

Nevada's New Data Security Law

An Overview and Assessment

Paul R. Mudgett, CISSP, CISA

On January 1, 2010 Nevada's new data security law goes into effect. Efforts made during the 2009 session of the Nevada Legislature produced this landmark bill which the Governor signed into law and soon will impact the way businesses and government agencies within Nevada transmit and store personally identifiable information (PII). The new section within Nevada Revised Statutes Chapter 603A essentially contains the measures for the protection of PII, a "safe harbor" clause, and definitions.

"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 Data Security Standard, as adopted by the PCI Security Standards Council or its successor organization..."

The PCI Security Standards Council is represented by the five major credit card brands: Visa, MasterCard, American Express, Discover Financial Services, and JCB International. They developed and adopted 12 requirements for the protection of credit card information for those merchants who store, process, or transmit credit card information. Those merchants who fail to meet PCI compliance are subject to fine or the removal of credit card processing capability. This industry standard has become State law with the addition of this section in the legislation.

Rank	Victim State	Complaints per 100,000 Population	Complaints
1	Arizona	149.0	9,683
2	California	139.1	51,140
3	Florida	133.3	24,440
4	Texas	130.3	31,708
5	Nevada	126.0	3,275
6	New York	116.2	22,647
7	Georgia	111.0	10,748
8	Illinois	106.4	13,726
9	New Mexico	104.9	2,081
10	Colorado	100.9	4,983

"Consumer Sentinel Network Data Book for January – December 2008" Federal Trade Commission. February 2009

What does this mean? Essentially, if you process, store or transmit credit card information as part of your business, you must comply with PCI-DSS. Adding this to NRS really has no significant impact as the requirement to comply already existed. While the 12 requirements of PCI-DSS only applies to credit card information, these same requirements can aid substantially in protecting other PII such social security number and date of birth if applied to these components.

"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"

What does this mean? You cannot send PII over e-mail, ftp, or other manner if the information is not encrypted. This includes attachments that are sent if they are not encrypted. This has always been a bad

idea anyway considering e-mail is an electronic version of a postcard. E-mail is not the only concern when it comes to the unauthorized disclosure of PII. Ask yourself the following:

- Do employees have unmonitored access to social networking sites such as Facebook, Twitter, LinkedIn, and MySpace?
- Have employees installed P2P file sharing and communication software such as Kazaa and Skype that may include the ability to transfer files with PII unencrypted?
- Do employees use Instant Messaging platforms to communicate externally such as GoogleTalk, Windows Live, AIM, and Yahoo?

These are all potential exposures that need to be considered when complying with a law designed to protect PII. However, compliance here is not necessarily cost prohibitive. Of course an appropriate use policy needs to be in place however, that may not be enough as employees may accidentally send prohibited data over e-mail or they may ignore the statute in the interest of “convenience”. There are however several inexpensive or even free applications that can be deployed that can encrypt information while in transit. The key here is to train your staff to use these tools appropriately.

(b) Move any data storage device containing personal information beyond the logical or physical controls of the data collector or its data storage contractor unless the data collector uses encryption to ensure the security of the information.

This particular section of the new law creates the most potential for change in process and technology for an organization. This refers to information kept on removable media that leaves the physical controls of the office or facility. The data storage device could be a laptop, thumb drive, iPhone or Blackberry, portable hard drive, or CD/DVD among other sources. Some questions to ask include:

- Do employees carry laptops that have spreadsheets and other documents that may contain PII on the hard drive?
- Do we allow thumb drives and other removable media within our environment that may allow for PII to be carried off-site?
- What information can be accessed by PDA’s and smartphones?
- Do we share information with a partner using CD/DVD and the US Mail?

This obviously creates an issue for today’s mobile workforce. Solutions vary from policies prohibiting PII on laptops (presents the ‘how do you know’ problem) to full disk encryption with key escrow (can be expensive and complex) to everything in between. Whatever solution you decide should weigh the risk of disclosure and non-compliance with the ability for employees to perform their business functions.

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.***

This is the “safe harbor” clause of this legislation. Basically, if you meet or exceed the standards of “best practices” established by the state of Nevada, the law grants a shield from liability. It does not prevent civil action being taken against you for a breach but may offer some protection against damages in the event of a breach. The thresholds for “best practice” will most likely be determined in court but those who take serious efforts to comply using administrative and technical controls will most likely be better positioned to defend against a civil action.

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.*

The definition here is important. Effectively, any device that can store PII is covered under the provisions of this NRS Chapter. As noted earlier, if any of these devices leaves the physical control of the office or facility, that information must be encrypted. This would include but certainly isn't limited to laptops, netbooks, iPhones, Blackberry's, thumb drives, portable hard drives, and DVD's.

- (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; and*
 - (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.*

This replaces the previous definition of encryption in NRS which allowed any type of encryption standard to be used even if it was obsolete. What this means is if you are to use encryption for data in transit or in storage, it must meet the requirements established by a recognized standards setting body. Following NIST is a good choice and most legitimate encryption programs will adhere to such standards.

The second piece of this is safeguarding the keys used for encryption. Encryption is pretty useless if the keys are not protected. When using encryption it is important to consider key management including key generation, use, storage, recovery and destruction. Think about how to support or recover data if the key is destroyed or if changing keys, how will it affect access to the data.

Ultimately, this new law simply reinforces good security practices for businesses that handle personally identifiable information. Organizations can reduce the intimidation factor by simply engaging in efforts to understand how PII flows inside and outside the organization, evaluate business processes that use PII and then investigate both open source and commercial software that best meet the specific protection requirements of the organization. Remember that information security is an ongoing process, not a check the box exercise. As always, seek legal advice when it comes to complying with State and Federal laws.



About the Author: Paul Mudgett is an internationally certified information security professional with over 15 years experience working with organizations in highly regulated environments, government agencies, and higher education to meet security and compliance obligations. Mudgett continues to focus on the discipline of information security leadership, developing positive security behavior in the workplace, and aligning information security with business strategy.