

# PCI "Straight Talk" 2

**Diana Kelley and Ed Moyle**

---

# Agenda

- **Understanding the Requirements**
- **Requirements 1 through 6**
- **Wrap Up**

## Compliance: Improve Your Processes, Leverage Technologies and Reduce Costs

---

# Agenda

## ● Understanding the Requirements

- Approaching the Requirements
- For More Information

## ● Requirements 1 through 6

## ● Wrap Up

# Understanding the Requirements

- **The requirements are simple, but comprehensive**  
("a minute to learn, a lifetime to master")
- **Use multiple sources to understand each requirement**
  - The PCI Standard documentation
  - Self-assessment questionnaire
  - Audit procedures
  - *Remember that 1.2 changes the lineup*
- **Remember that the QSA must assess you to the audit document (so it's like an exam you can look at ahead of time)**

## Information Sources

- **PCI Data Security Standard\***
- **PCI Self-Assessment Documentation\***
- **PCI Audit Procedures\***
- **Ask Your QSA**
- **PCI Blogs/Forums (e.g. pcianswers.com)**

# The PCI Requirements "at a Glance"

**Requirement 1: Install and maintain a firewall configuration to protect cardholder data**

**Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters**

**Requirement 3: Protect stored cardholder data**

**Requirement 4: Encrypt transmission of cardholder data across open, public networks**

**Requirement 5: Use and regularly update anti-virus software**

**Requirement 6: Develop and maintain secure systems and applications**

Requirement 7: Restrict access to cardholder data by business need-to-know

Requirement 8: Assign a unique ID to each person with computer access

Requirement 9: Restrict physical access to cardholder data

Requirement 10: Track and monitor all access to network resources and cardholder data

Requirement 11: Regularly test security systems and processes

Requirement 12: Maintain a policy that addresses information security

# Agenda

- Understanding the Requirements
- **Requirements 1 through 6**
- Wrap Up

## Compliance: Improve Your Processes, Leverage Technologies and Reduce Costs

### Requirement 1: Firewalls

“Install and maintain a firewall configuration to protect cardholder data”

#### ● What it means

- “Stateful inspection” devices separating untrusted networks (e.g. the Internet) from the cardholder environment
- Documented procedures supporting how the firewalls are deployed and maintained

#### ● Questions

- Do we need a firewall for every store?
- How about a router with ... ?

#### ● Gotchas

- Documentation



# Impact and Quick Hit: Firewalls

## 1.2 Impact

- Relaxed ruleset review (was quarterly, now biannually)
- Clarified applicability to routers as well as firewalls

## Quick Hits

- Need current and accurate network diagram
  - Showing the cardholder environment in relation to the Internet
- A list of services allowed in and out of the CDE, including:
  - Business justification for services
- Documented configurations
- Review of rules (at least twice annually)

## Compliance: Improve Your Processes, Leverage Technologies and Reduce Costs

### Requirement 2: Defaults

**“Do not use vendor-supplied defaults for system passwords and other security parameters”**

#### ● What it means

- Document a secure configuration, including removing of vendor-enabled passwords, and unnecessary services
- Enable security features like encryption for administrative connections

#### ● Questions

- One function per server? What about virtualization?

#### ● Gotchas

- Legacy infrastructure and applications
- Telnet, r-services, ftp
- HTTP management interfaces

**This includes all systems. Most firms have trouble with the legacy environment.**



# Impact and Quick Hits: Defaults

## 1.2 Impact

- **Removed requirement to disable SSID broadcast**
- **Clarified hosting provider requirements**

## Quick Hits

- **Employ one function per server (i.e., the billing server is different from the domain controller)**
- **Remove unneeded services**
- **Remove telnet, ftp, rsh, rexec, rlogin - even if you're not using them**

## Compliance: Improve Your Processes, Leverage Technologies and Reduce Costs

# Requirement 3: Protect Data

**“Protect stored cardholder data”**

## ● What it means

- Use encryption (or don't store) cardholder data
- Don't store (even with encryption) sensitive authentication data (like the mag stripe)

## ● Questions

- *Never* store the CVV? We heard we have to in some cases.
- Does 1.2 mean we don't have to encrypt backup tapes now?

## ● Gotchas

- “One click” means you need to keep the PAN (therefore encrypt it)
- If you encrypt, you need to manage the keys

# Impact and Quick Hits: Protect Data

## 1.2 Impact

- Removed specific requirement for media (i.e. backup) encryption

## Quick Hits

- Have a policy for data retention/disposal
- Mask the PAN on screen
- Look at existing apps to see if there are plaintext PANs
- Don't store auth data post authorization. (No matter who tells you to. Really.)



Once they start looking for it, most firms find they're already storing the PAN unencrypted – even if they thought they weren't.

## Compliance: Improve Your Processes, Leverage Technologies and Reduce Costs

# Requirement 4: Encrypt Transmissions

“Encrypt transmission of cardholder data across open, public networks”

## ● What it means

- Encrypt data when it travels over the Internet (or other public network)
- Encrypt data on wireless

## ● Questions

- What about WEP?
- What about our POS?

## ● Gotchas

- WEP is going away, look to SSL/TLS/IPSEC
- Web services

## Compliance: Improve Your Processes, Leverage Technologies and Reduce Costs

# Impact and Quick Hits: Encrypt Transmissions

## 1.2 Impact

### ● NO MORE WEP

- No new WEP after 3/31/09, all WEP phased out by 6/30/10

## Quick Hits

- Have a policy stating not to email unencrypted PAN
- Use an email encryption package if you email PANs
- Use TLS/VPN/IPSEC over open networks (don't forget retail locations...)

## Compliance: Improve Your Processes, Leverage Technologies and Reduce Costs

### Requirement 5: Anti-Virus

**“Use and regularly update anti-virus software”**

#### ● What it means

- You employ software for malware scanning

#### ● Questions

- What about UNIX? Mainframes? The old Amiga in the closet?
- What about HIPS?
- What about POS systems?

#### ● Gotchas

- Don't forget about spyware



**Make sure your AV supports anti-spyware (sometimes it costs extra)**

# Impact and Quick Hits: Anti-Virus

## 1.2 Impact

- Log requirements for AV changed to mirror other log requirements
- Expanded scope to include all OSs
  - Intent appears to be universal AV
  - Except where technology isn't available

## Quick Hits

- Current signatures
- Log generation and alerting features enabled
- An AV package that can detect spyware, adware, rootkits, and "greyware" (like hacking tools)
- AV for "non-core" platforms

## Compliance: Improve Your Processes, Leverage Technologies and Reduce Costs

# Requirement 6: Systems & Applications

**“Develop and maintain secure systems and applications”**

## ● What it means

- You use secure coding techniques (and test applications for security)
- You have processes to make sure that systems are secure against vulnerabilities

## ● Questions

- How soon do we have to patch?
- What's the PA-DSS?
- Code scanning for custom code? Do they mean manual review or a product? What code do they mean?

## ● Gotchas

- External web-apps require external review *or* app firewall

## Compliance: Improve Your Processes, Leverage Technologies and Reduce Costs

# Impact and Quick Hits: Systems and Applications

## 1.2 Impact

- Changes to 6.6 (now “Web Application Firewall”)
- You can now prioritize patches (high: one month; low: 3 months)
- Code review/testing process now requires fixing issues prior to release
- Specifically includes automated testing tools for code review

## Quick Hits

- Have change control procedures
- Have a process for identifying new vulnerabilities
- Test production changes
- Have a documented software development lifecycle
- Perform code reviews of custom code
- Have separate personnel and environments for production and test

**Compliance: Improve Your Processes, Leverage Technologies and Reduce Costs**

---

## **Requirements: To Be Continued**

- **Join us in the next session to hear the “rest of the story” on specific PCI DSS requirements**

# Agenda

- Understanding the Requirements
- Requirements 1 through 6
- **Wrap Up**

## Wrap Up: Understanding the Requirements

- **Try to understand your weak areas before the audit starts**
  - Self assessment documentation
  - Auditing guidelines
- **Documenting the work you do to address requirements is never wasted**

## Questions? Comments?

- **Questions about specific requirements?**