Senate Bill No. 347–Senators Wiener, Titus, Raggio and Townsend

Joint Sponsor: Assemblyman Anderson

CHAPTER.....

AN ACT relating to personal identifying information; prohibiting the establishment or possession of a financial forgery laboratory; enhancing the penalties for crimes involving personal identifying information that are committed against older persons and vulnerable persons; requiring the issuer of a credit card to provide a notice including certain information concerning its policies regarding identity theft and the rights of cardholders when issuing a credit card to a cardholder; requiring data collectors to provide notification concerning any breach of security involving system data; making various other changes concerning personal identifying information; providing penalties; and providing other matters properly relating thereto.

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

Section 1. Chapter 205 of NRS is hereby amended by adding thereto the provisions set forth as sections 2 to 6, inclusive, of this act.

Sec. 2. ***"Artificial person" means any corporation, limited-liability company, limited-liability partnership, limited partnership, limited-liability limited partnership, business trust or municipal corporation or any comparable entity which is created and existing under the laws of this State, any other state, territory or foreign government, or the Government of the United States and which is doing business in this State.***

Sec. 3. ***"Older person" means a person who is 60 years of age or older.***

Sec. 4. ***"Vulnerable person" means a person who:***

1. Suffers from a condition of physical or mental incapacitation because of a developmental disability, organic brain damage or mental illness; or

2. Has one or more physical or mental limitations that restrict the ability of the person to perform the normal activities of daily living.

Sec. 5. ***In any case in which a person is convicted of violating any provision of NRS 205.461 to 205.4657, inclusive, and sections 2 to 5, inclusive, of this act, the court records must clearly reflect that the violation was committed by the person convicted of***

the violation and not by the person whose personal identifying information forms a part of the violation.

Sec. 6. ***1. A person shall not establish or possess a financial forgery laboratory with the intent to commit any unlawful act.***

2. Unless a greater penalty is provided pursuant to specific statute, a person who violates this section is guilty of a category B felony and shall be punished by imprisonment in the state prison for a minimum term of not less than 1 year and a maximum term of not more than 20 years, and may be further punished by a fine of not more than $100,000.

3. For the purposes of prosecuting a violation of this section, the prosecuting attorney may present expert testimony to provide a prima facie case that any computer, system, program or electronic or mechanical device, or any combination thereof, is specifically configured for any purpose set forth in subparagraph (1) or (2) of paragraph (b) of subsection 4.

4. As used in this section:

(a) "Computer" has the meaning ascribed to it in NRS 205.4735.

(b) "Financial forgery laboratory" means any computer, system, program or other electronic or mechanical device, or any combination thereof, that is specifically configured for the purpose of unlawfully:

(1) Obtaining personal identifying information of another person to commit an unlawful act; or

(2) Manufacturing any forged or fraudulent financial instrument, document or item, including, without limitation, any negotiable instrument, check, draft, bond, credit card, debit card, stock certificate, annuity, bank bill or note, draft, bill of exchange, contract, promissory note, traveler's check or money order.

(c) "Personal identifying information" has the meaning ascribed to it in NRS 205.4617.

(d) "Program" has the meaning ascribed to it in NRS 205.475.

(e) "System" has the meaning ascribed to it in NRS 205.476.

Sec. 7. NRS 205.461 is hereby amended to read as follows:

205.461 As used in NRS 205.461 to 205.4657, inclusive, ***and sections 2 to 5, inclusive, of this act,*** unless the context otherwise requires, the words and terms defined in NRS 205.4613 to 205.4627, inclusive, ***and sections 2, 3 and 4 of this act*** have the meanings ascribed to them in those sections.

Sec. 8. NRS 205.4617 is hereby amended to read as follows:

205.4617 ~~["Personal]~~

1. Except as otherwise provided in subsection 2, "personal identifying information" means any information designed, commonly used or capable of being used, alone or in conjunction

with any other information, to identify a living or deceased person, including, without limitation:

~~[1.]~~ ***(a)*** The ***current or former*** name, driver's license number, ***identification card number,*** social security number, ***checking account number,*** savings account number, credit card number, debit card number, ***financial services account number,*** date of birth, place of employment and maiden name of the mother of a person ***.*** ~~[;~~ ~~and~~

~~2.]~~ ***(b)*** The ***unique biometric data of a person, including, without limitation, the*** fingerprints, ***facial scan identifiers,*** voiceprint, retina image and iris image of a person.

(c) The electronic signature, unique electronic identification number, address or routing code, telecommunication identifying information or access device of a person.

(d) The personal identification number or password of a person.

(e) The alien registration number, government passport number, employer identification number, taxpayer identification number, Medicaid account number, food stamp account number, medical identification number or health insurance identification number of a person.

(f) The number of any professional, occupational, recreational or governmental license, certificate, permit or membership of a person.

(g) The number, code or other identifying information of a person who receives medical treatment as part of a confidential clinical trial or study, who participates in a confidential clinical trial or study involving the use of prescription drugs or who participates in any other confidential medical, psychological or behavioral experiment, study or trial.

(h) The utility account number of a person.

2. To the extent that any information listed in subsection 1 is designed, commonly used or capable of being used, alone or in conjunction with any other information, to identify an artificial person, "personal identifying information" includes information pertaining to an artificial person.

Sec. 9. NRS 205.463 is hereby amended to read as follows:

205.463 1. Except as otherwise provided in ~~[subsection 2,]~~ ***subsections 2 and 3,*** a person who knowingly:

(a) Obtains any personal identifying information of another person; and

(b) Uses the personal identifying information to harm that other person or for any unlawful purpose, including, without limitation, to obtain credit, a good, a service or anything of value in the name of that person,

➥ is guilty of a category B felony and shall be punished by imprisonment in the state prison for a minimum term of not less than 1 year and a maximum term of not more than 20 years, and may be further punished by a fine of not more than $100,000.

2. ~~[A]~~ ***Except as otherwise provided in subsection 3, a*** person who knowingly:

(a) Obtains any personal identifying information of another person; and

(b) Uses the personal identifying information to avoid or delay being prosecuted for an unlawful act,

➥ is guilty of a category ~~[E]~~ ***C*** felony and shall be punished as provided in NRS 193.130.

3. ***A person who violates:***

(a) Subsection 1 or 2 by obtaining and using the personal identifying information of an older person or a vulnerable person; or

(b) Subsection 2 to avoid or delay being prosecuted for an unlawful act that is punishable as a category A felony or category B felony,

➥ is guilty of a category B felony and shall be punished by imprisonment in the state prison for a minimum term of not less than 3 years and a maximum term of not more than 20 years, and may be further punished by a fine of not more than $100,000.

4. In addition to any other penalty, the court shall order a person convicted of violating subsection 1 to pay restitution, including, without limitation, any attorney's fees and costs incurred to:

(a) Repair the credit history or rating of the person whose personal identifying information he obtained and used in violation of subsection 1; and

(b) Satisfy a debt, lien or other obligation incurred by the person whose personal identifying information he obtained and used in violation of subsection 1.

Sec. 10. NRS 205.464 is hereby amended to read as follows:

205.464 1. ~~[A]~~ ***Except as otherwise provided in subsection 2, a*** public officer or public employee who knowingly:

(a) Obtains any personal identifying information of another person from any document, file, database, source or process used by a public body to collect, store, maintain, transfer, reproduce, manage or administer personal identifying information; and

(b) Uses the personal identifying information to harm that other person or for any unlawful purpose, including, without limitation, to obtain credit, a good, a service or anything of value in the name of that person,

➥ is guilty of a category B felony and shall be punished by imprisonment in the state prison for a minimum term of not less

than 5 years and a maximum term of not more than 20 years, and may be further punished by a fine of not more than $100,000.

2. ~~[In addition to any other penalty, the court shall order a public officer or public employee convicted of violating subsection 1 to pay restitution, including, without limitation, any attorney's fees and costs incurred to:~~

~~(a) Repair the credit history or rating of the person whose personal identifying information the public officer or public employee obtained and used in violation of subsection 1; and~~

~~(b) Satisfy a debt, lien or other obligation incurred by the person whose personal identifying information the public officer or public employee obtained and used in violation of subsection 1.~~

~~3.]~~ A ***public officer or public employee who violates subsection 1 by obtaining and using the personal identifying information of an older person or a vulnerable person is guilty of a category B felony and shall be punished by imprisonment in the state prison for a minimum term of not less than 7 years and a maximum term of not more than 20 years, and may be further punished by a fine of not more than $100,000.***

3. Except as otherwise provided in subsection 4, a public officer or public employee who knowingly:

(a) Obtains any personal identifying information of another person from any document, file, database, source or process used by a public body to collect, store, maintain, transfer, reproduce, manage or administer personal identifying information; and

(b) Possesses, sells or transfers the personal identifying information for the purpose of establishing a false status, occupation, membership, license or identity for himself or any other person,

➥ is guilty of a category C felony and shall be punished as provided in NRS 193.130.

4. A public officer or public employee who ***violates subsection 3 by obtaining and possessing, selling or transferring the personal identifying information of an older person or a vulnerable person is guilty of a category B felony and shall be punished by imprisonment in the state prison for a minimum term of not less than 1 year and a maximum term of not more than 20 years, and may be further punished by a fine of not more than $100,000.***

5. Except as otherwise provided in subsection 6, a public officer or public employee who knowingly aids another public officer or public employee to commit a violation of any provision of this section is guilty of a category C felony and shall be punished as provided in NRS 193.130.

~~[5.]~~ ***6. A public officer or public employee who violates subsection 5 by knowingly aiding another public officer or public employee in committing a violation of this section by obtaining the***

personal identifying information of an older person or a vulnerable person is guilty of a category B felony and shall be punished by imprisonment in the state prison for a minimum term of not less than 1 year and a maximum term of not more than 20 years, and may be further punished by a fine of not more than $100,000.

7. The provisions of this section do not prohibit the possession or use of any personal identifying information by officers of local police, sheriff and metropolitan police departments and by agents of the Investigation Division of the Department of Public Safety while engaged in undercover investigations related to the lawful discharge of their duties.

8. In addition to any other penalty, the court shall order a public officer or public employee convicted of violating any provision of this section to pay restitution, including, without limitation, any attorney's fees and costs incurred to:

(a) Repair the credit history or rating of the person whose personal identifying information the public officer or public employee obtained and used in violation of subsection 1; and

(b) Satisfy a debt, lien or other obligation incurred by the person whose personal identifying information the public officer or public employee obtained and used in violation of this section.

Sec. 11. NRS 205.465 is hereby amended to read as follows:

205.465 1. It is unlawful for a person to possess, sell or transfer any document or personal identifying information for the purpose of establishing a false status, occupation, membership, license or identity for himself or any other person.

2. ~~[A]~~ ***Except as otherwise provided in subsection 3, a*** person who:

(a) Sells or transfers any such document or personal identifying information in violation of subsection 1; or

(b) Possesses any such document or personal identifying information in violation of subsection 1 to commit any of the crimes set forth in NRS 205.085 to 205.217, inclusive, 205.473 to 205.513, inclusive, or 205.610 to 205.810, inclusive,

➥ is guilty of a category C felony and shall be punished as provided in NRS 193.130.

3. ***A person who violates subsection 2 by selling or transferring the personal identifying information of an older person or a vulnerable person is guilty of a category B felony and shall be punished by imprisonment in the state prison for a minimum term of not less than 1 year and a maximum term of not more than 20 years, and may be further punished by a fine of not more than $100,000.***

4. Except as otherwise provided in this subsection and ~~[subsection 2,]~~ ***subsections 2 and 3,*** a person who possesses any

such document or personal identifying information in violation of subsection 1 is guilty of a category E felony and shall be punished as provided in NRS 193.130. If a person possesses any such document or personal identifying information in violation of subsection 1 for the sole purpose of establishing false proof of age, including, without limitation, establishing false proof of age to game, purchase alcoholic beverages or purchase cigarettes or other tobacco products, the person is guilty of a misdemeanor.

~~[4.]~~ ***5.*** Subsection 1 does not:

(a) Preclude the adoption by a city or county of an ordinance prohibiting the possession of any such document or personal identifying information; or

(b) Prohibit the possession or use of any such document or personal identifying information by officers of local police, sheriff and metropolitan police departments and by agents of the Investigation Division of the Department of Public Safety while engaged in undercover investigations related to the lawful discharge of their duties.

Sec. 12. NRS 205.4653 is hereby amended to read as follows:

205.4653 A person who violates any provision of NRS 205.461 to 205.4657, inclusive, ***and sections 2 to 5, inclusive, of this act*** may be prosecuted for the violation whether or not the person whose personal identifying information forms a part of the violation ~~[is]~~ ***:***

1. Is living or deceased during the course of the violation or the prosecution.

2. Is an artificial person.

3. Suffers financial loss or injury as the result of the violation.

Sec. 13. NRS 205.4657 is hereby amended to read as follows:

205.4657 ***1.*** In any prosecution for a violation of any provision of NRS 205.461 to 205.4657, inclusive, ***and sections 2 to 5, inclusive, of this act,*** the State is not required to establish and it is no defense that:

~~[1.]~~ ***(a)*** An accessory has not been convicted, apprehended or identified; or

~~[2.]~~ ***(b)*** Some of the acts constituting elements of the crime did not occur in this State or that where such acts did occur they were not a crime or elements of a crime.

2. In any prosecution for a violation of any provision of NRS 205.461 to 205.4657, inclusive, and sections 2 to 5, inclusive, of this act, the violation shall be deemed to have been committed and may be prosecuted in any jurisdiction in this State in which:

(a) The person whose personal identifying information forms a part of the violation currently resides or is found; or

(b) Any act constituting an element of the crime occurred, regardless of whether the defendant was ever physically present in that jurisdiction.

Sec. 14. Chapter 97A of NRS is hereby amended by adding thereto a new section to read as follows:

1. When issuing a credit card to a cardholder in this State, an issuer shall provide the cardholder with the written notice in the form prescribed by the Commissioner of Financial Institutions pursuant to this section.

2. The Commissioner of Financial Institutions shall adopt regulations prescribing the form of the written notice required pursuant to this section. The regulations must provide that the written notice must:

(a) Include, without limitation, the following information:

(1) The policies and procedures adopted by the issuer to protect the personal identifying information and credit information of the cardholder from any unlawful use by another person; and

(2) The legal rights and responsibilities of the cardholder if another person unlawfully uses the personal identifying information and credit information of the cardholder; and

(b) Be printed in a separate box created by bold lines that includes:

(1) A heading indicating the general subject matter of the notice that is printed in at least 12-point type; and

(2) The text of the notice that is printed in at least 10-point type.

3. An issuer that 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.

4. As used in this section:

(a) "Credit information" means any information that is related to credit and derived from a consumer credit report, found on a consumer credit report or provided on an application for a credit card.

(b) "Personal identifying information" has the meaning ascribed to it in NRS 205.4617.

Sec. 15. NRS 97A.140 is hereby amended to read as follows:

97A.140 1. An issuer located in this State shall not issue a credit card to a cardholder unless ~~[he first receives]~~ ***the issuer first:***

(a) Provides the written notice required pursuant to section 14 of this act to the cardholder; and

(b) Receives a written or oral request from the cardholder for the issuance of the credit card.

2. An issuer shall provide the cardholder with the terms and conditions that govern the use of the credit card, in writing, before or at the time of the receipt of the credit card. A cardholder shall be deemed to have accepted the written terms and conditions provided by the issuer upon subsequent actual use of the credit card.

3. The rate of interest charged, and any other fees or charges imposed for the use of the credit card, must be in an amount agreed upon by the issuer and cardholder.

4. An issuer may unilaterally change any term or condition for the use of a credit card without prior written notice to the cardholder unless the change will adversely affect or increase the costs to the cardholder for the use of the credit card. If the change will increase such costs, the issuer shall provide notice to the cardholder of the change at least 30 days before the change becomes effective.

5. Unless otherwise stated as a term or condition, the law of this State governs all transactions relating to the use of a credit card if an issuer, or the service provider of an issuer, is located in this State.

Sec. 16. Chapter 239B of NRS is hereby amended by adding thereto a new section to read as follows:

1. If a public body maintains a website on the Internet, the public body shall not disclose on that website personal information unless the disclosure is required by a federal or state statute or regulation.

2. If it appears that a public body has engaged in or is about to engage in any act or practice which violates subsection 1, the Attorney General or the appropriate district attorney may file an action in any court of competent jurisdiction for an injunction to prevent the occurrence or continuance of that act or practice.

3. An injunction:

(a) May be issued without proof of actual damage sustained by any person.

(b) Does not preclude the criminal prosecution and punishment of an act or practice that may otherwise be prohibited by law.

4. As used in this section:

(a) "Personal information" has the meaning ascribed to it in section 21 of this act.

(b) "Public body" has the meaning ascribed to it in NRS 205.462.

Sec. 17. Title 52 of NRS is hereby amended by adding thereto a new chapter to consist of the provisions set forth as sections 18 to 28, inclusive, of this act.

Sec. 18. ***As used in this chapter, unless the context otherwise requires, the words and terms defined in sections 19, 20 and 21 of this act have the meanings ascribed to them in those sections.***

Sec. 19. *"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.*

Sec. 20. *"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.*

Sec. 21. *"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:*

1. Social security number or employer identification number.

2. Driver's license number or identification card number.

3. 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.

➥ The term does not include publicly available information that is lawfully made available to the general public.

Sec. 22. *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.

Sec. 23. *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.

Sec. 24. *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.

Sec. 25. *A data collector who provides the notification required pursuant to section 24 of this act 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.*

Sec. 26. *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 section 24 of this act, including, without limitation, labor, materials, postage and any other costs reasonably related to providing such notification.

Sec. 27. ***Any waiver of the provisions of this chapter is contrary to public policy, void and unenforceable.***

Sec. 28. ***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, he may bring an action against that person to obtain a temporary or permanent injunction against the violation.***

Sec. 29. Chapter 597 of NRS is hereby amended by adding thereto a new section to read as follows:

1. A business in this State shall not transfer any personal information of a customer through an electronic transmission other than a facsimile to a person outside of the secure system of the business unless the business uses encryption to ensure the security of electronic transmission.

2. As used in this section:

(a) "Encryption" has the meaning ascribed to it in NRS 205.4742.

(b) "Personal information" has the meaning ascribed to it in section 21 of this act.

Sec. 30. 1. This section and sections 1 to 13, inclusive, of this act become effective on October 1, 2005.

2. Sections 14 to 28, inclusive, of this act become effective on January 1, 2006.

3. Section 29 of this act becomes effective on October 1, 2008.