By Ross Federgreen

A Common STANDARD

Taking the Mystery out of PCI

One of the many issues that will be addressed during ETA's 2006 Annual Meeting and Expo is the accepted common standard known as Payment Card Industry Data Security Standard (PCI). The result of ongoing industry efforts to promulgate a common standard, PCI derives from Visa's Cardholder Information Security Program (CISP) and the MasterCard's Site Data Protection Program (SDP). In addition, the PCI has been accepted and endorsed by American Express, Discover Financial Services and Japanese Credit Bureau (JCB).

The PCI requirements apply to all members, merchants and service providers that store, process or transmit cardholder data, and affect all "system components."

The program applies to all payment channels, including retail (known as brick-and-mortar), mail/telephone order and e-commerce, and its stated goal is to protect cardholder data—wherever it resides. This ensures that members, merchants and service providers maintain the highest information security standard.

PCI consists of a framework of 12 requirements, which are driven by the number and type of transactions that an individual entity stores, processes or transmits.

Visa, and others, use PCI as the common framework for the specific requirements of security compliance. Compliance with PCI is divided into two major categories—service providers and merchants. Each group is also subdivided by amount and type of transaction.

Service providers are divided into three categories. However, from the viewpoint of PCI, no distinction exists. All service providers were expected to have achieved validation by Sept. 30, 2004. Validation requires an annual onsite PCI Data Security Assessment by a qualified data security company, as well as ongoing quarterly network scans by a qualified independent scan vendor.

Under the PCI Standard, acquirers are responsible for determining their merchants' compliance validation levels. All merchants will fall into one of the four merchant levels based on annual Visa transaction volume—determined by the aggregate number of Visa transactions.

Compliance validation is required for Level 1 through 3 merchants (see

The Compliance Puzzle

Understanding the maze of compliance issues that vary from one card company to the next is a constant struggle for most payments professionals. With so many rules and regulations, getting the whole picture of compliance can be challenging even to the most adept of puzzle solvers.

This month, the Electronic Transactions Association (ETA) will bring Visa, MasterCard, American Express and Discover together in an unprecedented all-day seminar. Conveniently scheduled in conjunction with the 2006 Annual Meeting and Expo in Las Vegas, ETA will debut to its membership its newest educational program—Compliance Day.

"This event will be the one place to get answers to complex issues and insight directly from representatives of each of the major card brands," says Karin Van Duyse, ETA's director of education & professional development. Compliance Day has been designed to provide the attendee with not only an in-depth understanding of compliance, but also a congruent perspective for operating within card companies' rules and regulations.

The moderator for the event will be former ETA president, Mary Gerdts, president and CEO of POST Integrations Inc. "I am extremely excited about Compliance Day," she says. "It will offer, for the very first time, important compliance information from all the card brands, on a single stage."

— **By April Watkins,** *Transaction Trends* Contributing Editor

“Merchant Category Levels” chart), and is highly recommended for Level 4 merchants. Specific validation requirements vary, but are as follows:

For Level 1 merchants, a qualified data security company must complete an annual onsite PCI Data Security Assessment, or a company officer must perform an internal audit; a quarterly network scan by an independent scan vendor is also necessary at this level. By Sept. 30, 2004, all Level 1 merchants must have met compliance requirements.

At Levels 2 and 3, the merchant must complete an annual self-assessment questionnaire, as well as a quarterly network scan; all Level 2 and 3 merchants must have met compliance requirements by June 30, 2005.

For Level 4, the merchant should also be sure to file a yearly self-assessment questionnaire. These merchants must comply with PCI as well. However, the acquirer determines the actual compliance validation for all Level 4 merchants.

A Prescription for PCI

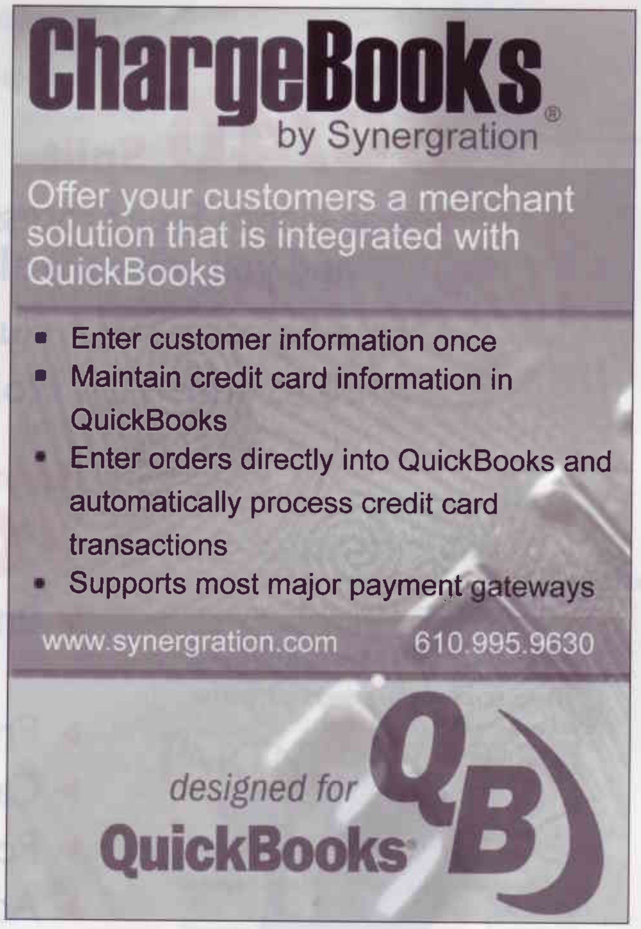
“The great strength of the PCI is that it is a blend of policy and prescription. It defines the core framework for creating an organization’s information assurance standard—but also provides specific guidance in key areas that matter,” says Aaron Bills, vice president and co-founder of 3 Delta Systems, who has hands-on experience with PCI.

“The greatest challenge for payment industry leaders is to accept the reality that we must care about the information we process and ensure that our employees have the same mindset,” he adds. “If the organizational attitude and culture are set, the rest is mechanics.”

Michael Smith, senior vice president, corporate risk and compliance for Visa USA, says “the effect of PCI has been overwhelmingly positive. PCI has focused the attention of all participants in the payments chain on what is necessary to safeguard cardholder data. PCI also has galvanized companies of all sizes to achieve comprehensive and uniform data security for their businesses, subject to verification.”

Seana Pitt, vice president of network development at American Express, agrees PCI is a good thing for the payment industry. “The original mission of the Data Security Industry Group, formed over two years ago, was to align on standards to eliminate confusion in the marketplace and drive merchant and POS provider adoption; this vision is becoming a reality,” Pitt says. “We are starting to see a much higher level of merchant engagement in gaining and working toward PCI compliance. With POS service providers, PCI compliance and certification is becoming a marketplace advantage.”

Echoing Bills, Smith says PCI has progressed, but, there is still much to do. To him, the greatest challenge to overcome



Merchant Category Levels

- **Level 1 (Four independent groups)**
  1. Any merchant—regardless of acceptance channel-processing more than 6 million Visa transactions per year.
  2. Any merchant that has suffered a hack or an attack that resulted in an account data compromise.
  3. Any merchant that Visa, at its sole discretion, determines should meet the Level 1 merchant requirements to minimize risk to the Visa system.
  4. Any merchant identified by any other payment card brand as Level 1.
- **Level 2** Any merchant processing 150,000 to 6 million Visa e-commerce transactions per year.
- **Level 3** Any merchant processing 20,000 to 150,000 Visa e-commerce transactions per year.
- **Level 4** Any merchant processing fewer than 20,000 Visa e-commerce transactions per year, and all other merchants processing up to 6 million Visa transactions per year.

is building awareness about the mandate of standardized security requirements.

Overall, PCI has eased data security for merchants, leading to higher levels of adoption and compliance, contends Pitt. Smith also says it has enlightened VISA about the compliance questions merchants still need clarified.

To achieve more uniform compliance, Pitt says PCI should not be static, and should evolve to better protect card members and merchants.

"For example, the tendency of some to focus the majority of resources and attention on e-commerce should be expanded to include all merchant industries," he says. "No industry is immune to compromises; risk is not isolated to e-commerce." American Express has already made its data security operating policy a requirement across industries, adds Pitt.

In summary, more universal understanding and knowledge of the complex PCI rules and regulations is needed to survive in today's dynamic payments industry. Compliance is no longer a meaningless platitude, but a core responsibility of everyone in the industry. ***TT***

Ross Federgreen is founder of CSRSI in Port Saint Lucie, FL, which advises clients on electronic payments costs, security, fraud, compliance and liability.