

TWO STATES PASS STRICT PCI COMPLIANCE LAWS

Nevada and Massachusetts have passed laws that deal strictly with Payment Card Industry (PCI) compliance. The laws focus on protecting personal information of consumers while it is “at rest” as well as when it is transmitted.

NEVADA

Nevada Senate Bill 227, *Nevada Data Security and Privacy Law*, was effective January 1, 2010. It is called a groundbreaking law because it is the first state to require compliance with PCI-DSS (Data Security Standard) in its *entirety*. It remains to be seen whether this law will create a nationwide response similar to what happened after California enacted the first information security breach notification statute.

To understand any law, it is important to understand the definitions. In this law, the following are essential to comprehension:

Data Collector – includes corporations and financial institutions that (whether by automated collection or otherwise) handle, collect, disseminate or otherwise deal with nonpublic personal information.

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.

Personal Information - Includes:

- Social Security number (SSN) (excluding truncated ones with only the last 4 digits);
- Drivers license (DL) or identification card (ID) number; or
- Account number, credit card or debit card number, in combination with any required code that permits access to an account.

REQUIREMENTS OF THE LAW

If accepting payments via payment card, the data collector must comply with PCI-DSS in its entirety.

If not accepting payments via a payment card, the data collector must use encryption to transmit consumer’s personal information electronically beyond its secure environment or if a data storage device is moved beyond the logical or physical controls of the collector or its data storage contractor.

This law applies to a company’s operation anywhere in the U.S. if the company does business in Nevada. It applies regardless of whether the personal information involved is related to Nevada residents or residents of other states.

The requirements do not apply to:

- A telecommunications provider acting solely in the role of conveying the communications of other persons; or
- Data transmission over a secure, private communication channel for specified reasons.

The law may be read at http://leg.state.nv.us/75th2009/Bills/SB/SB227_EN.pdf.

MASSACHUSETTS

Massachusetts Commonwealth Rule 17.00, *Standards for Protection of Personal Information of Residents of the Commonwealth*, will be effective March 1, 2010. While it does not go to the same level of requiring compliance with PCI in its entirety as the Nevada law, it does require extensive protection of personal consumer information.

Definitions

Owns or licenses – Receives, stores, maintains, processes, or otherwise has access to personal information in connection with the provision of goods or services or in connection with employment.

Person

A natural person, corporation, association, a partnership or other legal entity, other than an entity of the Commonwealth or its branches or political subdivisions.

Personal Information

A Massachusetts resident's first and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident.

- SSN;
- DL or state-issued ID card; or
- Financial account number, or credit or debit card number, with or without any required security code, access code, PIN or password, that would permit access to a resident's financial account; provided, however, that "personal information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

Service Provider

Any person that receives, stores, maintains, processes, or otherwise is permitted access to personal information through its provision of services directly to a person that is subject to this regulation.

REQUIREMENTS OF THE LAW

Applies to every "person" that owns or licenses personal information about a resident of Massachusetts. That "person" must develop, implement, and maintain a written comprehensive information security program. The Law requires the plan to be appropriate to the size, scope and type of business; the amount of resources available; the amount of stored data; and the need for security and confidentiality of both consumer and employee information.

The "person" must appoint one or more employees to maintain the information security program. The law requires the development of a process to identify and assess reasonably foreseeable internal and external risks. In the law there are six elements that must be covered by this identification and assessment process.

Computer System Security

Requirements include ensuring that certain items be included in the information security program covering its computers, including any wireless system that at a minimum, and to the extent technically feasible, has the eight listed elements.

This Law does not require "certification" to these standards or an outside assessment. (An earlier version did require certification.)

The Law may be reviewed at <http://op.bna.com/pl.nsf/id/byul-7xbun5>.