WHO, WHAT, WHY: PCI

Tess Casey Flanagan
Senior Manager and Counsel, Global Compliance Operations

PCI Overview

What is PCI?
Global standards required by major payment card brands (enforced by the banks) for entities that store, process, or transmit cardholder data

Who must comply?
Merchants that store, process, or transmit card and debit cards (cardholder data or CHD) via retail stores, e-commerce, call centers, and mobile, and Service Providers that store, process, or transmit CHD, or impact the security of a cardholder data environment (CDE)

Impacts of non-compliance
- Fines
- Higher transaction fees
- Removal from payment card network
- Brand Damage

Benefits of compliance
- Maintain/improve relationships with third parties
- Inform strategic decisions
- Protect your customers and brand
Myth 1: PCI and GDPR are the same.

Myth: If you are PCI compliant, you are also GDPR compliant.

Fact: While there are key intersections, the European Union General Data Protection Regulation (GDPR) and the PCI DSS are two very different compliance standards.

The PCI DSS is a mature standard addressing the protection and security of cardholder data globally. The GDPR is a new law, effective May 2018, is limited to the EU, and governs all personal data, of which cardholder data is a subset.

Additionally, GDPR goes beyond security controls. In fact, security is only 1 of the 6 GDPR principles. That being said, if you are compliant with the PCI DSS in your EU channels, you are meeting the security control standards of the GDPR.

To be GDPR compliant, you must ensure that you are implementing security controls for other types of personal data, beyond cardholder information, as well as address the other 5 GDPR principles.
What is the PCI?

PCI stands for Payment Card Industry.

PCI compliance means compliance with the PCI Data Security Standard (DSS).

The PCI DSS is a common security standard of over 400 controls required by the major payment card brands guiding how you store, process, or transmit cardholder data.

What is cardholder data (CHD)?

<table>
<thead>
<tr>
<th>Account Data</th>
<th>Storage Permitted</th>
<th>Protection Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cardholder Data (CHD)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Sensitive Authentication Data (SAD)</td>
<td>No</td>
<td>N/A – Cannot store per 3.2</td>
</tr>
</tbody>
</table>

Source: https://www.pcisecuritystandards.org/documents/PCI%20SSC%20Quick%20Reference%20Guide.pdf
PCI Myth 2: Geography

Myth: PCI compliance only applies in the US.

Fact: PCI is a global standard and applies to all Visa, American Express, MasterCard, Discover, and JCB payments.

Merchant Levels

<table>
<thead>
<tr>
<th>Merchant level</th>
<th>Merchant definition</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 1</td>
<td>More than six million transactions annually across all channels, including e-commerce</td>
<td>Annual Onsite PCI Data Security Assessment and Quarterly Network Scans</td>
</tr>
<tr>
<td>Level 2</td>
<td>1,000,000 - 5,999,999 transactions annually</td>
<td>Annual Self-Assessment and Quarterly Network Scans</td>
</tr>
<tr>
<td>Level 3</td>
<td>20,000 - 1,000,000 e-commerce transactions annually</td>
<td>Annual Self-Assessment and Quarterly Network Scans</td>
</tr>
<tr>
<td>Level 4</td>
<td>Less than 20,000 e-commerce transactions annually, and all merchants across channel up to 1,000,000 VISA transactions annually</td>
<td>Annual Self-Assessment and Annual Network Scans</td>
</tr>
</tbody>
</table>

Source: https://www.pcisecuritystandards.org/
**Merchant Levels**

<table>
<thead>
<tr>
<th>Merchant Level</th>
<th>Documentation</th>
<th>Completed by</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 2-4</td>
<td>Self-Assessment Questionnaire (SAQ)*</td>
<td>Internal Security Assessor (ISA)</td>
</tr>
<tr>
<td>Level 1</td>
<td>Report on Compliance (ROC)*</td>
<td>Qualified Security Assessor (QSA)</td>
</tr>
</tbody>
</table>

*Also complete an Attestation of Compliance (AOC)*

**SAQ Types and Level of Effort**

Manage your scope: know the FAQs
https://www.pcisecuritystandards.org/faqs
Maintaining Compliance

PCI-related buzz words to listen for

- Credit cards
- Debit cards
- Payment cards
- Cardholder data
- Payment Processor

RETAIL
- Payment devices
- Mobile point of sale (MPOS)

CALL CENTER
- Call recording
- Regional call center

E-COMM
- Tokenization
- Mobile payments
- Cloud
- Platform Hosting

WHO
Who is Involved?

ISA or QSA

Merchant Internal Teams

Payment Processor

Acquirer

Card Brands

3rd Party Service Provider
Who is In-Scope for PCI?

People, processes, technology

that

Store, process, or transmit CHD, or impact the security of a cardholder data environment

Internal Teams

Teams involved in PCI:

- Ecomm
- IT
- Cyber Security
- Mobile Applications
- Call Center
- Retail Ops
- Procurement
- Asset Protection
- HR
- Accounting
- Insurance
- Legal
- Compliance or Internal Audit
PCI Myth 3: Outsourcing

Myth: Outsourcing card processing makes you compliant.

Fact: Outsourcing simplifies payment card processing but does not provide automatic compliance. You still, at a minimum, have obligations to monitor your service providers and ensure providers’ applications are PCI compliant, train your team, have a data incident response plan, and have in place data security policies and procedures.

How are you getting to your 3rd Party?

<table>
<thead>
<tr>
<th>E-commerce Method</th>
<th>SAQ Type</th>
<th>Guidance for merchants who are required to submit a Report on Compliance (ROC)</th>
<th>Number of Questions under PCI-DSS v3.2 (not including any relevant appendices)</th>
<th>Ease</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wholly Outsourced e-Commerce</td>
<td>SAQ A</td>
<td>Merchants may be required to submit a Report on Compliance (ROC) but may be able to use SAQ A as a reference to identify applicable PCI DSS requirements for that environment, providing the environment fully meets all eligibility criteria defined in that SAQ.</td>
<td>22</td>
<td>🏷️</td>
</tr>
<tr>
<td>Redirect</td>
<td>SAQ A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>iFrame</td>
<td>SAQ A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Direct Post</td>
<td>SAQ A-EP</td>
<td>Merchants may be required to submit a Report on Compliance (ROC) but may be able to use SAQ A-EP as a reference to identify applicable PCI DSS requirements for that environment, providing the environment fully meets all eligibility criteria defined in that SAQ.</td>
<td>191</td>
<td>🏷️</td>
</tr>
<tr>
<td>JavaScript</td>
<td>SAQ A-EP</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>API</td>
<td>SAQ D</td>
<td>Some requirements of SAQ D or ROC may be marked “not applicable” if they do not apply to the specific e-commerce channel. Consult with QSA or acquirer for further guidance.</td>
<td>250</td>
<td>🏷️</td>
</tr>
<tr>
<td>Other</td>
<td>SAQ D</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Iframe v. Modal v. Java

WHY
Why be PCI compliant?

<table>
<thead>
<tr>
<th>Impacts of Non-Compliance</th>
<th>Benefits of Compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fines</td>
<td>Maintain/improve relationships with third parties</td>
</tr>
<tr>
<td>Higher transaction fees</td>
<td>Inform strategic decisions</td>
</tr>
<tr>
<td>Removal from payment card network</td>
<td>Protect your customers and brand</td>
</tr>
<tr>
<td>Brand damage</td>
<td></td>
</tr>
</tbody>
</table>

Conclusion

One person’s
- Lessons learned
- Tips and tricks
- Final thoughts
## Appendix 1: Acronym Cheat Sheet

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>AOC</td>
<td>Attestation of Compliance</td>
</tr>
<tr>
<td>CDE</td>
<td>Cardholder Data Environment</td>
</tr>
<tr>
<td>CHD</td>
<td>Cardholder Data</td>
</tr>
<tr>
<td>GDPR</td>
<td>General Data Protection Regulation</td>
</tr>
<tr>
<td>ISA</td>
<td>Internal Security Assessor</td>
</tr>
<tr>
<td>PCI</td>
<td>Payment Card Industry</td>
</tr>
<tr>
<td>PCI DSS</td>
<td>Payment Card Industry Data Security Standard</td>
</tr>
<tr>
<td>QSA</td>
<td>Qualified Security Assessor</td>
</tr>
<tr>
<td>ROC</td>
<td>Report on Compliance</td>
</tr>
<tr>
<td>SAQ</td>
<td>Self Assessment Questionnaire</td>
</tr>
</tbody>
</table>