PCI: Eye to eye with federal law

By Ross Federgreen
CSRSI

The Payment Card Industry (PCI) Data Security Standard is consistent with broad-based federal legislation dating back to the early 1990s. It is essential that you, as ISOs and merchant level salespeople, have basic knowledge of these laws so you can offer greater value to your customers.

The majority of merchants believe PCI does not affect them, is unfair, unenforceable, unnecessary and without merit. Also, those who recognize the importance of PCI and have attempted to become compliant have been given much erroneous information.

Take penetration scans, for example, which many mistakenly believe satisfy PCI compliance. In truth, penetration scans, while important, constitute neither the core nor the majority of PCI requirements.

Penetration scans are a minor PCI component that do not and will not prevent the majority of breaches, which are local in nature. By local breaches, I mean at merchants' facilities and perpetrated by employees or other parties in trusted relationships.

Legislation on the books

A significant number of major federal laws overlap with PCI. The emphasis in all of these is on appropriate procedure and policy to protect data integrity. The relevant acts include the:

- Hospital Insurance Portability and Accountability Act of 1996 (HIPAA), Title II, Security
- Graham Leach Bliley Act of 1999 (GLB Act)
- Public Company Accounting Reform and Investor Protection Act of 2002 (Sarbanes-Oxley Act, also called SOX and Sarbox)
- Fair and Accurate Transaction Act of 2003 (FACTA)
- Department of Veterans Affairs Information Security Act of 2006
- Family Educational Rights and Privacy Act (FERPA)
- Drivers Privacy Protection Act of 1994 (DPPA)
- Customer Identification Program Rules implementing Section 326 of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA Patriot Act)
- Federal Trade Commission Act of 1914 (FTC Act) and FTC Standards for Safeguarding Customer Information (FTC Safeguards Rule) enacted in 2003.

Acts in the wings

Additionally, there is ongoing legislative activity in these areas both on the federal and state level. The most important piece of pending federal legislation is the 2007 Privacy and Data Security Act. On the state level, there has been much activity since the TJX Companies Inc. breach, placing additional regulatory and financial burdens on merchants.

A compelling concept voiced in the Privacy and Data Security Act of 2007 is the notion of "safe harbor" for compliance. Although the application of this to individual merchants is not clear, it is being offered in a carrot and stick fashion.

Regulations in motion

Three of the security statutes that have wide application are the HIPAA Title II, GLB Act Title V and FTC Safeguards Rule. A brief synopsis of each follows:

HIPAA Title II, Security Rule

According to the Federal Register, HIPAA Title II affects

up to four million entities. This includes everything from major medical centers to individual medical offices of every type.

Many of these facilities now accept credit cards, and the list is growing. Careful analysis of the requirements of HIPAA Title II reveals much overlap with PCI.

HIPAA Title II's final security compliance date for all entities covered by the act was April 2006.

HIPAA has potential to cause far-reaching impact on enterprises in unrelated industries such as banking, accounting and financial services. This originates with HIPAA's provision governing the "business associates" of health care organizations.

The final security rule is divided into three broad categories of safeguards: administrative, physical and technical. It contains 42 security specifications.

The rule addresses the security posture needed to support the HIPAA Title I, Privacy Rule. The 42 security specifications are divided into those that are addressable and those that are required.

Addressable rules must be implemented based upon specific characteristics of a given entity. Required rules must be implemented by all covered entities. Required security specifications that overlap with PCI include:

- Risk management
- Information security activity review
- Assigned security responsibility
- Information access management
- Security awareness and training
- Security incident procedures
- Response and reporting
- Data backup plan
- Disaster recovery plan
- Business associate contracts and other arrangements
- Workstation use
- Workstation security
- Disposal
- Unique user identification
- Audit controls
- Person or entity authentication

Almost every required security issue listed in HIPAA Title II is associated with specific areas within PCI. The "rule book" for implementation of HIPAA Title

II is Medicare & Medicaid Services (CMS) Business Partners Systems Security Manual, Rev. 8, published April 6, 2007. The manual is 532 pages.

GLB Act

The GLB Act addresses privacy and security obligations of financial institutions, which are defined broadly as entities engaged in financial activities such as banking, lending, insurance, loan brokering and credit reporting.

The act governs two distinct types of protection for personal information: protection of security and protection of privacy. The security provisions require standards regarding appropriate physical, technical and procedural safeguards to ensure the security and confidentiality of customer records and information, and to protect against anticipated threats and unauthorized access to such information.

FTC Safeguards Rule

The FTC Safeguards Rule applies to a variety of financial institutions that are not subject to the GLB Act. Examples include nonbank mortgage lenders, loan brokers, tax preparers and debt collectors. The rule requires covered entities to develop a written information security plan that assigns employees to:

- oversee the program
- conduct risk assessment
- design and implement an information safeguards program
- require service providers to protect customers' information
- evaluate and adjust the program based on the entity's particular characteristics.

It also mandates a data security plan that accounts for each entity's particular circumstances, including size and complexity, the nature and scope of activities, and the sensitivity of customer information it handles.

The critical concept of PCI is to empower merchants with the information necessary to understand where security lapses may be present within their environments and afford them true guidance about necessary rules and regulations that must be applied to obtain data security objectives.

This is why it is imperative to emphasize the policies and procedures that will achieve PCI compliance for merchants and, thus, protection for both consumers and the overall system.

Ross Federgreen is founder of CSRSI, The Payment Advisors, a leading electronic payment consultancy specifically focused on the merchant. He can be reached at 866-462-7774, ext. 23, or rfedergreen@csrsi.com.