AFP ENTERPRISE PAYMENTS SERIES

A Complimentary Virtual Event for Payments Professionals

The Importance of PCI Compliance for Your Organization

Protecting Payment Card Data and Building Customer Trust

George Uko Senior Credit Manager
Kubota

Today's Agenda

- What PCI DSS is and why it exists
- Who must comply and when it applies
- Key PCI DSS requirements (v4.0 – high level)
- Impacts of non-compliance for businesses and customers
- How organizations become and stay PCI compliant
- Where to go for help, training, and reporting concerns

What is PCI Compliance?

- PCI = Payment Card Industry Data Security Standard (PCI DSS)
- Global security standard for any organization that stores, processes, or transmits payment card data
- Created by the major card brands (Visa, Mastercard, American Express, Discover, JCB) through the PCI Security Standards Council
- Goal: reduce payment card fraud by protecting cardholder data end to end

Why Does PCI Compliance Matter?

- Protects customers from card fraud and identity theft
- Helps prevent costly data breaches and business disruption
- Required by the card brands and acquiring banks as a condition of accepting card payments
- Demonstrates security maturity and builds trust with customers, partners, and regulators

What Happens If You Don’t Follow PCI Guidelines?

- Increased risk of breaches and card data theft
- Fines from card brands and banks (often $5,000–$100,000 per month until compliant)
- Costs of incident response, investigations, and card re-issuance
- Potential lawsuits, regulatory scrutiny, and brand damage

Real-World Breach Example (High Level)

- Large retailer’s point-of-sale network was compromised by malware
- Attackers stole tens of millions of card numbers during the holiday season
- Company paid hundreds of millions in settlements, technology upgrades, and legal costs
- Breach became a case study in why continuous security – not just one-time compliance – is critical

Who Is Responsible for PCI Compliance?

- Ultimately: the organization that accepts or handles card payments
- Business leadership and owners: accountable for funding and prioritizing PCI efforts
- IT and security teams: implement technical controls and monitoring
- Operations and frontline staff: follow secure processes in day-to-day work
- Third-party service providers: share responsibility where they store, process, or transmit card data

Are All Credit Cards Part of PCI Compliance?

- PCI DSS applies to payment cards from the major global card brands (Visa, Mastercard, AmEx, Discover, JCB, etc.)
- If a card displays one of these brands' logos, PCI DSS requirements apply somewhere in the payment flow
- Rules cover both credit and debit cards, including chip, mag-stripe, contactless, and e-commerce transactions
- Local store cards or closed-loop gift cards may have different requirements, but many follow PCI-style controls

PCI DSS: The 12 Core Requirements (v4.0 Overview)

- 1. Install and maintain network security controls (e.g., firewalls)
- 2. Apply secure configurations to all system components
- 3. Protect stored account/cardholder data
- 4. Protect cardholder data in transit over open, public networks
- 5. Protect systems and networks from malware and keep anti-malware current
- 6. Develop and maintain secure systems and software

PCI DSS: The 12 Core Requirements (v4.0 Overview, cont.)

- 7. Restrict access to systems and cardholder data by business need-to-know
- 8. Identify and authenticate users accessing systems (strong authentication)
- 9. Restrict physical access to cardholder data
- 10. Log and monitor all access to systems and cardholder data
- 11. Test security of systems and networks regularly (e.g., scans, penetration tests)
- 12. Support information security with policies, governance, and ongoing programs

Steps to Become PCI Compliant

- 1. Determine your PCI scope: where card data is stored, processed, or transmitted
- 2. Identify your merchant/service provider level and validation requirements
- 3. Gap assessment: compare current controls to the 12 PCI DSS requirements
- 4. Remediate gaps (technology, processes, training, vendor changes)
- 5. Validate compliance (Self-Assessment Questionnaire or QSA-led assessment)
- 6. Implement continuous monitoring and annual re-validation

Business Implications of Non-Compliance

- Direct financial penalties from banks and card brands
- Higher transaction fees or loss of ability to process card payments
- Incident response, forensics, legal, and notification costs after a breach
- Increased cyber insurance premiums or reduced coverage
- Loss of customer trust, reduced sales, and long-term brand damage

Is PCI DSS Just for the U.S.?

- No – PCI DSS is a global standard used in over 180 countries
- Card brands and acquiring banks require PCI compliance worldwide
- Many regional regulations (e.g., privacy and cybersecurity laws) reference or align with PCI principles
- Multinational organizations often harmonize PCI with laws like GDPR, state privacy laws, and other security frameworks

- Define and update PCI DSS and related standards via the PCI Security Standards Council
- Provide programs and tools (e.g., merchant guidelines, self-assessment questionnaires, validation programs)
- Encourage secure technologies like EMV chips, tokenization, and point-to-point encryption
- Operate fraud monitoring, alerts, and dispute processes to detect and respond to suspicious activity

PCI Compliance Levels

- Merchant and service provider levels are based mainly on annual transaction volume
- Level 1: highest volume (often 6M+ transactions per year) – requires annual QSA assessment
- Levels 2–4: lower volumes – may validate with Self-Assessment Questionnaires, plus scans
- Regardless of level, all must meet the same 12 PCI DSS requirements

Customer Impacts When Standards Aren’t Followed

- Fraudulent charges and potential account takeover
- Time spent cancelling cards, updating autopay, and monitoring statements
- Possible identity theft and long-term credit impacts if data is reused elsewhere
- Loss of trust in the brand and reluctance to shop or transact again

How to Report PCI Concerns

- If you suspect card data isn't handled securely at a business:
- • Report concerns to the business's management or security/privacy contact
- • Contact your card issuer (bank) if you see suspicious charges
- • Card brands provide channels to report suspected payment security issues
- If you work for the business: follow internal escalation and incident-reporting processes immediately

PCI Security Standards Council (PCI SSC)

- Independent body founded by major card brands to manage PCI standards
- Publishes PCI DSS and related standards (e.g., P2PE, PA-DSS replacement frameworks)
- Maintains lists of validated payment applications, devices, and service providers
- Provides guidance documents, FAQs, and training for the global payments community

Where to Get PCI Compliance Training

- PCI Security Standards Council: official awareness and professional training (e.g., PCIP, ISA)
- Card brands and acquirers: merchant-focused webinars, guides, and security bulletins
- Specialized security training providers and Qualified Security Assessors (QSAs)
- Internal security teams: role-based training tailored to your organization’s environment

Key Takeaways

- PCI DSS is a global standard focused on protecting payment card data and reducing fraud
- Compliance is mandatory for organizations that store, process, or transmit card data
- The 12 requirements work together as a layered, risk-based security program
- Non-compliance can be extremely costly for businesses and painful for customers
- Successful PCI programs treat it as ongoing security, not just a yearly checkbox