SENATE BILL NO. 267–SENATOR WIENER

MARCH 18, 2011

Referred to Committee on Commerce, Labor and Energy

SUMMARY—Revises provisions governing personal information. (BDR 52-110)

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 personal information; requiring a business entity or data collector to encrypt or destroy personal information that is stored on a copier, facsimile machine or multifunction device under certain circumstances; requiring an owner or lessor of certain copiers, facsimile machines or multifunction devices to destroy any personal information that is stored on the copier, facsimile machine or multifunction device under certain circumstances; and providing other matters properly relating thereto.

Legislative Counsel's Digest:

Section 4 of this bill requires a business entity or a data collector to ensure that any personal information which is stored on the data storage device of a copier, facsimile machine or multifunction device in the possession of the business entity or data collector is securely encrypted or destroyed by certain approved methods before the business entity or data collector relinquishes ownership, physical control or custody of the copier, facsimile machine or multifunction device to another person. **Section 4** also requires the owner or lessor of a copier, facsimile machine or multifunction device that is leased or rented to a business entity or data collector to ensure that any personal information which is stored on the copier, facsimile machine or multifunction device is destroyed by certain approved methods as soon as practicable after the termination or cancellation of the lease agreement or rental contract, or upon assuming physical custody or control of the copier, facsimile machine or multifunction device.

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 the provisions set forth as sections 2, 3 and 4 of this act.

Sec. 2. ***"Data storage device" means any device that stores information or data from any electronic or optical medium, including, without limitation, a computer, cellular telephone, magnetic tape, electronic computer drive and optical computer drive, and the medium itself.***

Sec. 3. ***"Encryption" means the protection of data in electronic or optical form, in storage or in transit, using:***

1. An encryption technology which has been adopted by an established standards setting body, including, without limitation, the Federal Information Processing Standards issued by the National Institute of Standards and Technology, or its successor organization, and 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, without limitation, the National Institute of Standards and Technology or its successor organization.

Sec. 4. ***1. Except as otherwise provided in subsections 2 and 3, a business entity or data collector that owns or possesses a copier, facsimile machine or multifunction device which uses a data storage device to store, reproduce, transmit or receive data or images that may contain personal information shall, before the business entity or data collector relinquishes ownership, physical custody or control of the copier, facsimile machine or multifunction device to another person, ensure that any personal information which is stored on the data storage device of the copier, facsimile machine or multifunction device is:***

(a) Secured through the use of encryption; or

(b) Destroyed through the use of a physical or technological method that has been adopted by an established standards setting body, including, without limitation, a method prescribed by the most recent version of the Federal Information Processing Standards issued by the National Institute of Standards and Technology or its successor organization.

2. Except as otherwise provided in subsection 3, if a business entity or data collector uses or possesses a copier, facsimile machine or multifunction device which uses a data storage device

to store, reproduce, transmit or receive data or images that may contain personal information pursuant to a lease agreement or rental contract, the owner or lessor of the copier, facsimile machine or multifunction device shall, as soon as practicable after the termination or cancellation of the lease agreement or rental contract, or upon assuming physical custody or control of the copier, facsimile machine or multifunction device, ensure that any personal information which is stored on the data storage device of the copier, facsimile machine or multifunctional device is destroyed through the use of a physical or technological method that has been adopted by an established standards setting body, including, without limitation, a method prescribed by the most recent version of the Federal Information Processing Standards issued by the National Institute of Standards and Technology or its successor organization.

3. The provisions of subsections 1 and 2 do not apply to a copier, facsimile machine or multifunction device which is used or configured in such a way as to prevent the storage of data or images that may contain personal information.

4. As used in this section, "multifunction device" means a machine that incorporates the functionality of multiple devices, which may include, without limitation, a printer, copier, scanner, facsimile machine or electronic mail terminal, to provide for the centralized management, distribution or production of documents.

Sec. 5. NRS 603A.010 is hereby amended to read as follows:

603A.010 As used in this chapter, unless the context otherwise requires, the words and terms defined in NRS 603A.020, 603A.030 and 603A.040 ***and sections 2 and 3 of this act*** have the meanings ascribed to them in those sections.

Sec. 6. NRS 603A.215 is hereby amended to read as follows:

603A.215 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)]~~ ***(b)*** "Payment card" has the meaning ascribed to it in NRS 205.602.

~~[(e)]~~ ***(c)*** "Telecommunication provider" has the meaning ascribed to it in NRS 704.027.

㉚