information" includes** ~~←~~§ any of the information listed in Subsections

62a (3)(a)(i) through (viii) without the

63 person's name ~~§~~→ [~~;~~ **address, or telephone number**] ~~←~~§ if the information is sufficient to allow a

63a person

64 to obtain money, credit, or services through unauthorized use of the information.

64a **~~§~~→ (c) "Personal information" does not include information, regardless of its source, contained**

64b **~~in federal, state, or local government records or in widely distributed media that are lawfully~~**

64c **~~made available to the general public.~~ ~~←~~§**

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

66 electronic.

67 Section 3. Section **13-42-201** is enacted to read:

68 **Part 2. Protection of Personal Information**

69 **13-42-201. Protection of personal information.**

70 (1) Any person who conducts business in the state and maintains personal information

71 shall:

72 (a) implement and maintain reasonable procedures to prevent unlawful use or

73 disclosure of personal information collected or maintained in the regular course of business;

74 and

75 (b) destroy, or arrange for the destruction of, records containing personal information

76 that are not to be retained by the person.

77 (2) The destruction of records under Subsection (1)(b) shall be by:

78 (a) shredding;

79 (b) erasing; or

80 (c) otherwise modifying the personal information to make the information

81 indecipherable.

82 (3) This section does not apply to a financial institution as defined by 15 U.S.C.

83 Section 6809.

84 Section 4. Section **13-42-202** is enacted to read:

85 **13-42-202. Personal information -- Disclosure of system security breach.**

86 **~~§~~→ [(1) (a) A person possessing personal information shall, upon becoming aware of a**

87 **~~breach of system security, conduct in good faith a reasonable and prompt investigation to] ~~←~~§~~**

88 ~~§→ [determine the likelihood that personal information has been or will be misused:~~
89 ~~—— (b) If the investigation determines that the misuse of information about the resident of~~
90 ~~the state occurs or is highly likely to occur, the person shall disclose the breach to the resident.~~
91 ~~—— (2) If a person is required to notify more than 10,000 residents of this state of a breach~~
92 ~~of system security under this section, the person shall also notify any consumer reporting~~
93 ~~agency, as defined in 15 U.S.C. Section 1681a, that does business on a nationwide basis of the~~
94 ~~circumstances surrounding the required notification, including:~~
95 ~~—— (a) when the notification is made;~~
96 ~~—— (b) to whom the notification is made; and~~
97 ~~—— (c) the extent of the breach of system security.~~
98 ~~—— (3) (a) A person required to provide notification under Subsection (1) shall provide the~~
99 ~~notification as soon as possible after determining the scope of the breach of system security and~~
100 ~~restoring the integrity of the personal information in the person's possession.~~
101 ~~—— (b) (i) Notwithstanding Subsection (3)(a), a person may delay providing a notification~~
102 ~~required by Subsection (1) at the request of a law enforcement agency that determines that~~
103 ~~notification could impede a criminal investigation.~~
104 ~~—— (ii) A person who delays providing notification under Subsection (3)(b)(i) shall provide~~
105 ~~notice immediately after the law enforcement agency informs the person that notification will~~
106 ~~no longer impede the criminal investigation.]~~

106a (1)(a) A person who owns or licenses computerized data that includes personal information
106b about a Utah resident shall, when the person becomes aware of a breach of system security,
106c conduct in good faith a reasonable and prompt investigation to determine the likelihood that
106d personal information has been or will be misused.

106e (b) If an investigation under Subsection (1)(a) reveals that the misuse of personal information
106f has occurred, or is reasonably likely to occur, the person shall provide notification to each affected
106g Utah resident as soon as possible.

106h (2) A person required to provide notification under Subsection (1) shall provide the
106i notification as soon as possible:
106j (a) considering legitimate investigative needs of law enforcement;
106k (b) after determining the scope of the breach of system security; and
106l (c) after restoring the integrity of the system.

106m (3)(a) A person who maintains computerized data that includes personal information that the
106n person does not own or license shall notify and cooperate with the owner or licensee of the
106o information of any breach of system security immediately following the person's discovery of
106p the breach if misuse of the personal information occurs or is reasonably likely to occur.

106q (b) Cooperation under Subsection (3)(a) includes sharing information relevant to the breach
106r with the owner or licensee of the information.

106s (4)(a) Notwithstanding Subsection (2), a person may delay providing notification under
106t Subsection (1) at the request of a law enforcement agency that determines that ←§

106u **§→ notification may impede a criminal investigation.**
 106v **(b) A person who delays providing notification under Subsection (4)(a) shall provide**
 106w **notification in good faith without unreasonable delay as soon as possible after the law**
 106x **enforcement agency informs the person that notification will no longer impede the criminal**
 106y **investigation.**

107 ~~[(4)] (5) ←§~~ (a) A notification required by this section may be provided:
 108 (i) in writing by first-class mail; or
 109 (ii) electronically, if provided in accordance with the consumer disclosure provisions of
 110 15 U.S.C. Section 7001.

111 (b) Notwithstanding Subsection ~~§→ [(4)] (5) ←§~~ (a), if the cost of providing notification
 111a will exceed
 112 \$150,000, the number of affected persons exceeds 100,000, or the person does not have
 113 sufficient contact information for affected persons, the notice may be provided by:
 114 (i) electronic mail, if the person has an electronic mail address for the affected person;
 115 (ii) conspicuous posting on the person's Internet website; or
 116 (iii) publishing and broadcasting notice in major, statewide media.

117 **§→ [(c) If a person possessing personal information maintains notification procedures**
 118 **substantially similar to those required by this section, that person need not provide the] ←§**

119 ~~§→ [notification required by this section if the notification is nevertheless provided within the time~~
 120 ~~period prescribed in this section:~~

121 ~~—— (d) A person possessing personal information who is required by federal law to~~
 122 ~~maintain procedures for a breach of system security is considered to be in compliance with this~~
 123 ~~chapter if the person notifies state residents of a breach of system security in accordance with~~
 124 ~~the federal procedures.] (c) If a person maintains the person's own notification procedures as~~
 124a ~~part of an information security policy for the treatment of personal information is considered~~
 124b ~~to be in compliance with this chapter's notification requirements if the procedures are~~
 124c ~~otherwise consistent with this chapter's timing requirements and the person notifies each~~
 124d ~~affected Utah resident in accordance with the person's information security policy in the event~~
 124e ~~of a breach.~~

124f (d) A person who is regulated by state or federal law and maintains procedures for a
 124g breach of system security under applicable law established by the primary state or federal
 124h regulator is considered to be in compliance with this part if the person notifies each affected
 124i Utah resident in accordance with the other applicable law in the event of a breach.

125 ~~[(5)] (6) ←§~~ A waiver of this section is contrary to public policy and is void and
 125a unenforceable.

126 Section 5. Section **13-42-301** is enacted to read:

127 **Part 3. Enforcement**

128 **13-42-301. Enforcement.**

129 (1) The attorney general may enforce this chapter's provisions.

130 (2) Nothing in this chapter affects any private right of action under other law, including
 131 contract or tort.

132 (3) (a) A person who violates this chapter's provisions is subject to a civil fine of:

133 (i) no greater than \$2,500 for a violation or series of violations concerning a specific
 134 consumer; and

135 (ii) no greater than \$100,000 in the aggregate for related violations concerning more
 136 than one consumer.

137 (b) A person subject to a civil fine under Subsection (3)(a) is also liable for attorney
 138 fees and costs, including investigatory costs, incurred by the attorney general.

139 (4) In addition to the penalties provided in Subsection (3), the attorney general may
 140 seek injunctive relief to prevent future violations of this chapter in:

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

142 (b) the district court for the district in which resides a consumer who is affected by the

143 violation.

144 Section 6. **Appropriation.**

145 (1) There is appropriated from the General Fund to the attorney general:

146 (a) as an ongoing appropriation, subject to future budget constraints, \$178,800 for

147 fiscal year 2006-07; and

148 (b) \$46,000 for fiscal year 2006-07 only.

149 (2) It is the intent of the Legislature that:

150 (a) the monies appropriated under Subsection (1)(a) be used to fund investigatory
151 activities that may lead to an enforcement action by the attorney general under Section
152 13-42-301; and

153 (b) the monies appropriated under Subsection (1)(b) be used to purchase equipment
154 required for investigatory activities that may lead to an enforcement action by the attorney
155 general under Section 13-42-301.

State Impact

The bill provides a one-time General Fund appropriation of \$46,000 for FY 2007 and an ongoing General Fund appropriation of \$178,800 beginning FY 2007 to the Attorney General to implement provisions of the bill.

	<u>FY 2007</u> <u>Approp.</u>	<u>FY 2008</u> <u>Approp.</u>	<u>FY 2007</u> <u>Revenue</u>	<u>FY 2008</u> <u>Revenue</u>
General Fund	\$224,800	\$178,800	\$0	\$0
TOTAL	\$224,800	\$178,800	\$0	\$0

Individual and Business Impact

Violators of the bill's provisions could face significant financial fines and penalties.
