Emerging Payment and Payment Card Trends

Payment Card Industry (PCI)

Technical and operational requirements set by the PCI Security Standards Council (PCI SSC) to protect cardholder data.

Applies to all entities that store, process, and/or transmit cardholder data. *If you accept or process payment cards, PCI Data Security Standard (DSS) applies to you.*

The PCI SSC is responsible for managing the security standards, enforced by the card brands: American Express, Discover Financial Services, JCB, MasterCard, and Visa.

PCI DSS is a continuous process, entities are required to report on their PCI DSS compliance on an annual basis.

Failure to comply may lead to fines and / or your ability to process credit cards.

Knowing Your Merchant Level and Reporting Responsibilities

Level 1

- Processing over 6 million credit card transactions per year
- Requires annual onsite
- Assessment and quarterly approved scanning vendors (ASV) scan

Level 2

- Processing between 1 million and 6 million credit card transactions per year
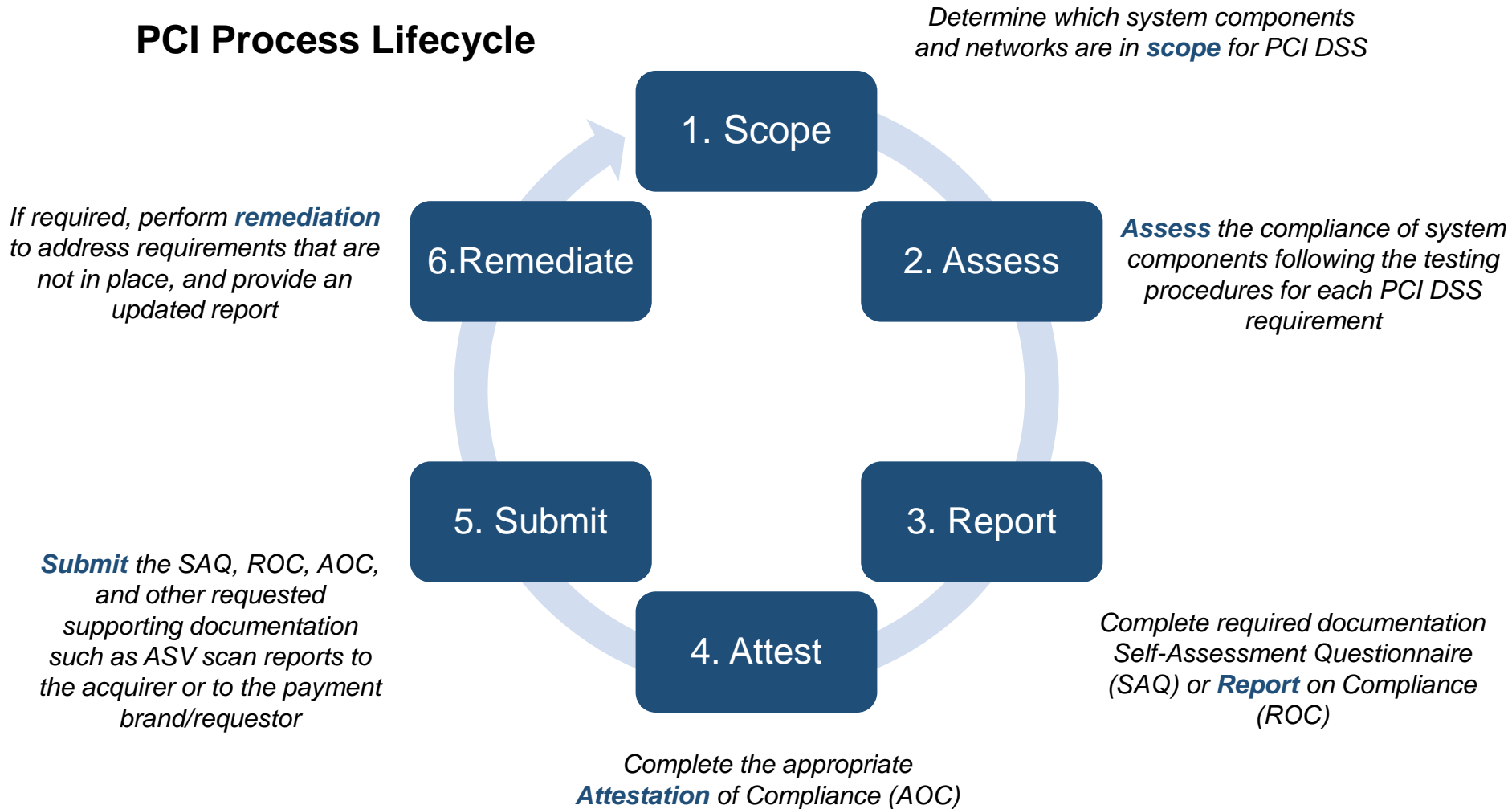- Requires annual onsite assessment and quarterly ASV scans

Level 3

- Processing between 20K and 1 million credit card transactions per year
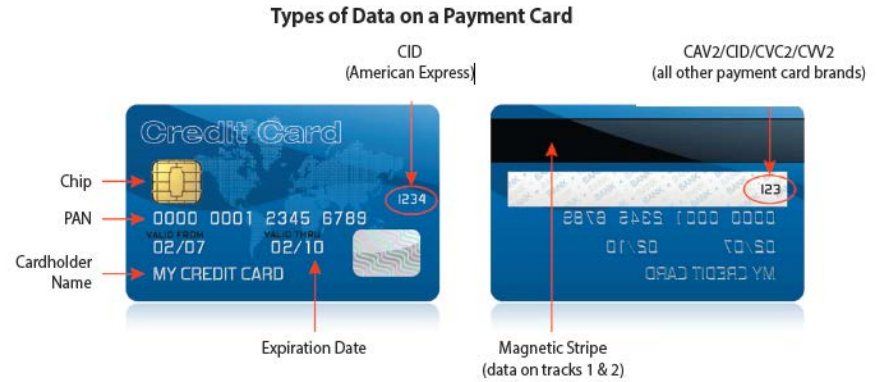- Annual self assessment and quarterly ASV scan

Level 4

- Process less than 20K credit card transactions per year
- Annual self assessment and quarterly ASV scan

PCI Process Lifecycle

Determine which system components and networks are in **scope** for PCI DSS

1. Scope

2. Assess — **Assess** the compliance of system components following the testing procedures for each PCI DSS requirement

6. Remediate — If required, perform **remediation** to address requirements that are not in place, and provide an updated report

3. Report — Complete required documentation Self-Assessment Questionnaire (SAQ) or **Report** on Compliance (ROC)

5. Submit — **Submit** the SAQ, ROC, AOC, and other requested supporting documentation such as ASV scan reports to the acquirer or to the payment brand/requestor

4. Attest — Complete the appropriate **Attestation** of Compliance (AOC)

Elements of Payment Card Data

Types of Data on a Payment Card

CID (American Express)

CAV2/CID/CVC2/CVW2 (all other payment card brands)

Chip

PAN

Cardholder Name

0000 0001 2345 6789

VALID FROM 02/07   VALID THRU 02/10

MY CREDIT CARD

Expiration Date

Magnetic Stripe (data on tracks 1 & 2)

	Data Element	Storage Permitted	Render Stored Data Unreadable per Requirement 3.4
Account Data — **Cardholder Data**	Primary Account Number (PAN)	Yes	Yes
	Cardholder Name	Yes	No
	Service Code	Yes	No
	Expiration Date	Yes	No
Sensitive Authentication of Data2	Full Track Data3	No	Cannot store per Requirement 3.2
	CAV2/CVC2/CVV2/CID4	No	Cannot store per Requirement 3.2
	PIN/PIN Block5	No	Cannot store per Requirement 3.2

What is new with PCI DSS v3.2?

- ✓ Multi Factor Authentication for administrative access into your credit card data environment

- ✓ Secure Sockets Layer (SSL) and early Transport Layer Security (TLS) not supported, have until June 30, 2018 to complete migration

- ✓ Key dates in becoming compliant with PCI DSS v3.2

  - Any assessment started after October 2016 will be conducted using PCI DSS v3.2

  - As of February 2018 all requirements within PCI DSS become effective

Techniques to Reducing Your Exposure and Scope

- ✓ Network Segmentation

- ✓ Storage of credit card data

- ✓ Point-to-Point Encryption (P2PE)

- ✓ Tokenization

- ✓ Outsourcing for payment processing

PCI Takeaways

✓ Determine your merchant level and compliance responsibility

✓ Document your credit card process flows

✓ Understand where your credit card data is within your network

✓ Document policies and procedures

✓ Determine ways to reduce your scope and risk exposure

Europay, MasterCard, and Visa (EMV)

Characteristics:

- ✓ Unlike magnetic-stripe cards, every time an EMV card is used for payment, the card chip creates a unique transaction code that cannot be used again
- ✓ Helps to reduce fraud

Metrics:

- ✓ Visa reported chip enabled merchants saw 52% drop off in fraud in 2016
- ✓ Since October 2015 the liability for card-present fraud has shifted to the party is the least EMV-compliant in a fraudulent transaction
- ✓ Early rollout of EMV encountered performance problems
- ✓ Globally 52% of transactions are EMV
- ✓ United States, 52% of cards have EMV Technology, accounting for 18.6% of transactions

Mobile Wallets, Digital Payments and Contactless Payments

Characteristics:

- ✓ Contactless POS and Payment Cards
- ✓ Utilizes Near Field Communication (NFC) and / or Biometrics
- ✓ Access to APIs
- ✓ Development of payment applications and back end services

Metrics:

- ✓ Reduces transactions cost for banks, thus reducing operating cost
- ✓ $3.6 trillion in global transactions
- ✓ 20% growth since 2015
- ✓ 60% of this growth attributed to contactless payments

Mobile POS (mPos) and Cloud Based POS

Characteristics:

- ✓ Cost effective
- ✓ Convenience, smaller footprint in retail space
- ✓ Accessibility for smaller merchants

Metrics:

- ✓ Forecast 27M + devices in United States by 2021, 3.2M in 2014

  http://www.businessinsider.com/future-of-payments-trends-in-payment-processing-2016-10

- ✓ Estimated annual growth rate of 19% over next six years (2016-2023)

  https://www.fractovia.org/news/industry-research-report/point-of-sale-pos-terminals-market

Cryptocurrency

- ✓ A digital or virtual currency that uses cryptography for security

- ✓ Not issued by a central authority

- ✓ Transfer of funds facilitated through the use of public and private keys

- ✓ Utilizes "block chain"
  - ✓ Distributed database that is used to maintain a continuously growing list of records, "blocks"
  - ✓ Managed in Peer-to-Peer network

- ✓ Volatile and varying degrees of fluctuation

- ✓ Lack of regulation

Emerging payment technology considerations:

- ✓ Desire to have quick and immediate transactions

- ✓ Contactless payments and payment technology on the rise

- ✓ Security and Regulation considerations with new technology

For More Information Contact:

Brad Hanscom
bhanscom@berrydunn.com

Matthew Bria
mbria@berrydunn.com