

**ACCELERATING YOUR CASH FLOW***By Silka Gonzalez and Matthew Oakes*

You can add PCI compliance to the list of things keeping financial executives up at night.

Developed by the major credit card companies, the Payment Card Industry Data Security Standard (PCI DSS) is a set of standards for credit card data security. While not a regulation, technically, it's as good as one. The standard covers any entity that accepts, stores, and/or processes credit cards and cardholder information. PCI DSS includes rigorous, and often complicated, requirements for security management, policies, procedures, network architecture, software design and other critical measures.

PCI compliance projects can be time consuming and require dedication of resources. Requirements such as network segmentation and encryption of payment account data flow can be especially tough on organizations that have not yet properly implemented their credit card processing environment.

But businesses ranging from small to Fortune 500 must all comply with the security standards, or risk revocation of their card-processing privileges, or worse, heavy fines from credit card companies. On top of the penalties and fines from credit card companies, failure to comply with PCI security standards can seriously impact an organization's financial stability, customer trust and reputation.

As the PCI standards have evolved and grown in complexity, financial executives are expected to understand their organization's requirements, and what it needs to do to maintain compliance. What's more, at the end of the day, an organization's top management will be held primarily responsible for being hacked, which is why it is also important to choose an auditor with discretion.

All of this has financial executives worried.

To help you sleep at night, here is a primer on PCI compliance.

**PCI OVERVIEW**

Developed by the founding payment brands (American Express, Discover, MasterCard, VISA and JCB) of the PCI Security Standards Council, PCI standards have been established to enhance the overall

security of credit card transactions to prevent fraud and identity theft crimes.

When implemented robustly, the PCI DSS offers several benefits:

- Protects cardholder information and identity.
- Prevents electronic payment fraud.
- Ensures consistent audits of security procedures.

Specifically, the standards target the security of payment account data (PCI DSS) and the development of secure payment applications that support compliance (PA DSS).

Each payment brand defines its own PCI compliance validation requirements, and develops and enforces its own penalties, fines, requirements, mandates and dates of compliance.

**WHO IT AFFECTS**

The PCI DSS affects any entity involved in credit card transactions and/or cardholder information flow, including the processing, storage and transmission of data. This can mean that companies at all stops on the financial supply chain may need to comply -- from merchants, to acquirers, issuers, payment application vendors, and other service providers, including transaction processors, payment gateways, payment application software vendors, credit reporting services, and many more.

**WHAT IS REQUIRED**

Depending on your role in credit card transactions, and the level of service based on volume, your compliance requirements may vary. Acquirers--typically merchant banks who acquire transactions and issue merchant IDs--are ultimately responsible for the compliance of their merchant population.

Merchants and service providers are required to undergo at least one of the following:

- A network scan performed quarterly by an Approved Scanning Vendor (ASV).

- 
- 
- An annual onsite review and security assessment by a Qualified Security Assessor (QSA).

The onsite review requires companies to follow these standards under strict guidelines:

- Build and maintain a secure network.
- Real-time credit card authorization and settlement
- Protect cardholder data
- Maintain a vulnerability management program.
- Implement strong access control measures.
- Monitor and test networks regularly.
- Maintain an information security policy.
- Complete an annual Self-Assessment Questionnaire.

The PCI DSS self-assessment questionnaire is a validation tool specifically designed to assist merchants and service providers in self-evaluating their compliance with PCI DSS standards.

#### **WHO TO GO TO FOR COMPLIANCE ASSISTANCE**

Fortunately, there are resources that financial executives can leverage to help with PCI compliance. Among them are ASVs, companies authorized to perform PCI scanning tests, and QSAs, companies and individuals qualified to perform PCI and PA DSS audits and reviews. Companies employing QSAs are responsible for providing an opinion regarding whether the PCI and/or PA DSS requirements are being met and documenting the results of the review. QSAs must determine whether or not compliance has been achieved. Additionally, financial executives should look for PCI-compliant payments solutions.

#### **THE BOTTOM LINE**

PCI compliance is here to stay and will definitely bring more and more countries, merchants/services providers, and cardholder information processing entities under the compliance umbrella. Statistically, too, there has never been a regulation with regards to information security that has faded away. They've always grown more and more in influence and become more important across industries.

Taking a larger role in their company's PCI efforts may seem like the last thing a financial executive would want to do in these challenging times. But the risks are too high for them to sit back.

The clock is ticking for all businesses that need to comply with the PCI security standards.

*Silka Gonzalez is president of Enterprise Risk Management, a leading provider of IT security and risk management services. Silka can be reached at [info@emrisk.com](mailto:info@emrisk.com). Matthew Oakes is president and chief executive officer of Direct Insite, a leading global provider of on-demand accounts payable, accounts receivable and payments solutions. Matthew can be reached at [matthew.oakes@directinsite.com](mailto:matthew.oakes@directinsite.com).*

---

*For more information, visit [www.directinsite.com](http://www.directinsite.com) or call 631-873-2900.*