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

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.**

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
1. **Scope**

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

2. **Assess**

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

3. **Report**

Complete required documentation such as ASV scan reports to the acquirer or to the payment brand/requestor.

4. **Attest**

Complete the appropriate **Attestation of Compliance (AOC)**.

5. **Submit**

Submit the SAQ, ROC, AOC, and other requested supporting documentation to the acquirer or to the payment brand/requestor.

6. **Remediate**

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

---

**PCI Process Lifecycle**

**Scope**

**Assess**

**Report**

**Attest**

**Submit**

**Remediate**
## Elements of Payment Card Data

<table>
<thead>
<tr>
<th>Data Element</th>
<th>Storage Permitted</th>
<th>Render Stored Data Unreadable per Requirement 3.4</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cardholder Data</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Primary Account Number (PAN)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Cardholder Name</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Service Code</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Expiration Date</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td><strong>Sensitive Authentication of Data</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Full Track Data3</td>
<td>No</td>
<td>Cannot store per Requirement 3.2</td>
</tr>
<tr>
<td>CAV2/CVC2/CVV2/CID4</td>
<td>No</td>
<td>Cannot store per Requirement 3.2</td>
</tr>
<tr>
<td>PIN/PIN Block5</td>
<td>No</td>
<td>Cannot store per Requirement 3.2</td>
</tr>
</tbody>
</table>

### Types of Data on a Payment Card

- **CID** (American Express) on Track 1
- **CAV2/CID/CVC2/CVV2** (all other payment card brands) on Track 2
- Magnetic Stripe (data on tracks 1 & 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 with 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
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.

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