CHAPTER 603A - SECURITY OF PERSONAL INFORMATION

GENERAL PROVISIONS

NRS 603A.010 Definitions.
NRS 603A.020 "Breach of the security of the system data" defined.
NRS 603A.030 "Data collector" defined.
NRS 603A.040 "Personal information" defined.

APPLICABILITY

NRS 603A.100 Applicability; waiver of provisions of chapter prohibited.

REGULATION OF BUSINESS PRACTICES

NRS 603A.200 Destruction of certain records.
NRS 603A.210 Security measures.
NRS 603A.215 Security measures for data collector that accepts payment card; use of encryption; liability for damages; applicability.
NRS 603A.217 Alternative methods of and technologies for encryption: Adoption of regulations.
NRS 603A.220 Disclosure of breach of security of system data; methods of disclosure.

REMEDIES AND PENALTIES

NRS 603A.900 Civil action.
NRS 603A.910 Restitution.
NRS 603A.920 Injunction.

GENERAL PROVISIONS

NRS 603A.010 Definitions. As used in this chapter, 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.
(Added to NRS by 2005, 2503)

NRS 603A.020 "Breach of the security of the system data" defined. "Breach of the security of the system data" means unauthorized 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.
(Added to NRS by 2005, 2503)

NRS 603A.030 "Data collector" defined. "Data collector" means any governmental agency, institution of higher education, corporation, financial institution or retail operator or any other type of business entity or association that, for any purpose, whether by automated collection or otherwise, handles, collects, disseminates or otherwise deals with nonpublic personal information.
(Added to NRS by 2005, 2504)

NRS 603A.040 "Personal information" defined.
1. "Personal information" means a natural person's first name or first initial and last name in combination with any one or more of the following data elements, when the name and data elements are not encrypted:
(a) Social security number.
(b) Driver's license number, driver authorization card number or identification card number.
(c) Account number, credit card number or debit card number, in combination with any required security code, access code or password that would permit access to the person's financial account.
(d) A medical identification number or a health insurance identification number.
(e) A user name, unique identifier or electronic mail address in combination with a password, access code or security question and answer that would permit access to an online account.
2. The term does not include the last four digits of a social security number, the last four digits of a driver's license number, the last four digits of a driver authorization card number or the last four digits of an identification card number or publicly available information that is lawfully made available to the general public from federal, state or local governmental records.
(Added to NRS by 2005, 2504; A 2005, 22nd Special Session, 109; 2007, 1314; 2011, 2411; 2015, 241)

APPLICABILITY

NRS 603A.100 Applicability; waiver of provisions of chapter prohibited.

1. The provisions of this chapter 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. Any waiver of the provisions of this chapter is contrary to public policy, void and unenforceable.

(Added to NRS by 2005, 2506; A 2011, 1762)

REGULATION OF BUSINESS PRACTICES

NRS 603A.200 Destruction of certain records.

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. 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.

(Added to NRS by 2005, 2504)

NRS 603A.210 Security measures.

1. A data collector that maintains records which contain personal information of a resident of this State shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification or disclosure.

2. 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.

3. If a state or federal law requires a data collector to provide greater protection to records that contain personal information of a 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.

(Added to NRS by 2005, 2504)

NRS 603A.215 Security measures for data collector that accepts payment card; use of encryption; liability for damages; applicability.

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 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.

(Added to NRS by 2009, 1603; A 2011, 2002)

NRS 603A.217 Alternative methods of and technologies for encryption: Adoption of regulations. Upon receipt of a well-founded petition, the Office of Information Security of the Division of Enterprise Information Technology Services of the Department of Administration 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.

(Added to NRS by 2011, 2002)

NRS 603A.220 Disclosure of breach of security of system data; methods of disclosure.

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. 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.

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, as that term is defined in 15 U.S.C. § 1681a(p), that compiles and maintains files on consumers on a nationwide basis, of the time the notification is distributed and the content of the notification.

(Added to NRS by 2005, 2504)

REMEDIES AND PENALTIES

NRS 603A.900 Civil action. 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. 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.

(Added to NRS by 2005, 2506)

NRS 603A.910 Restitution. 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 or benefiting from personal information obtained 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.

(Added to NRS by 2005, 2506)

NRS 603A.920 Injunction. 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 this chapter, the Attorney General or district attorney may bring an action against that person to obtain a temporary or permanent injunction against the violation.

(Added to NRS by 2005, 2506)