A Merchant Progress Report

The Payment Card Industry Data Security Standard in 2007

In March 2007, RSA, The Security Division of EMC, conducted a study of businesses impacted by the Payment Card Industry (PCI) Data Security Standard (DSS) in North America. The survey gauged the progress of merchants in meeting the PCI DSS requirements and collected data regarding perceptions of the standard.

Individual respondents came from eighty companies impacted by the PCI DSS and represented all merchant levels as defined by Visa.

Progress and Outlook for Achieving Compliance

RSA asked survey respondents whether their respective companies have reported compliance as a result of either an internal or an external audit (conducted by a Qualified Security Assessor). Aggregated results were near even: 52.5 percent have not reported compliance, while 47.5% have done so. However, while 55 percent of merchants within Levels 1, 2 and 3 have met the requirements, compliance drops significantly within the Level 4 merchant community. In fact, only 19 percent of Level 4 merchants said they had reported compliance.

Of the respondents polled who have not achieved compliance, the outlook is varied. Nineteen percent of those surveyed believe it will take more than 18 months to comply, while 26 percent expect to become compliant within 12–18 months. Twenty-four percent anticipate meeting the PCI DSS requirements in 6–12 months, and almost one-third believes compliance will be attained within 6 months.

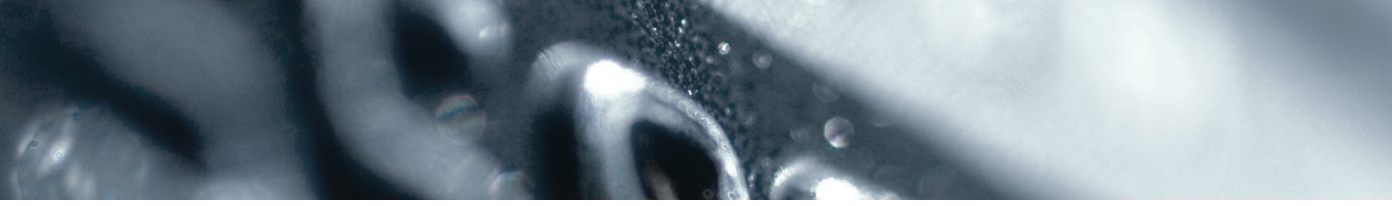
Merchant Levels (as defined by Visa)

- Level 1 More than six million Visa transactions per year. regardless of acceptance channel
- Level 2 One to 6 million Visa transactions per year, regardless of acceptance channel
- Level 3 20,000 to one million Visa e-commerce transactions per year
- Level 4 Fewer than 20,000 Visa e-commerce transactions per year, and all other merchants—regardless of acceptance channel—processing up to 1,000,000 Visa transactions per year

Of the merchants that are already compliant, nearly half said that meeting the PCI DSS requirements took over a year. Five percent said it took over two years, 16 percent said the process took 18–24 months and 27 percent said the timeframe from conducting an initial gap analysis/assessment to submitting the compliance report took approximately 12–18 months. Almost 19 percent said achieving compliance took less than half a year.

Compliance by Merchant Level

	Compliant	Non-compliant
Level 1	55%	45%
Level 2	55%	45%
Level 3	55%	45%
Level 4	19%	81%



RSA also asked merchants the degree to which they believe others within the same industry have progressed toward compliance. The overwhelming majority of merchants surveyed—68 percent—believe businesses within the same industry have made "moderate progress toward achieving PCI compliance." Only ten percent believe companies in their industry have made "significant progress."

Companies in my industry have made …	
> Significant progress	10%
> Moderate progress	68%
> Slight progress	18%
> Little or no progress	5%

Demonstrating Compliance to Banks and Card Brands

RSA also queried merchants regarding their plans for managing the annual PCI audit process. A slight majority of those surveyed (54 percent) said a Qualified Security Assessor would handle the audit. Seventy-five percent of Level 4 merchants plan to manage audits internally, while 64 percent of Level 3 merchants will rely on internal audits. Internal audit rates drop significantly at Level 2, where only 40 percent expect to proceed in such a manner. Only 30 percent of Level 1 merchants will certify audits internally, which requires the audit to be signed by an officer of the company.

Motivations for Meeting the PCI DSS Requirements

RSA's research shows that the majority of merchants approach the PCI DSS as an opportunity to protect their brand and their consumers, rather than as an opportunity to mitigate legal exposure.

Thirty-six percent of merchants said they are motivated to address the PCI standard because of a desire to protect the card data of consumers. Another 25 percent said the motivating factor was protecting the company and/or brand.

One-fourth, however, was motivated because PCI DSS is a requirement. Only ten percent said mitigating the chances of fines or civil litigation were the driving factors behind the PCI initiatives. Results were consistent among both compliant and non-compliant merchants.

Motivation to Comply	Compliant	Non-compliant
> Avoid fines	8%	5%
> Avoid civil litigation	3%	5%
> Protect company/brand	24%	26%
> Protect consumer data	37%	36%
> Meet a requirement	29%	24%

Perceptions of the PCI DSS

RSA's study shows that merchants perceive the PCI DSS requirements as providing a framework for effectively protecting consumer card data. Ninety percent of those surveyed believe the requirements will be either moderately or highly effective, and only 10 percent view the standard as slightly effective or not at all effective.

The PCI requirements will be ...

> Highly effective	34%
> Moderately effective	56%
> Slightly effective	9%
> Not at all effective	1%

Challenges in Meeting the PCI DSS Requirements

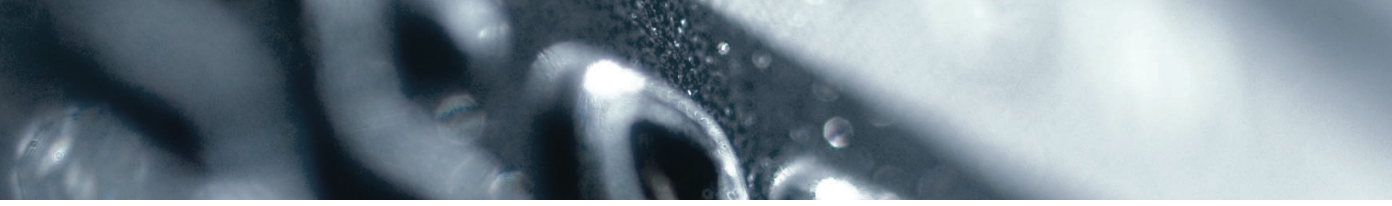
According to RSA's survey, over 60 percent of participants say their company views complying with the PCI DSS as a moderate challenge, and one-third calls the requirements a "very significant challenge." Only about 6 percent believe PCI DSS poses either a minor challenge or no challenge at all.

Merchants also shared feedback regarding the most significant technology challenges they face when addressing PCI. Multiple responses were accepted:

- Tracking and monitoring access to the network and systems with cardholder data: 51%
- Encrypting card data: 48%
- Controlling logical access to systems containing card data: 35%
- Authenticating users accessing systems containing card data: 23%
- Intrusion detection/intrusion prevention: 16%
- Conducting vulnerability scanning: 15%
- Installing and maintaining firewalls: 11%
- Conducting penetration testing: 11%
- Updating and using anti-virus systems: 6%

About the RSA PCI DSS Survey

The RSA PCI DSS survey was conducted between February 26 – March 1, 2007. This Web-based survey polled organizations in the United States and Canada affected by the PCI standard, and individuals from eighty companies participated. For more information on the PCI DSS, visit www.rsa.com/pci.



RSA is your trusted partner

RSA, The Security Division of EMC, is the expert in information-centric security, enabling the protection of information throughout its lifecycle. RSA enables customers to cost-effectively secure critical information assets and online identities wherever they live and at every step of the way, and manage security information and events to ease the burden of compliance.

RSA offers industry-leading solutions in identity assurance & access control, encryption & key management, compliance & security information management and fraud protection. These solutions bring trust to millions of user identities, the transactions that they perform, and the data that is generated. For more information, please visit www.RSA.com and www.EMC.com.

PCIRPT SB 0307

RSA
The Security Division of EMC

RSA Security Inc.
RSA Security Ireland Limited
www.rsa.com