SENATE BILL NO. 227–SENATOR WIENER

MARCH 13, 2009

Referred to Committee on Judiciary

SUMMARY—Revises certain provisions concerning identity theft. (BDR 52-72)

FISCAL NOTE: Effect on Local Government: No.
Effect on the State: No.

~

EXPLANATION – Matter in ***bolded italics*** is new; matter between brackets [omitted material] is material to be omitted.

AN ACT relating to security of personal information; requiring the compliance with certain standards or the use of encryption by data collectors when transferring personal information; and providing other matters properly relating thereto.

Legislative Counsel's Digest:

Section 1 of this bill requires that a data collector comply with certain standards or use encryption to protect information that is either transmitted electronically or contained on a data storage device that is moved beyond the controls of the data collector. **Section 1** also renders a data collector not liable for a breach of the security of the system data in certain circumstances.

THE PEOPLE OF THE STATE OF NEVADA, REPRESENTED IN SENATE AND ASSEMBLY, DO ENACT AS FOLLOWS:

Section 1. Chapter 603A of NRS is hereby amended by adding thereto a new section to read as follows:

1. If a data collector doing business in this State accepts a payment card in connection with a sale of goods or services, the data collector shall comply with the current version of the Payment Card Industry (PCI) Data Security Standard, as adopted by the PCI Security Standards Council or its successor organization, with respect to those transactions, not later than the date for compliance set forth in the Payment Card Industry (PCI) Data Security Standard or by the PCI Security Standards Council or its successor organization.

2. A data collector doing business in this State to whom subsection 1 does not apply shall not:

(a) Transfer any personal information through an electronic, nonvoice transmission other than a facsimile to a person outside of the secure system of the data collector unless the data collector uses encryption to ensure the security of electronic transmission; or

(b) Move any data storage device containing personal information beyond the logical or physical controls of the data collector or its data storage contractor unless the data collector uses encryption to ensure the security of the information.

3. A data collector shall not be liable for damages for a breach of the security of the system data if:

(a) The data collector is in compliance with this section; and

(b) The breach is not caused by the gross negligence or intentional misconduct of the data collector, its officers, employees or agents.

4. The requirements of this section do not apply to:

(a) A telecommunication provider acting solely in the role of conveying the communications of other persons, regardless of the mode of conveyance used, including, without limitation:

(1) Optical, wire line and wireless facilities;

(2) Analog transmission; and

(3) Digital subscriber line transmission, voice over Internet protocol and other digital transmission technology.

(b) Data transmission over a secure, private communication channel for:

(1) Approval or processing of negotiable instruments, electronic fund transfers or similar payment methods; or

(2) Issuance of reports regarding account closures due to fraud, substantial overdrafts, abuse of automatic teller machines or related information regarding a customer.

5. As used in this section:

(a) "Data storage device" means any device that stores information or data from any electronic or optical medium, including, but not limited to, computers, cellular telephones, magnetic tape, electronic computer drives and optical computer drives, and the medium itself.

(b) "Encryption" means the protection of data in electronic or optical form, in storage or in transit, using:

(1) An encryption technology that has been adopted by an established standards setting body, including, but not limited to, the Federal Information Processing Standards issued by the National Institute of Standards and Technology, which renders such data indecipherable in the absence of associated

cryptographic keys necessary to enable decryption of such data; and

(2) Appropriate management and safeguards of cryptographic keys to protect the integrity of the encryption using guidelines promulgated by an established standards setting body, including, but not limited to, the National Institute of Standards and Technology.

(c) "Facsimile" means an electronic transmission between two dedicated fax machines using Group 3 or Group 4 digital formats that conform to the International Telecommunications Union T.4 or T.38 standards or computer modems that conform to the International Telecommunications Union T.31 or T.32 standards. The term does not include onward transmission to a third device after protocol conversion, including, but not limited to, any data storage device.

(d) "Payment card" has the meaning ascribed to it in NRS 205.602.

(e) "Telecommunication provider" has the meaning ascribed to it in NRS 704.027.

Sec. 2. NRS 597.970 is hereby repealed.

Sec. 3. This act becomes effective on January 1, 2010.

TEXT OF REPEALED SECTION

597.970 Restrictions on transfer of personal information through electronic transmission.

1. A business in this State shall not transfer any personal information of a customer through an electronic transmission other than a facsimile to a person outside of the secure system of the business unless the business uses encryption to ensure the security of electronic transmission.

2. As used in this section:

(a) "Encryption" has the meaning ascribed to it in NRS 205.4742.

(b) "Personal information" has the meaning ascribed to it in NRS 603A.040.