A.B. 179
Data Breach Notification Law

Assembly Committee: Commerce and Labor
Exhibit: I Page 1 of 10 Date: 03/16/2015
Submitted by: Edgar Flores

By:
Assemblyman Edgar Flores
Expert Witnesses: Ira Victor and Jim Elste

Committee: Commerce and Labor
March 16, 2015

Overview of NRS 603A

NRS 603A requires for Data Collectors and businesses that maintain records containing "personal information" to do the following:

1) implement reasonable security measures to protect the information from unauthorized access or use

2) provide immediate notification concerning any breach of security

3) not transfer a customer's personal information outside of the secure system unless the business uses encryption to ensure the security, and

4) take reasonable steps to destroy any records containing "personal information" whenever it is no longer needed to maintain the records.

Overview of NRS 603A continued

For purposes of these requirements, NRS 603A defines "personal information" as:

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:

I-3

- Social security number or employer identification.
- Driver's license number or identification card number.
- 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. Under current state law, a business or data collector who experiences a breach of customer information is only required to notify the person if the data falls into the categories covered in NRS 603A.040.

Why Data Breach Notification Laws?

- Puts victims on notice
- Allows victims to take evasive action (cancel credit cards, change passwords, etc)
- Most cyber criminals operate from outside our U.S. borders
- Least burdensome approach for businesses (no complex encryption requirements, sanctions, etc.)

Current Issues with NRS 603A

- If records containing personal information such as passport numbers, medical identification numbers, or passwords are compromised, a business or data collector is currently not required to notify the affected consumers.

Proposed Amendment

- In an effort to address the issues with 603A this bill was put forth amending the current statute to expand the definition of Personal Information to ensure more information is protected and victims have to be notified
- Why the new amendment to the bill
- Please refer to Amendment handout

New Language

- Data collectors and businesses must be in compliance by January 1, 2017

NRS 603A.040 "Personal information" defined. "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 email address, in combination with a password, access code or security question and answer that would permit access to an online account.

The term does not include the last four digits of a social security number, the last four digits of a driver's license number or the last four digits of an identification card number or publicly available information that is lawfully made available to the general public.

Implementation

- Data Collectors and Businesses are already required to have reasonable (whatever is customary in the industry) firewalls in place to protect Personal Information; hence this is more of a settings change.

Good Public Policy

- Many Data collectors and Businesses Already Notify Consumers When This Personal Information Is Stolen
- Examples of data breaches: Lowes, LinkedIn, and Target
- This amendment is following the national trend
- Victims have a right to know
- Not overly burdensome to data collectors and businesses

What this bill does not do

- This bill does not alter the current "reasonable measures standard" to protect personal information
- This bill does not alter any of the current remedies
- This bill does not create new sanctions for failure to comply with NRS 603A nor does it create new penalties or punishment for engaging in cyber crime