



Visa Inc. – Data Security Update

**Jackie Jason
JJASON@VISA.COM**



Trustwave[®]

Information Security & Compliance



Elements of a Successful Level 4 PCI Program

Presented by:
James Taylor, VP of Alliances

Agenda

- Brief Trustwave overview
- Recent compromise Statistics
- Why it's important
- Current state of Level 4 compliance
- The elements of a successful Level 4 program

The leader in PCI DSS compliance

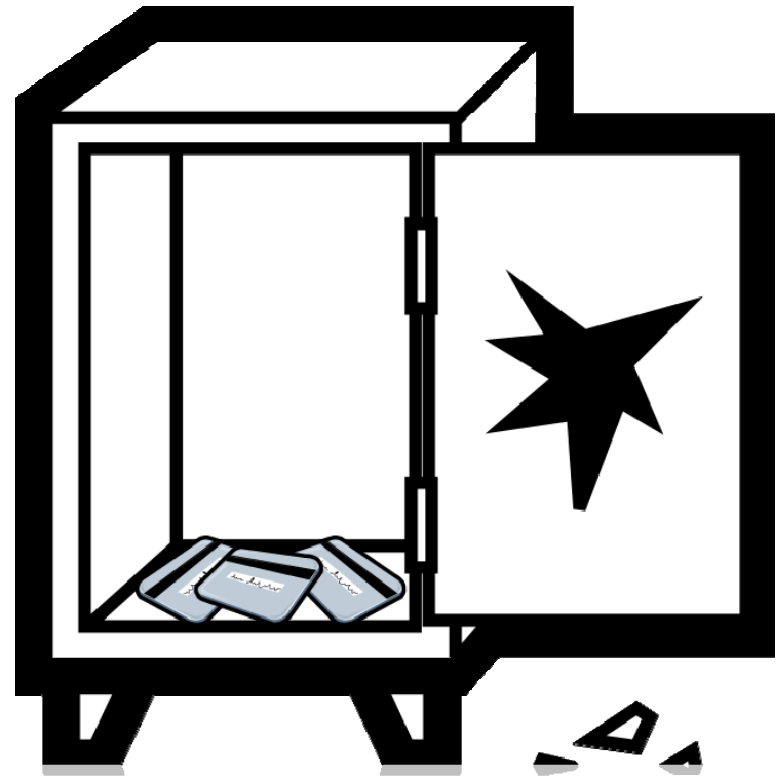
Since the inception of their data security programs almost a decade ago, Trustwave has worked with the card brands to protect cardholder data.

- **Qualified Security Assessor (QSA)**
- **Authorized Scanning Vendor (ASV)**
- **Qualified Incident Response Vendor (QIRV)**
- **Qualified Payment Application Security Company (QPASC)**

Card Compromise Recent History

- Over 90% of compromises are Level 4 merchants
- 49% are restaurants
- 68% involve card present merchants
- 66% are an exploit of a non-compliant payment application
- 91% of compromises occurred through an “always on” Internet connection

** Compromise data summarized from over 500 investigations*



The Cost of Non-compliance

Non-compliant, compromised business could expect the following:

- Financial loss
- Data loss
- Charge-backs for fraudulent transactions
- Operations disruption
- Sensitive info disclosure
- Denial of service to customers
- Individual executives held liable
- Possibility of business closure



Current State of Level 4 PCI Compliance

- Level 4 merchants don't understand what cardholder data they store/process/transmit
- They don't know that they are at risk of a compromise
- Level 4 merchant response to PCI marketing campaigns is limited due to lack of awareness
- They get compromised: Over 90% of Trustwave forensic investigations involve Level 4 Merchants



Level 4 Programs: The Goal

- Should sync with card brands' requirements for acquirers:
 - Identify and prioritize merchants based on their exposure to payment card compromise
 - Educate Level 4 merchants about PCI DSS compliance
 - Execute a compliance strategy that:
 - Eliminates the storage of prohibited data
 - Protects stored data
 - Secures the merchant environment via compliance with the PCI DSS
 - Identifies the payment applications used
 - Track and report on the program's progress each month



Step 1: Determine Type of Program

- Determine the type of program you want to implement
 - Establish your objective:
 - Compliance and data security?
 - Risk mitigation while covering expenses?
 - Identifying high-risk merchants?
 - Will it be mandatory or optional?
 - Providing value-added services to merchants?
- The type of program will help determine how it's enforced and communicated

Step 2: Segment Your Merchant Portfolio

- Refine strategy by categorizing merchants by processing type
 - Dial-up POS Merchants
 - eCommerce
 - Internet-connected POS Merchants
- Determine go-to-market strategy
 - Existing merchant base
 - Staged Rollout, Added Value
 - Newly boarded merchants
 - Sell up front, part of welcome kit



Step 3: Determine Communication Strategy

- Clear, concise program intent
- Avoid overwhelming merchants up front
- Program needs to drive awareness—internal and external
 - Pre-launch internal education (acquirer and assessor)
 - Launch phase communication elements
 - Communication channels and vehicles
 - Key message development
 - Timing and frequency
 - Informational web-site
 - Adoption phase communication activities
 - On-going compliance status communications
 - Non-compliance fees
 - Educational webinars and compliance help desk services

Step 4: Offer Value

- Don't treat PCI like a "stick"
 - This is a partnership between you and the merchant, geared towards keeping the merchant in business
- Consider incentives to drive participation
 - e.g., Breach Insurance, SSL Certificates, Security Awareness, Policies and procedures, etc.
- Provide tools to help merchants through the process
 - Awareness Training
 - Security Policy Help
 - Automated tools to help merchants with more complex requirements
- Use partners to provide a path to solutions to compliance problems, or simply combine PCI with things the merchant wants or needs
 - Firewalls, Log Monitoring, etc.

Step 5: Choose a Trusted Partner

- Do your homework and consider the following factors:
 - Product offerings
 - Do they have the right technology?
 - Is the technology easy to use?
 - Do they allow you to track the success of the program?
 - Experience (particularly Level 4 experience)
 - Established history and good standing within the PCI community
 - Support
 - How is merchant support handled?
 - Who owns merchant relationship?
 - Communication and marketing capabilities

Step 6: Offer Technology and Merchant Tools

- Program needs to provide value-added services to merchants while simplifying the compliance process
 - Tools to identify prohibited data
 - “Risk-Profiling” services
 - Intelligent SAQs
 - Vulnerability scanning services
 - Web-based training
 - Webinars and education seminars
 - Security policies and procedures
 - Certification--web site seals and printable compliance certificates
 - Merchant support—real time guidance



Step 7: Build a Solid On-Going Support Structure

- Program should be flexible and sustainable
- Measure the progress of the program regularly
- Consider taking 'first-call' support
- Build operations manual that governs assessor/acquirer relationship
- Develop ongoing education program—internal and external
- Embed PCI DSS language in your merchant agreements
- Bundle PCI DSS solutions with your existing products and services
- Survey your merchant population
- Have regular milestone meetings with assessor

Final Thoughts

- Level 4 PCI Programs can be rolled out successfully
- Level 4 PCI Programs produce demonstrable improvements in compromise risk factors
- Think beyond “SAQ + Scan”
- Tailor the program to your portfolio
- Consider adding value for your merchants
- Remember that there are two partnerships:
 1. You and your merchants
 2. You and your compliance partner
 - Understands your business model & goals



Trustwave[®]

Information Security & Compliance



Questions



Secure POS Vendor Alliance

Jeff Wakefield

Chairman, SPVA Threat Analysis and Intelligence Working Group

State of the Industry – All pieces have to fit

Application Standards

- OS security
- R&D process
- Application life cycle management



Site Standards

- Compliance too costly for small merchants
- Compliance to standard is a snapshot in time.



Hardware Standards

- Addresses only PIN Security
- Ccard-holder information
- R&D, supply chain & maintenance functions
- Inconsistent enforcement



Network Standards

- Dial-up lines
- Legacy networks (x.25, SDLC, etc.)



SPVA Vision

- **The SPVA will foster compliance** with widely accepted global payment security standards and develop new industry guidelines to further advance security of consumer and payment card information
- **The SPVA will increase awareness of security issues**, encourage adoption of best practices and eliminate inconsistencies between standards governing disparate components and participants in the payment environment
- **The SPVA offers its members the opportunity to increase their value to customers** through the application of increased security that protects cardholder information and defends merchants, acquirers and issuers against security breaches and associated liabilities
- **The SPVA offers merchants & acquirers a consistent, high level of security** when they choose to deploy “SPVA-Approved” solutions

SPVA Mission

- The SPVA provides a forum for payment industry participants to collectively address security challenges at the point of sale by bringing forth the knowledge and skills of the experts in the payment systems environment
- The SPVA will pursue aggressive, yet achievable goals to:
 - Standardize interpretation of existing industry rules and regulations among the secure POS vendor community
 - Move beyond minimum standards compliance, to ensure security, durability and interoperability of all payment system elements
 - Define end-to-end management standards and best practices for payment systems
 - » *Secure Terminal downloads*
 - » *Remote Diagnostics and Tamper Detection*
 - » *Remote Key Injection*
 - » *End to End Encryption*
 - » *Digital Certificates Application Signing*
 - » *Asset Tracking and Management*
 - » *Secure POS Interfaces*
 - Continuously review security exposures of existing payment systems currently in the market to identify and mitigate potential threats

SPVA Governance



- Maintain an open and inclusive membership
- Facilitate “Technical Working Groups”
 - ↳ Entire membership contributes to new guidelines or standards
- Publish best practice and auditable security guidelines
 - ↳ Once ratified, Secure POS Vendors can seek “SPVA-Approval”
- Consolidate Secure POS Vendor input to other standard bodies
- Maintain a Forum to increase awareness of security threats

SPVA “Approved” Solutions Program

The SPVA approval program will be targeted at Secure POS system vendors wishing to display the SPVA Logo on their solutions

- Merchants, Acquirers and Processors choosing SPVA-approved solutions can be assured of the highest level of security currently available
- Simplifies compliance with industry security mandates such as PCI and the rules of individual card brands, reducing risk and ensuring control of payment solutions over the life of the product
- SPVA approved solutions must, at minimum, initially comply with major card brand security standards
- SPVA will also seek to establish baseline compliance requirements in areas where card brand security interpretations differ

Initial Technical Working Groups

- ***Standardized Implementation of Existing Security Standards.***

Goal: Release a common interpretation of existing security standards and publish collective Implementation guidelines

- ***Security of Payment Device Lifecycle.***

Goal: - Develop end to end lifecycle security guidelines

- Ensure security during all the complete POS terminal lifecycle - from manufacture through deployment, field maintenance and application software upgrades and eventual end-of-life and removal and secure destruction.
- Manage digitally-signed applications
- Provide mechanisms to track & manage devices, to ensure security compliance & respond to new threats
- Create development, manufacturing/supply chain, deployment and repair security guidelines and audit procedures

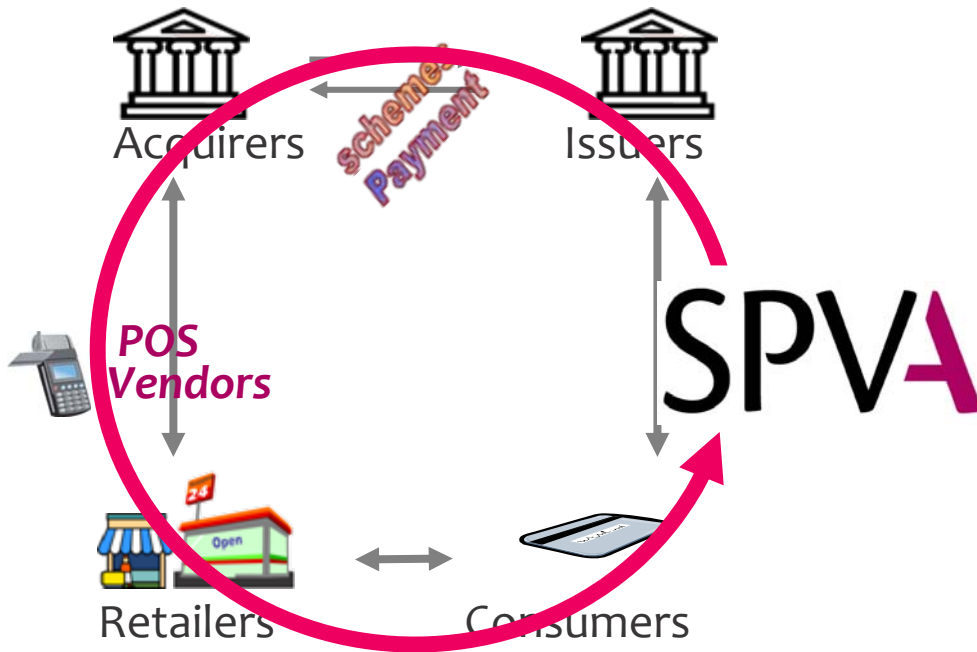
- ***Security Threat Analysis and Intelligence.***

Goal: - Provide education and resources to educate members and payment industry stakeholders regarding the current threats and ways to mitigate them.

- ***End-to-End Security Transactions .***

Goal: - create industry encryption framework of cardholder data utilizing hardware level security module capabilities of secure payments systems to adequately secure cardholder information before it enters the application environment.

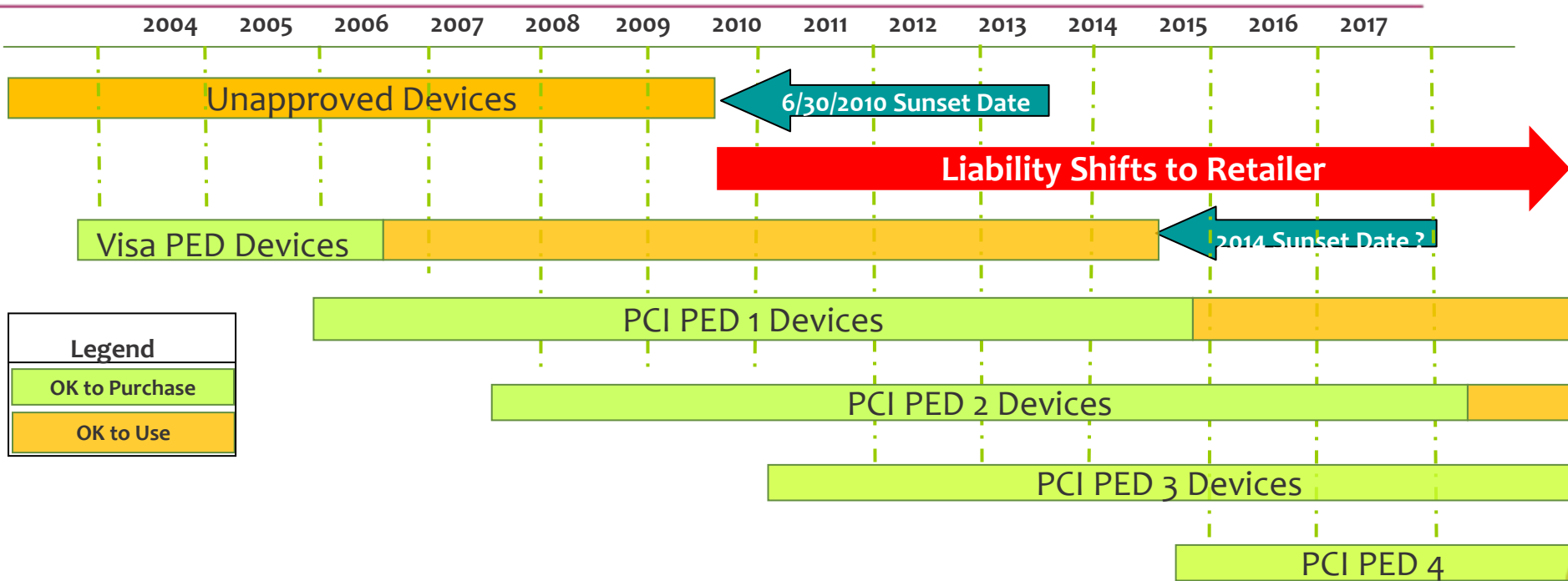
Benefits to each payment industry stakeholders



Enhance security along the payment value chain is absolutely mandatory to protect all stakeholder interests,

while in the meantime, security must also be synonymous with convenience, cost control and the ability to be easily deployed and maintained.

PCI PED Terminal Timetable



Legend
OK to Purchase
OK to Use

Customers: Unapproved Devices must be removed by 7/1/10

Opportunity: Develop a plan to insure your merchants upgrade to PCI PED approved devices by 7/1/10

PCI Compliance Myths

- PCI Does not apply to me
- PCI in a Box is possible
- There is a silver bullet PCI Solution
- PCI Compliance means PCI Security
- PCI Compliance is an event

Press Q & A



delivering comprehensive
payment security experience

www.spva.org