

# Is Nevada's New Privacy Law a 'Game-Changer?'

## A First: PCI Compliance Mandated for State's Merchants

July 6, 2009 - Linda McGlasson, Managing Editor, *BankInfoSecurity.com*

Should individual states mandate that businesses comply with the Payment Card Industry's Data Security Standard (**PCI DSS**)?

The answer is "yes," according to Nevada, which has **passed a new law** that, as of next year, requires businesses to comply with PCI when collecting or transmitting payment card information.

Nevada is the first state to mandate full PCI compliance for businesses. Minnesota in 2007 incorporated only a portion of PCI in its **Plastic Card Security Law**.

According to Nevada's new law, if a data collector doing business in that state accepts a payment card in connection with a sale of goods or services, the data collector shall comply with the current version of PCI DSS, 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.

### Is it a Game-Changer?

As states rush to adopt or strengthen privacy legislation, Nevada's move is seen by some observers as a potential "game-changer." But they question whether states should be in the business of mandating compliance with an industry standard.

Privacy and information security expert Dr. Larry Ponemon, President and Founder of the Ponemon Institute, says that generally the law makes sense because PCI provides reasonable security requirements that should be achievable by most companies. Yet, he is somewhat concerned that government entities like Nevada are now legislating detailed information security requirements for business. "PCI is a self-regulatory program. I'm sure that mandated compliance through legislation was never anticipated by the program founders," Ponemon states.

"I imagine that many other states that have been waiting in the wings will also follow suit, as happened after the California Data Breach Notification Laws," says Nick Holland, senior analyst at Aite Group, a research firm that studies trends in the financial services industry. "I'm not sure, however, if leaving the compliance dates to individual card brands rather than the PCI Security Standards Council may cause some problematic ambiguity. Would there be a possibility for card networks having separate compliance dates?"

Holland notes that Aite has just conducted some research of payment card industry executives that shows respondents say while states may bring legislation forward,

they do not believe that government intervention is required to make PCI enforceable. "Instead, it was considered that the card networks need to play a bigger role in enforcing compliance," he notes.

When Agnes Bundy Scanlan, an attorney at Goodwin Proctor and a board member of the International Association of Privacy Professionals (IAPP), recently attended a privacy association meeting, she was surprised to learn that this new law was not on privacy professionals' radar. "Notably the law has not attracted the same attention as the new [Massachusetts law](#) or any of the California data and privacy laws," says Bundy Scanlan. "Nevertheless, like the Massachusetts law, this Nevada PCI compliance might become a model for other states. Also of note -- this law has a safe harbor for merchant already compliant with PCI."

### **Law Categorizes Merchants**

The law places companies that collect personal identifiable information (PII) into one of two categories: those that accept payment cards, and all others. For the ones that accept payment cards and are already subject to PCI-DSS, not much changes for them apart from they can held liable for noncompliance, instead of just disqualified from accepting cards, notes Tom Wills, Senior Analyst, Security & Fraud, Javelin Strategy and Research.