

# Overview and Recommendations for PCI Compliance

Jignesh Patel

President – *Lumenor Consulting Group*

*A Technology and Business Consulting Company*

**Lumenor**  
Consulting Group

# Overview of PCI DSS

- Working together, the major payment card providers have developed a set of data security standards and created a council for enforcing them.
- In June 2005, American Express, DiscoverCard, JCB, MasterCard and Visa founded the PCI Security Council
- PCI council does not enforce the compliance. Enforcement is left to specific credit card companies

# Overview of DSS

- DSS specifications are standards for securing system components: e.g. servers, POS terminal, network and other applications.
- DSS can be divided in 3 broad categories:
  - Collecting and Storing: Secure collection and tamper-proof storage of data
  - Reporting: Being able to prove compliance if audited and present evidence about controls in place
  - Monitoring and alerting: Have systems in place to help administrators constantly monitor access and usage of data.

# Overview of DSS - continued

## CONTROL OBJECTIVES

Build and maintain a secure network

Protect cardholder data

Maintain a vulnerability management program

Implement strong access control measures

Regularly monitor and test networks

Maintain an information security policy

## COMPLIANCE REQUIREMENTS

1. Install and maintain a firewall configuration to protect data
2. Change vendor-supplied defaults for system passwords and other security parameters
3. Protect stored data
4. Encrypt transmission of cardholder magnetic-stripe data and sensitive information across public networks
5. Use and regularly update antivirus software
6. Develop and maintain secure systems and applications
7. Restrict access to data to a need-to-know basis
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data
10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes
12. Maintain a policy that addresses information security

*Lumenor Consulting Group*

# Why PCI?

- PCI is an industry-regulated security standard in most US states
- Minnesota recently implemented the standard into law and several other states have proposed that it become law.
- Credit card companies hold merchants accountable for protecting stored consumer data and securing the network
- Contractual penalties, including fines of up to \$500,000 per incident and revocation of company's right to accept credit cards

# Basic Approach

- Articulate business requirements.
- Develop a risk assessment that helps generate both security policy and control frameworks.
- Design technology architecture, guidelines and control standards, to help form policy management and feedback processes.
- Integrating DSS with corporate security standards ensure the security controls are rigorously enforced

# 12 Steps to PCI Compliance

## CONTROL OBJECTIVES

Build and maintain a secure network

Protect cardholder data

Maintain a vulnerability management program

Implement strong access control measures

Regularly monitor and test networks

Maintain an information security policy

## COMPLIANCE REQUIREMENTS

1. Install and maintain a firewall configuration to protect data
2. Change vendor-supplied defaults for system passwords and other security parameters
3. Protect stored data
4. Encrypt transmission of cardholder magnetic-stripe data and sensitive information across public networks
5. Use and regularly update antivirus software
6. Develop and maintain secure systems and applications
7. Restrict access to data to a need-to-know basis
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data
10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes
12. Maintain a policy that addresses information security

Five23 Group

# Follow up

Any Questions?

Jignesh Patel, President

(404) 509-3055

[jpatel@523group.com](mailto:jpatel@523group.com)

Bridgette Karra, CEO

(404) 918-9078

[bkarra@523group.com](mailto:bkarra@523group.com)

**Lumenor**  
Consulting Group