SENATE BILL NO. 239–SENATOR SEEVERS GANSERT

MARCH 15, 2021

Referred to Committee on Commerce and Labor

SUMMARY—Revises provisions relating to cybersecurity. (BDR 52-63)

FISCAL NOTE: Effect on Local Government: May have Fiscal Impact.
Effect on the State: Yes.

~

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

AN ACT relating to cybersecurity; providing immunity from liability for damages arising from the commission of certain unfair trade practices under certain circumstances to certain owners of the rights to a proprietary program or the data stored in a computer who have adopted certain security controls or standards; providing additional circumstances under which certain data collectors are immune from liability for damages for a breach of the security of the system data; expanding the circumstances that constitute a breach of the security of the system data; requiring a data collector to provide notice to certain persons whose personal information has been or is reasonably believed to have been subject to unauthorized access; and providing other matters properly relating thereto.

Legislative Counsel's Digest:

Existing law makes it an unfair trade practice for a person to commit certain acts related to obtaining unauthorized possession of or access to a proprietary program or data stored in a computer. (NRS 603.040) **Section 1** of this bill provides that an owner of a program or data against whom such an unfair trade practice has been committed is not liable to a third person for damages arising from the commission of the unfair trade practice if the owner is in compliance with certain specified controls or standards with respect to the security of the owner's information assets. **Section 1** defines the term "information asset" to mean any computer, program, cloud service, data resource or infrastructure used to communicate, process, store or retrieve data.

Existing law requires a data collector to: (1) comply with certain standards related to transactions involving payment cards; or (2) if the data collector does not

engage in such transactions, comply with certain requirements concerning the use of encryption to ensure the security of personal information. A data collector that is in compliance with such requirements is not liable for damages for a breach of the security of the system data so long as the breach was not caused by the gross negligence or intentional misconduct of the data collector. (NRS 603A.215) **Section 4** of this bill provides additional circumstances in which certain data collectors will be shielded from liability for damages for a breach. Under **section 4**, a data collector that maintains records which contain personal information of a resident of this State is also shielded from liability for damages for a breach if the data collector is in compliance with certain controls or standards with respect to the collection, dissemination and maintenance of those records and the breach was not caused by the gross negligence or intentional misconduct of the data collector. **Section 8** of this bill revises the provisions of existing law that shield a data collector from liability for damages for a breach under certain circumstances to account for the addition of the additional circumstances in which a data collector is shielded from such liability set forth in **section 4**.

Existing law requires a data collector to, following a breach of the security of the system data, provide notice to certain persons whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person. (NRS 603A.220) Existing law provides that the acquisition of computerized data that compromises the security, confidentiality or integrity of personal information maintained by the data collector constitutes a breach of the security of the system data, and **section 6** of this bill includes unauthorized access of such data as a breach. (NRS 603A.020) **Section 9** of this bill requires a data collector to, following a breach of the security of the system data, provide notice to certain persons whose personal information was, or is reasonably believed to have been, subject to unauthorized access.

Existing law authorizes a data collector to commence a civil action against a person who has unlawfully obtained or benefited from personal information obtained from records maintained by the data collector. (NRS 603A.270) Existing law also authorizes a court to order a person convicted of unlawfully obtaining or benefiting from such information to pay restitution to the data collector. (NRS 603A.280) **Sections 10 and 11** of this bill revise these provisions to allow for such actions to be taken against a person who caused personal information in records maintained by the data collector to be subject to unauthorized access.

Sections 2, 3, 5, 7 and 12 of this bill make conforming changes to indicate the proper placement of **sections 1 and 4** in the Nevada Revised Statutes.

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

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

1. An owner of the rights to a proprietary program or the data stored in a computer against whom an unfair trade practice has been committed pursuant to subsection 1 of NRS 603.040 shall not be liable to a third person for any damages arising from the commission of the unfair trade practice if the owner is, with respect to the security of the owner's information assets, in compliance with:

(a) The current version of the CIS Controls, as published by the Center for Internet Security, Inc. or its successor organization;

(b) Standards that are equivalent to the controls described in paragraph (a) adopted by the National Institute of Standards and Technology of the United States Department of Commerce; or

(c) Controls and standards that provide greater protection to the information assets than the controls and standards described in paragraphs (a) and (b).

2. As used in this section, "information asset" means any computer, program, cloud service, data resource or infrastructure used to communicate, process, store or retrieve data.

Sec. 2. NRS 603.010 is hereby amended to read as follows:

603.010 As used in NRS 603.010 to 603.090, inclusive, ***and section 1 of this act,*** unless the context otherwise requires, the words and terms defined in NRS 603.020 and 603.030 have the meanings ascribed to them in those sections.

Sec. 3. NRS 603.090 is hereby amended to read as follows:

603.090 The civil remedies provided in NRS 603.010 to 603.090, inclusive ~~[.]~~ ***, and section 1 of this act:***

1. Do not preclude the prosecution of a defendant under the penal laws of this State.

2. Are in addition to any rights or remedies to which the owner of a proprietary program or data stored in a computer is entitled under the common law.

Sec. 4. Chapter 603A of NRS is hereby amended by adding thereto a new section to read as follows:

In addition to the circumstances in which a data collector is not liable for damages for a breach of the security of the system data pursuant to NRS 603A.215, a data collector that maintains records which contain personal information of a resident of this State shall not be liable for damages for a breach of the security of the system data if:

1. The data collector is, with respect to the collection, dissemination and maintenance of those records, in compliance with:

(a) The current version of the CIS Controls, as published by the Center for Internet Security, Inc., or its successor organization;

(b) Standards that are equivalent to the controls described in paragraph (a) adopted by the National Institute of Standards and Technology of the United States Department of Commerce; or

(c) Controls and standards that provide greater protection to records that contain personal information of a resident of this State than the controls and standards described in paragraphs (a) and (b); and

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

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

603A.010 As used in NRS 603A.010 to 603A.290, inclusive, ***and section 4 of this act,*** unless the context otherwise requires, the words and terms defined in NRS 603A.020, 603A.030 and 603A.040 have the meanings ascribed to them in those sections.

Sec. 6. NRS 603A.020 is hereby amended to read as follows:

603A.020 "Breach of the security of the system data" means unauthorized ***access or*** acquisition of computerized data that materially compromises the security, confidentiality or integrity of personal information maintained by the data collector. The term does not include the good faith acquisition of personal information by an employee or agent of the data collector for a legitimate purpose of the data collector, so long as the personal information is not used for a purpose unrelated to the data collector or subject to further unauthorized disclosure.

Sec. 7. NRS 603A.100 is hereby amended to read as follows:

603A.100 1. The provisions of NRS 603A.010 to 603A.290, inclusive, ***and section 4 of this act*** do not apply to the maintenance or transmittal of information in accordance with NRS 439.581 to 439.595, inclusive, and the regulations adopted pursuant thereto.

2. A data collector who is also an operator, as defined in NRS 603A.330, shall comply with the provisions of NRS 603A.300 to 603A.360, inclusive.

3. Any waiver of the provisions of NRS 603A.010 to 603A.290, inclusive, ***and section 4 of this act*** is contrary to public policy, void and unenforceable.

Sec. 8. 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, 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~~]~~ ***In addition to the circumstances in which a data collector is not liable for damages for a breach of the security of the system data pursuant to section 4 of this act, 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;

(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 Division of Enterprise Information Technology Services of the Department of Administration in regulations adopted pursuant to NRS 603A.217.

(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.

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

Sec. 9. NRS 603A.220 is hereby amended to read as follows:

603A.220 1. Any data collector that owns or licenses computerized data which includes personal information shall disclose any breach of the security of the system data following discovery or notification of the breach to any resident of this State whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person ~~[.]~~ ***or subject to unauthorized access.*** The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection 3, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system data.

2. Any data collector that maintains computerized data which includes personal information that the data collector does not own shall notify the owner or licensee of the information of any breach of the security of the system data immediately following discovery if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person ~~[.]~~ ***or subject to unauthorized access.***

3. The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section must be made after the law enforcement agency determines that the notification will not compromise the investigation.

4. For purposes of this section, except as otherwise provided in subsection 5, the notification required by this section may be provided by one of the following methods:

(a) Written notification.

(b) Electronic notification, if the notification provided is consistent with the provisions of the Electronic Signatures in Global and National Commerce Act, 15 U.S.C. §§ 7001 et seq.

(c) Substitute notification, if the data collector demonstrates that the cost of providing notification would exceed $250,000, the affected class of subject persons to be notified exceeds 500,000 or the data collector does not have sufficient contact information. Substitute notification must consist of all the following:

(1) Notification by electronic mail when the data collector has electronic mail addresses for the subject persons.

(2) Conspicuous posting of the notification on the Internet website of the data collector, if the data collector maintains an Internet website.

(3) Notification to major statewide media.

5. A data collector which:

(a) Maintains its own notification policies and procedures as part of an information security policy for the treatment of personal information that is otherwise consistent with the timing requirements of this section shall be deemed to be in compliance with the notification requirements of this section if the data collector notifies subject persons in accordance with its policies and procedures in the event of a breach of the security of the system data.

(b) Is subject to and complies with the privacy and security provisions of the Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801 et seq., shall be deemed to be in compliance with the notification requirements of this section.

6. If a data collector determines that notification is required to be given pursuant to the provisions of this section to more than 1,000 persons at any one time, the data collector shall also notify, without unreasonable delay, any consumer reporting agency that compiles and maintains files on consumers on a nationwide basis, as that term is defined in 15 U.S.C. § 1681a(p), of the time the notification is distributed and the content of the notification.

Sec. 10. NRS 603A.270 is hereby amended to read as follows:

603A.270 A data collector that provides the notification required pursuant to NRS 603A.220 may commence an action for damages against a person that unlawfully obtained or benefited from personal information obtained from records maintained by the data collector ~~[.]~~ ***or caused such information to be subject to unauthorized access.*** A data collector that prevails in such an action may be awarded damages which may include, without limitation, the reasonable costs of notification, reasonable attorney's fees and costs and punitive damages when appropriate. The costs of notification include, without limitation, labor, materials, postage and any other costs reasonably related to providing the notification.

Sec. 11. NRS 603A.280 is hereby amended to read as follows:

603A.280 In addition to any other penalty provided by law for the breach of the security of the system data maintained by a data collector, the court may order a person who is convicted of unlawfully ~~[obtaining]~~ ***:***

1. Obtaining or benefiting from personal information obtained as a result of such breach ***; or***

2. Causing personal information to be subject to unauthorized access as a result of such breach,

➥ to pay restitution to the data collector for the reasonable costs incurred by the data collector in providing the notification required pursuant to NRS 603A.220, including, without limitation, labor, materials, postage and any other costs reasonably related to providing such notification.

Sec. 12. NRS 603A.290 is hereby amended to read as follows:

603A.290 If the Attorney General or a district attorney of any county has reason to believe that any person is violating, proposes to violate or has violated the provisions of NRS 603A.010 to 603A.290, inclusive, ***and section 4 of this act,*** the Attorney General or district attorney may bring an action against that person to obtain a temporary or permanent injunction against the violation.