

# 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

# WHAT

## 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?

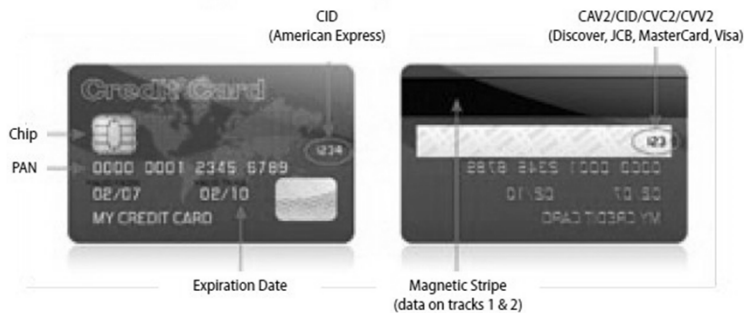
**PCI stands for Payment Card Industry.**

**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)?

**Types of Data on a Payment Card**



Account Data	Storage Permitted	Protection Required
Cardholder Data (CHD)	Yes	Yes
Sensitive Authentication Data (SAD)	No	N/A – Cannot store per 3.2

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

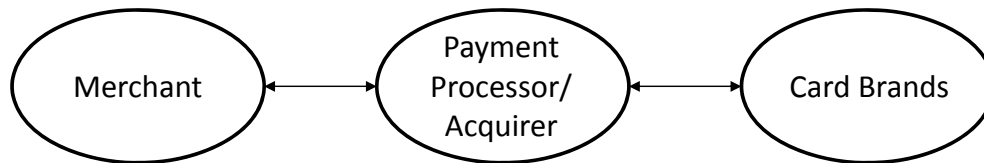
Merchant level	Merchant definition	Requirement
Level 1	More than six million transactions annually across all channels, including e-commerce	Annual Onsite PCI Data Security Assessment and Quarterly Network Scans
Level 2	1,000,000 - 5,999,999 transactions annually	Annual Self-Assessment and Quarterly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

Source: <https://www.pcisecuritystandards.org/>

## Merchant Levels

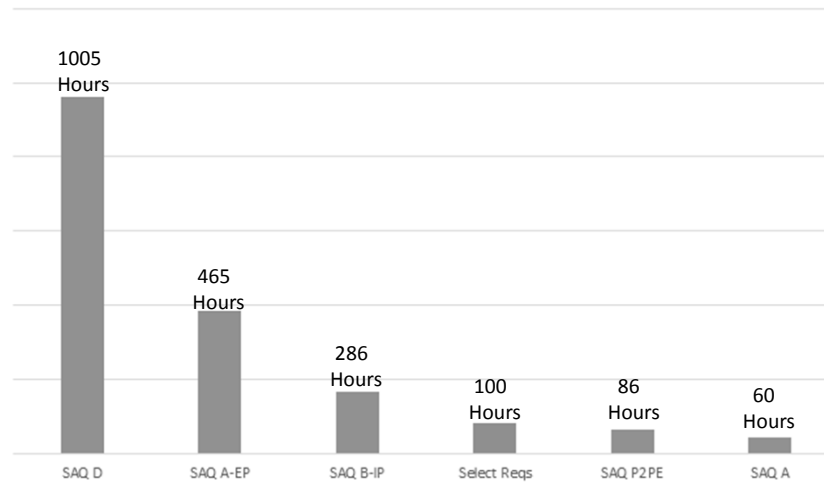
Merchant Level	Documentation	Completed by
Level 2-4	Self-Assessment Questionnaire (SAQ)*	Internal Security Assessor (ISA)
Level 1	Report on Compliance (ROC)*	Qualified Security Assessor (QSA)

\*Also complete an Attestation of Compliance (AOC)



## SAQ Types and Level of Effort

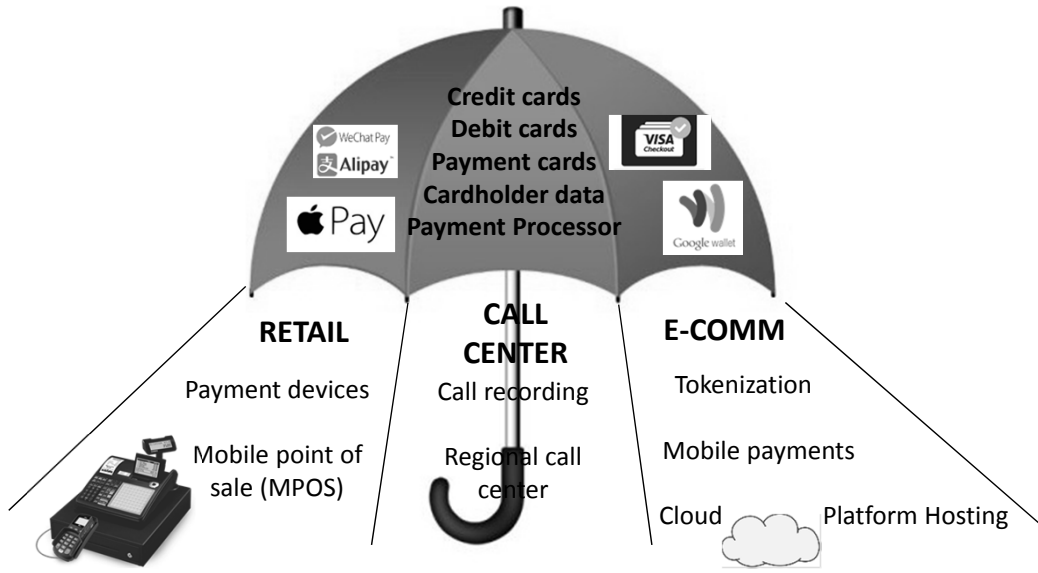
Number of Requirements



Manage your scope: know the FAQs  
<https://www.pcisecuritystandards.org/faqs>

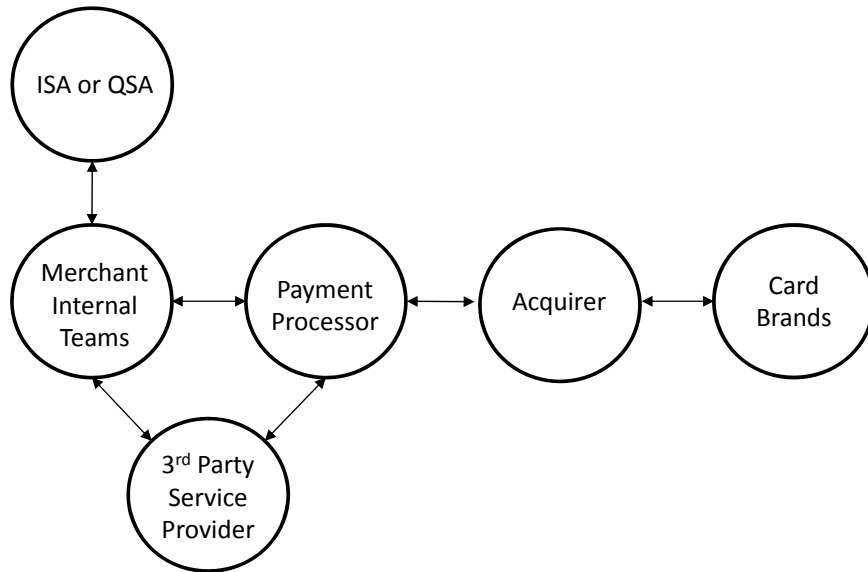
# Maintaining Compliance

PCI-related buzz words to listen for

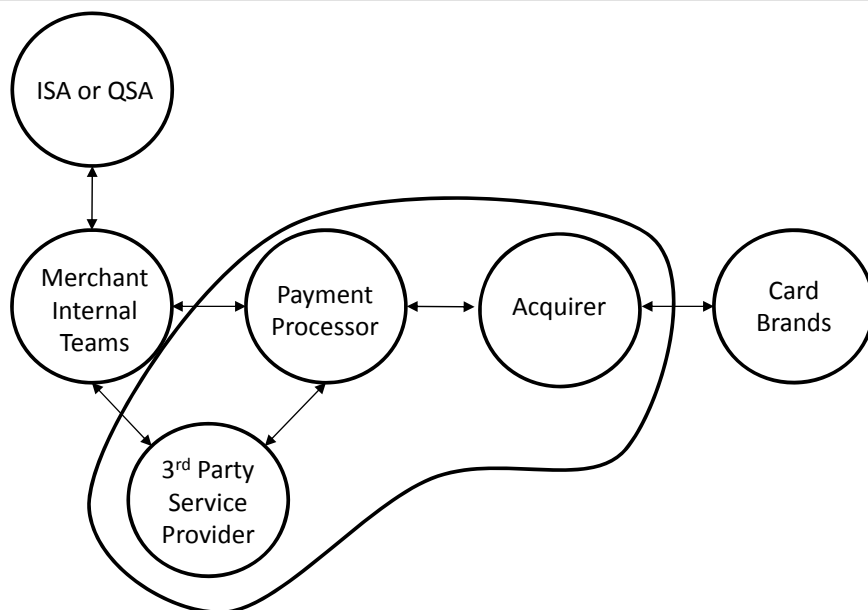


# WHO

## Who is Involved?



## Who is Involved?



## 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 3<sup>rd</sup> Party?

PCI DSS Documentation Requirements by E-commerce Method

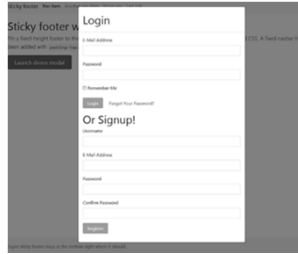
E-commerce Method	SAQ Type for eligible merchants	Guidance for merchants who are required to submit a Report on Compliance (ROC)	Number of Questions under PCI-DSS v3.2 (Not including any relevant appendices)	Ease
Wholly Outsourced e-Commerce	SAQ A	Merchants may be required to submit a Report on Compliance (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.	22	
Redirect	SAQ A			
iFrame	SAQ A			
Direct Post	SAQ A-EP	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.	191	
JavaScript	SAQ A-EP			
API	SAQ D	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.	250	
Other	SAQ D			

[https://www.pcisecuritystandards.org/pdfs/best\\_practices\\_securing\\_ecommerce.pdf?agreement=true&time=1505324401439](https://www.pcisecuritystandards.org/pdfs/best_practices_securing_ecommerce.pdf?agreement=true&time=1505324401439)

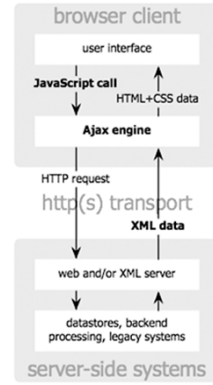
## IFrame v. Modal v. Java



IFrame



Modal



Java Ajax

# WHY

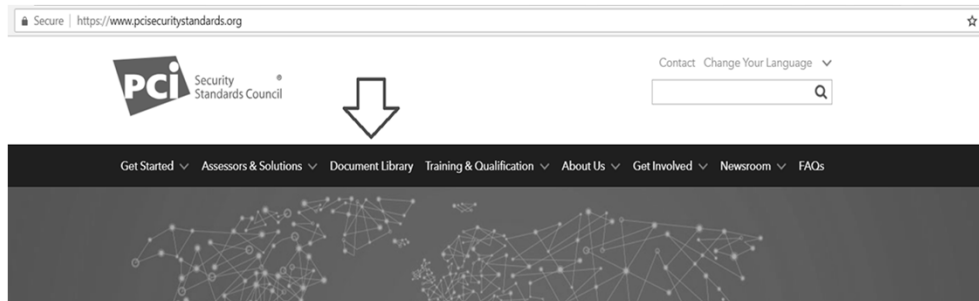
## Why be PCI compliant?

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

## Conclusion

### One person's

- Lessons learned
- Tips and tricks
- Final thoughts



## Appendix 1: Acronym Cheat Sheet

Acronym	Meaning
AOC	Attestation of Compliance
CDE	Cardholder Data Environment
CHD	Cardholder Data
GDPR	General Data Protection Regulation
ISA	Internal Security Assessor
PCI	Payment Card Industry
PCI DSS	Payment Card Industry Data Security Standard
QSA	Qualified Security Assessor
ROC	Report on Compliance
SAQ	Self Assessment Questionnaire