BANKCARD
COMPLIANCE GROUP

Bankcard Compliance Group

PIN Security & Key Management

TR-39

PCI PIN TRANSACTION SECURITY

2014

peter@bankcardcompliance.com 877-378-5344

BANKCARD
COMPLIANCE GROUP

What is a TR-39/PCI PTS?

- ANSI Technical Release – 39
  - Originally developed in late 1990’s, fka TG-3
- PCI PIN Transaction Security (PTS)
  - Developed September 2011, fka VISA PIN Self Audit
- Secure administration and distribution of cryptographic keys
- Secure PIN Transmission and Processing
- Method of Validation of compliance

What is a TR-39/PCI PTS?

- Policies and practices dealing with keys, keying material, hardware, and software
  - Technical
  - Administrative
  - Physical
- Dual Control / Split Knowledge of Keys

Who must complete?

- Depends:
  - FFIEC defines PIN as PII – requires documented and implemented procedures to protect
  - All VISA and MasterCard Branded Debit card acquirers/processors must meet the PCI PTS controls by 01/01/2016
  - Your PIN Debit Network requirements – see charts
    - Most processing acquirers must submit biennial report to networks
    - Most Non processing acquirers must complete biennial report
      - Must meet required controls
      - Be able to demonstrate compliance via periodic "self audit" on file
  - Entities which acquire and or process PIN's should complete a PIN Security Review

BANKCARD COMPLIANCE GROUP

Who must complete?

- Depends: Per STAR Compliance
  - "It is important for STAR Members to understand that removing the requirement to submit the Review to STAR in no way changes the obligations and liabilities of a STAR Member to comply with STAR security requirements… including PIN and Key Management……if a STAR Member were to fail to comply with such requirements and a compromise were to occur that could have been prevented if that STAR Member had been compliant, STAR will hold that STAR Member liable for the resultant fraud losses incurred by each other participant in the STAR Network. Each STAR Member should, therefore, continue to conduct a periodic Review of its environment to ensure that it and any third party acting on its behalf is compliant with STAR security requirements."

Who must complete?

Network	PIN Transactions Performed	Submit TR-39 to Network	Complete TR-39 and keep on file	Complete PCI PTS 01/2016
STAR NYCE PULSE	Acquire and Process PINS	🟥		
STAR NYCE PULSE	Acquire PINS		🟥	
VISA MasterCard	Acquire and Process PINS			🟥
CO-OP	Acquire OR Process PINS	🟥		
ACCEL	Acquire OR Process PINS		🟥	

BANKCARD
COMPLIANCE GROUP

Why do we do this?

- Risk = Probability X Impact
  - E.g.;1,000 compromised accounts x $100
- Low level fraud
  - Shoulder surfing, skimming, card jamming
- Mid level fraud
  - Fake ATM – PIN & PAN capture
- High level fraud
  - Encryption key compromise

Benefits?

- Comply with FFIEC or NCUA CFR 748, and your network requirements
- Reduce risk of debit compromise
  - Financial loss to customer
  - Financial loss to Institution
  - Reputational loss to Institution
  - Liability to 3rd party network members

Who performs review?

- Qualified Internal or External Auditors
- Most networks require processing entities to use a certified TR-39 auditor
- Non-processing entities must attest that the person completing the review is:
  - Independent from operations being reviewed
  - Knowledgeable of encryption controls
  - Knowledgeable of audit techniques

BANKCARD
COMPLIANCE GROUP

How are they done?

- Onsite Field Audit:
  - Device Inventory/Inspection
  - Policy & Procedure Review and Update (as necessary)
  - PIN Flow Diagram
  - Key Methodologies
  - Key Establishment
  - Key Lengths
  - PIN Block Formats
  - Working Paper Forms
  - Findings / Action Plan

How are they done?

- Offsite TR-39/PCI PTS Report Completion
- Review of Deliverable w/ Management
- Sign off by Officer
- Auditor Attestation and 3rd party Submission of TR-39 (if required)
  - Network
  - Approved 3rd party requesters (clients)

BANKCARD
COMPLIANCE GROUP

How long does it take?

- Usually 1 Day Site visit -
  - Locations
  - Cryptographic keys and key components maintained
  - Key life cycle functions
  - Hardware
  - Software
  - Policy/Procedures

About Us

- Bankcard Compliance Group (BCG)
- Founded in 2003
- Certified by NYCE, STAR, Pulse
- Focused on PIN Debit Security

BANKCARD
COMPLIANCE GROUP

About Us

- Principal Auditor – Peter Trombley, MBA, CTGA
  - Performing PIN Security Audits since 2000
    - STAR, Pulse, NYCE TR-39
    - PCI PTS (VISA, MasterCard)
    - STAR Online Debit
  - Former Consulting Manager Accenture
  - Experienced Information Security Consultant
  - Director TCT Federal Credit Union

Value to Clients

- Knowledgeable
- Experienced
- Certified (CTGA)
- Independent
- Focused
- Affordable (fixed fee)
- Two year support included w/ engagement

BANKCARD
COMPLIANCE GROUP

Selected References

- Provided with Confidential Proposal

Questions