Senate Bill No. 267–Senator Wiener

CHAPTER.....

AN ACT relating to personal information; authorizing the Office of Information Security of the Department of Information Technology to adopt certain regulations relating to encryption; revising provisions governing the protection of personal information collected by a data collector; and providing other matters properly relating thereto.

Legislative Counsel's Digest:

Existing law prohibits a data collector from moving any data storage device containing personal information beyond the control of the data collector or its data storage contractor unless the data collector uses encryption to ensure the security of the information. (NRS 603A.215) **Section 5.5** of this bill authorizes the Office of Information Security of the Department of Information Technology, upon receipt of a well-founded petition, to adopt regulations which identify alternative methods or technologies which may be used by a data collector to encrypt certain data. **Section 6** of this bill additionally prohibits a data collector from moving a data storage device which is used by or is a component of a multifunctional device beyond the control of the data collector, its data storage contractor or a person who assumes the obligation of the data collector to protect personal information unless the data collector uses encryption to ensure the security of the information.

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

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

Sections 1-5. (Deleted by amendment.)

Sec. 5.5. Chapter 603A of NRS is hereby amended by adding thereto a new section to read as follows:

Upon receipt of a well-founded petition, the Office of Information Security of the Department of Information Technology may, pursuant to chapter 233B of NRS, adopt regulations which identify alternative methods or technologies which may be used to encrypt data pursuant to NRS 603A.215.

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 ***or, if the data storage device is used by or is a component of a multifunctional device, a person who assumes the obligation of the data collector to protect personal information,*** 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 ~~[.]~~ ***; and***

(3) Any other technology or method identified by the Office of Information Security of the Department of Information Technology in regulations adopted pursuant to section 5.5 of this act.

(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) ***"Multifunctional device" means a machine that incorporates the functionality of 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.***

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

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