THE IMPACT P2PE SOLUTIONS HAVE ON BUSINESS OPERATIONS

May 22, 2019

payway®

AGENDA

- PCI Compliance – An Overview
- Methods of Terminal Encryption
- Case Study
- Recap

329

33

90

PCi Security Standards Council®

INTRODUCTION

- Founded in 2006 by American Express, Discover, JCB International, MasterCard and Visa Inc.
- Two priorities:
  - Help merchants and financial institutions understand and implement standards for protecting cardholder data.
  - Help vendors understand and implement standards for creating secure payment solutions.

payway®

PCI COMPLIANCE – AN OVERVIEW

The PCI Data Security Standard (PCI DSS) provides a baseline of technical and operational requirements designed to protect account data.

P2PE – SECURING CARD DATA

P2PE is a PCI DSS approved methodology for securing credit card data by encrypting it from the time a card is swiped until it reaches the payment processor where it is decrypted.

payway®

TWO TYPES OF TERMINAL ENCRYPTION

Unlisted E2EE solutions

PCI-listed P2PE solutions

TERMINAL ENCRYPTION REQUIREMENTS

Three high-level requirements that every P2PE/E2EE solution must offer:

1. The card data must be encrypted using strong cryptography
2. The encryption must be performed within a secure hardware device
3. It must not be feasible to decrypt the data within the merchant environment

payway®

END-TO-END ENCRYPTION (E2EE)

BENEFITS

- Encrypts within the point-of-interaction (POI) terminal
- Decrypts outside the merchant environment

DOWNSIDE

- No way to know if account data is properly protected
- Audit of Cardholder Data Environment (CDE) encompasses every component that comes in contact with cardholder data (networks, hardware, POI terminal, etc.)
- Must take PCI Self Assessment Questionnaire D

329 Number of questions in SAQ D

33

90

POINT-TO-POINT ENCRYPTION (P2PE)

BENEFITS

- Encrypts within the POI terminal
- Decrypts outside the merchant environment
- Audit of CDE reduced to POI terminal, network
- Eligible to take PCI Self Assessment Questionnai P2PE

payway®

329 Number of questions in SAQ D

33 Number of questions in SAQ P2PE

90

PCI DSS requires significant security controls around in-scope networks and systems

- Hardening
- Patching
- Logging
- Quarterly internal vulnerability scanning
- Quarterly external vulnerability scanning
- Annual internal penetration testing
- Annual external penetration testing

payway®

USE CASE: MOTO ENVIRONMENT USING E2EE

CARDHOLDER DATA

- Received by mail or telephone requiring manual entry
- All customer data including card number entered into keyboard
- Stored on an internally deployed payment system or entered into a third-party virtual terminal

CARDHOLDER DATA ENVIRONMENT

- Workstations
- All networks
- Non-segmented Internal services including employee email, file sharing services

PCI DSS AUDIT SCOPE

- Entire Merchant Network

USE CASE: MOTO ENVIRONMENT USING P2PE

CARDHOLDER DATA

- Received by mail or telephone requiring manual entry
- Customer data entered into keyboard
- Card information keyed into POI device

CARDHOLDER DATA ENVIRONMENT

- POI device
- Select networks

PCI DSS AUDIT SCOPE

- Select instances within Merchant Network

329 Number of questions in SAQ D

33 Number of questions in SAQ P2PE

90 Percent reduction in scope of audit

WHY YOU SHOULD USE A CERTIFIED P2PE SOLUTION

- P2PE is one of the best methods a merchant can use to protect their customers, themselves and prevent a credit card breach
- 90% reduction in audit scope reducing impact to business and operational costs

payway®

QUESTIONS?

CONTACT

David Fabrizio
Principal
Payway, Inc.
dfabrizio@paywaycomplete.com
978.880.7462

payway

Impact of PCI P2PE on PCI DSS Compliance & Scope Reduction

Date: May 10, 2019

Prepared by:
Barry Johnson
CISSP, CISA, QSA, PA-QSA, QSA (P2PE), CHPSE
Dara Security
President/CEO