



2007 SENATE BILL 439

February 1, 2008 – Introduced by Senators WIRCH, BRESKE, ELLIS, HANSEN, A. LASEE, LASSA, LEHMAN, OLSEN, ROESSLER, SCHULTZ and SULLIVAN, cosponsored by Representatives DAVIS, NEWCOMER, ALBERS, BALLWEG, BIES, BOYLE, GRONEMUS, GUNDERSON, HAHN, HILGENBERG, HINTZ, JESKEWITZ, KAUFERT, KERKMAN, F. LASEE, MONTGOMERY, MURSAU, MUSSER, NELSON, NYGREN, A. OTT, PRIDEMORE, SEIDEL, SHERIDAN, SUDER, TAUCHEN, TURNER, VAN AKKEREN, VOS, M. WILLIAMS, ZEPNICK and ZIEGELBAUER. Referred to Committee on Veterans and Military Affairs, Biotechnology and Financial Institutions.

- 1 **AN ACT to create** 100.545 of the statutes; **relating to:** prohibiting the retention
2 of certain information obtained in transactions using account access devices.

Analysis by the Legislative Reference Bureau

This bill prohibits the retention of certain data by a person who accepts payment for goods or services in the form of a card issued by a financial institution, generally, a credit card or debit card. The bill prohibits a person who accepts such payment for a sale from retaining a security code, personal identification number, or certain other data, after the sale is authorized. If a person violates the prohibition, the person must reimburse the financial institution that issued the card for the cost of reasonable action taken to protect personal information pertaining to, or to continue to provide service to, the financial institution's customers. A financial institution that is injured by a violation of the prohibition on data retention may bring an action for damages against the violator.

Under the bill, persons are exempt from the prohibition on data retention if they comply with certain federal privacy and security standards or with certain industry standards for data encryption and security.

For further information see the *state* fiscal estimate, which will be printed as an appendix to this bill.

The people of the state of Wisconsin, represented in senate and assembly, do enact as follows:

SENATE BILL 439**SECTION 1**

1 **SECTION 1.** 100.545 of the statutes is created to read:

2 **100.545 Account access devices; retention of information. (1)**

3 DEFINITIONS. In this section:

4 (a) “Account access device” means a card issued by a financial institution that
5 contains a means for storage of electronic data.

6 (b) “Financial institution” has the meaning given in s. 134.97 (1) (b).

7 (c) “Security code” means digits printed or electronically stored on an account
8 access device that are used to validate information during the authorization process.

9 (d) “Service provider” means a person that stores, processes, or transmits
10 account access device data on behalf of another person.

11 **(2) RETENTION OF CERTAIN INFORMATION PROHIBITED.** No person that accepts an
12 account access device in connection with a sale of goods or services shall retain a
13 security code, a personal identification number, or the full contents of any track of
14 data from a magnetic stripe on the access device obtained from an account access
15 device, or permit the person’s service provider to retain a security code, a personal
16 identification number, or the full contents of any track of data from a magnetic stripe
17 on the access device obtained from an account access device, after the sale is
18 authorized.

19 **(3) LIABILITY.** If a person violates this section and the violation causes the
20 security, confidentiality, or integrity of another person’s personal information to be
21 compromised, the violator shall reimburse the financial institution that issued any
22 account access device affected by the violation for the cost of reasonable action taken
23 by the financial institution to protect personal information pertaining to, or to
24 continue to provide service to, the financial institution’s customers, including the
25 cost of doing any of the following:

SENATE BILL 439

1 (a) Canceling or reissuing an account access device affected by the violation.

2 (b) Closing an account affected by the violation and taking action to stop
3 payments or block transactions involving the account.

4 (c) Opening or reopening an account affected by the violation.

5 (d) Refunding or crediting a customer to cover the cost of an unauthorized
6 transaction relating to the violation.

7 (e) Notifying customers affected by the violation.

8 **(4) EXEMPTION.** This section does not apply to any of the following:

9 (a) A person that is subject to, and in compliance with, the privacy and security
10 requirements of 15 USC 6801 to 6827.

11 (b) A person that encrypts transmission of data pertaining to a holder of an
12 account access device across open and public networks using Wi-Fi Protected Access
13 or Wi-Fi Protected Access 2 security specifications.

14 (c) A person who complies with the Payment Card Industry Data Security
15 Standard.

16 **(5) REMEDIES.** Any financial institution injured by a violation of this section
17 may bring an action against the violator for damages. Notwithstanding s. 814.04 (1),
18 a court shall award reasonable attorney fees to a plaintiff who prevails in an action
19 under this subsection.

20 **(END)**