SENATE BILL NO. 291–SENATORS DOÑATE, FLORES AND TAYLOR

MARCH 6, 2025

Referred to Committee on Commerce and Labor

SUMMARY—Revises provisions relating to personal information. (BDR 52-39)

FISCAL NOTE: Effect on Local Government: Increases or Newly Provides for Term of Imprisonment in County or City Jail or Detention Facility.
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 personal information; requiring certain employers to implement and maintain reasonable security measures to protect the personal information of certain former residents of this State; revising requirements for the provision of certain notifications in the event of a breach of the security of the system data; prohibiting certain persons from collecting social security numbers under certain circumstances; prohibiting an employer from retaliating against an employee for certain actions relating to the security of personal information; requiring the Department of Motor Vehicles to establish procedures by which a victim of identity theft may obtain a new driver's license number; providing penalties; and providing other matters properly relating thereto.

Legislative Counsel's Digest:

Existing law imposes certain requirements upon data collectors with respect to the security of personal information collected and maintained by the data collector. (NRS 603A.010-603A.290) Existing law requires a data collector that maintains records which contain personal information of a resident of this State to implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification or disclosure. (NRS 603A.210) **Section 8** of this bill additionally requires a data collector to implement and maintain such security measures to protect records containing personal information of a person who was a resident of this State at the time at which the personal information was obtained by the data collector. **Section 16** of this bill prohibits an employer from retaliating against an employee because the employee

has filed a formal complaint alleging that the employer has failed to comply with such requirements.

Existing law requires a data collector that owns, licenses or maintains computerized data which includes personal information, after discovery or notification of a breach of the security of the system data in which personal information maintained by the data collector was, or is reasonably believed to have been, acquired by an unauthorized person, to notify each affected resident of this State and certain other persons. (NRS 603A.220) **Section 9** of this bill requires a data collector to provide such a notification to a former resident of this State who was a resident of this State at the time at which the personal information was obtained by the data collector. **Section 9** provides that if the breach involves the personal information of a current employee or former employee of the data collector, the notification must be provided within 30 days after discovery or notification of the breach. **Section 9** deems a data collector to have complied with the requirement for notification with respect to a former employee if the data collector made a reasonable effort to provide the notification to the employee. **Section 4** of this bill requires a data collector who provides such a notification to a current employee or former employee to provide to the employee monitoring services and services to protect against identity theft at no cost for not less than 1 year after the date on which the notification was provided. **Section 2** of this bill defines "current employee" to mean a person who is currently employed by a data collector. **Section 3** of this bill defines "former employee" to mean a person who is not a current employee and who has been employed by a data collector in the immediately preceding 2 years.

Existing law makes a violation of the provisions governing the security of personal information maintained by data collectors a deceptive trade practice, thereby subjecting a data collector who violates those provisions to certain civil and criminal penalties. (NRS 598.0999, 603A.290) **Section 10** of this bill also makes a violation of the provisions of **sections 2-4** of this bill a deceptive trade practice.

Existing law provides for the issuance of drivers' licenses by the Department of Motor Vehicles. (Chapter 483 of NRS) **Section 12** of this bill requires the Department to establish procedures by which a licensee who is a victim of identity theft may request that the number of his or her driver's license be changed to a new unique number. **Section 14** of this bill prohibits the Department from charging a fee for making such a change. **Section 13** of this bill makes a conforming change so that the definitions applicable to the provisions of existing law governing drivers' licenses apply to **section 12**.

Section 7 of this bill prohibits, with certain exceptions, a business operating in this State that maintains records which contain personal information from requesting, collecting or maintaining the full social security number of a customer.

Section 17 of this bill prohibits, with certain exceptions, an employer from collecting the social security number of a prospective employee or requesting or requiring that a prospective employee disclose his or her social security number before the employer has made a formal offer of employment and the prospective employee has accepted the offer.

Section 5 of this bill applies the definitions in existing law governing the security of personal information maintained by data collectors to **sections 2-4**. **Section 6** of this bill provides that any waiver of the provisions of **sections 2-4** is contrary to public policy, void and unenforceable. **Section 11** of this bill authorizes the Attorney General or a district attorney to bring an action to obtain an injunction against a violation of **sections 2-4**.

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. ***"Current employee" means a person who is currently employed by a data collector.***

Sec. 3. ***"Former employee" means a person who is not a current employee and who has been employed by a data collector during the immediately preceding 2 years.***

Sec. 4. ***A data collector who, pursuant to NRS 603A.220, provides notification of a breach of the security of the system data to a current employee of the data collector or, if the data collector is able to provide the notification after making a reasonable effort, a former employee of the data collector shall provide to the employee, at no cost to the employee, services to monitor his or her credit and to protect against identity theft for not less than 1 year after the date on which the notification was provided.***

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 sections 2, 3 and 4 of this act,*** 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.100 is hereby amended to read as follows:

603A.100 1. The provisions of NRS 603A.010 to 603A.290, inclusive, ***and sections 2, 3 and 4 of this act*** do not apply to the maintenance or transmittal of information in accordance with NRS 439.581 to 439.597, 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 sections 2, 3 and 4 of this act*** is contrary to public policy, void and unenforceable.

Sec. 7. NRS 603A.200 is hereby amended to read as follows:

603A.200 1. A business that maintains records which contain personal information concerning the customers of the business shall take reasonable measures to ensure the destruction of those records when the business decides that it will no longer maintain the records.

2. ***Except as otherwise provided in subsection 3, a business shall not request, collect or maintain the full social security***

number of a customer of the business. Nothing in the provisions of this subsection prohibits a business from requesting, collecting or maintaining the driver's license number of a customer or any other number issued to a person by a governmental entity.

3. The provisions of subsection 2 do not apply to:

(a) A banking or financial institution, as defined in NRS 106.295.

(b) Any person who holds a nonrestricted license, as defined in NRS 463.0177, or an affiliate, as defined in NRS 463.0133, of such a person.

(c) The requesting, collection or maintenance of the full social security number of a customer:

(1) For the purpose of billing or another reasonable business purpose; or

(2) To comply with any provision of state or federal law, including, without limitation, to report any information required to be reported to the Internal Revenue Service.

4. As used in this section:

(a) "Business" means a proprietorship, corporation, partnership, association, trust, unincorporated organization or other enterprise doing business in this State.

(b) "Reasonable measures to ensure the destruction" means any method that modifies the records containing the personal information in such a way as to render the personal information contained in the records unreadable or undecipherable, including, without limitation:

(1) Shredding of the record containing the personal information; or

(2) Erasing of the personal information from the records.

Sec. 8. NRS 603A.210 is hereby amended to read as follows:

603A.210 1. A data collector that maintains records which contain personal information of a resident of this State ***or personal information of a person who was a resident of this State at the time at which the personal information was obtained by the data collector*** shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification or disclosure.

2. If a data collector is a governmental agency and maintains records which contain personal information of a resident of this State, the data collector shall, to the extent practicable, with respect to the collection, dissemination and maintenance of those records, comply with the current version of the CIS Controls as published by the Center for Internet Security, Inc. or its successor organization, or corresponding standards adopted by the National Institute of

Standards and Technology of the United States Department of Commerce.

3. A contract for the disclosure of the personal information of a resident of this State which is maintained by a data collector must include a provision requiring the person to whom the information is disclosed to implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification or disclosure.

4. If a state or federal law requires a data collector to provide greater protection to records that contain personal information of a resident ***or former resident*** of this State which are maintained by the data collector and the data collector is in compliance with the provisions of that state or federal law, the data collector shall be deemed to be in compliance with the provisions of this section.

5. The Office of Information Security of the Office of the Chief Information Officer within the Office of the Governor shall create, maintain and make available to the public a list of controls and standards with which the State is required to comply pursuant to any federal law, regulation or framework that also satisfy the controls and standards set forth in subsection 2.

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

603A.220 1. Except as otherwise provided in subsection ~~[7,]~~ ***8,*** a data collector that owns or licenses computerized data which includes personal information ***of a resident of this State or personal information of a person who was a resident of this State at the time at which the personal information was obtained by the data collector*** shall disclose any breach of the security of the system data following discovery or notification of the breach to any resident of this State ***or former resident of this State, if applicable,*** whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. 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. ***Except as otherwise provided in subsections 3 and 7, if the breach involves personal information of a current employee or former employee of the data collector, the data collector shall provide the disclosure required by this subsection to each affected current employee or former employee not less than 30 days after discovery or notification of the breach.***

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.

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 ~~[.]~~ ***with respect to customers of the data collector.***

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.

7. ***A data collector who makes a reasonable effort to provide the disclosure required by this section to a former employee shall be deemed to be in compliance with the notification requirements of this section with respect to the former employee.***

8. The provisions of this section do not apply to a person licensed pursuant to chapter 675 of NRS.

Sec. 10. NRS 603A.260 is hereby amended to read as follows:

603A.260 A violation of the provisions of NRS 603A.010 to 603A.290, inclusive, ***and sections 2, 3 and 4 of this act*** constitutes a deceptive trade practice for the purposes of NRS 598.0903 to 598.0999, inclusive.

Sec. 11. 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 sections 2, 3 and 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.

Sec. 12. Chapter 483 of NRS is hereby amended by adding thereto a new section to read as follows:

1. The Department shall establish procedures by which a licensee who is a victim of identity theft may request that the number of his or her driver's license be changed to a new unique number.

2. As used in this section, "identity theft" means a violation of the provisions of NRS 205.463, 205.464 or 205.465.

Sec. 13. NRS 483.020 is hereby amended to read as follows:

483.020 As used in NRS 483.010 to 483.630, inclusive, ***and section 12 of this act,*** unless the context otherwise requires, the words and terms defined in NRS 483.030 to 483.190, inclusive, have the meanings ascribed to them in those sections.

Sec. 14. NRS 483.410 is hereby amended to read as follows:

483.410 1. Except as otherwise provided in subsection 6 and NRS 483.330 and 483.417, for every driver's license, including a motorcycle driver's license, issued and service performed, the following fees must be charged:

An original or renewal license issued to a person 65 years of age or older	$13.50

An original or renewal license issued to any person less than 65 years of age which expires on the eighth anniversary of the licensee's birthday $37.00

An original or renewal license issued to any person less than 65 years of age which expires on or before the fourth anniversary of the licensee's birthday 18.50

Administration of the examination required by NRS 483.330 for a noncommercial driver's license 25.00

Each readministration to the same person of the examination required by NRS 483.330 for a noncommercial driver's license 10.00

Reinstatement of a license after suspension, revocation or cancellation, except a revocation for a violation of NRS 484C.110, 484C.120, 484C.130 or 484C.430, or pursuant to NRS 484C.210 and 484C.220 ..... 75.00

Reinstatement of a license after revocation for a violation of NRS 484C.110, 484C.120, 484C.130 or 484C.430, or pursuant to NRS 484C.210 and 484C.220 ..... 120.00

A new photograph, change of name, change of other information, except address, or any combination 5.00

A duplicate license 14.00

2. For every motorcycle endorsement to a driver's license, a fee of $5 must be charged.

3. If no other change is requested or required, the Department shall not charge a fee to ***change the number of a driver's license at the request of a licensee who is a victim of identity theft pursuant to section 12 of this act or to*** convert the number of a license from the licensee's social security number, or a number that was formulated by using the licensee's social security number as a basis for the number, to a unique number that is not based on the licensee's social security number.

4. Except as otherwise provided in NRS 483.417, the increase in fees authorized by NRS 483.347 and the fees charged pursuant to NRS 483.415 must be paid in addition to the fees charged pursuant to subsections 1 and 2.

5. A penalty of $10 must be paid by each person renewing a license after it has expired for a period of 30 days or more as

provided in NRS 483.386 unless the person is exempt pursuant to that section.

6. The Department may not charge a fee for the reinstatement of a driver's license that has been:

(a) Voluntarily surrendered for medical reasons; or

(b) Cancelled pursuant to NRS 483.310.

7. All fees and penalties are payable to the Administrator at the time a license or a renewal license is issued.

8. Except as otherwise provided in NRS 483.340, subsection 3 of NRS 483.3485, NRS 483.415 and 483.840, and subsection 3 of NRS 483.863, all money collected by the Department pursuant to this chapter must be deposited in the State Treasury for credit to the Motor Vehicle Fund.

Sec. 15. Chapter 613 of NRS is hereby amended by adding thereto the provisions set forth as sections 16 and 17 of this act.

Sec. 16. ***An employer shall not retaliate against an employee because the employee has filed a formal complaint alleging that the employer has not complied with the requirements of subsection 1 of NRS 603A.210.***

Sec. 17. ***1. Except as otherwise provided in subsection 2, an employer shall not collect the social security number of a prospective employee or request or require that a prospective employee disclose his or her social security number before the employer has made a formal offer of employment to the prospective employee and the prospective employee has accepted the offer.***

2. An employer may collect, request or require the disclosure of the social security number of a prospective employee before the period specified in subsection 1:

(a) To perform a background check on the prospective employee;

(b) If the position of employment requires a security clearance;

(c) To perform any form of preemployment screening that is authorized by law and which the employer deems necessary; or

(d) If necessary to comply with state or federal law.

Sec. 18. This act becomes effective on January 1, 2027.

㉚