Payment Facilitators and PCI DSS Compliance

Helen Huyton

Team Lead Scheme Compliance

adyen

Sam Pfanstiel, Ph.D.

CISSP CISM CISA CCAK CEH ISA PCIP

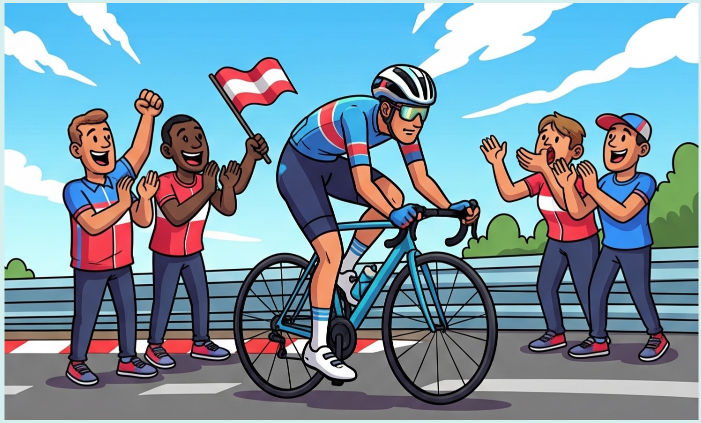
Principal Technical Compliance Analyst

toast

Agenda

PayFac Overview

Entities & Roles



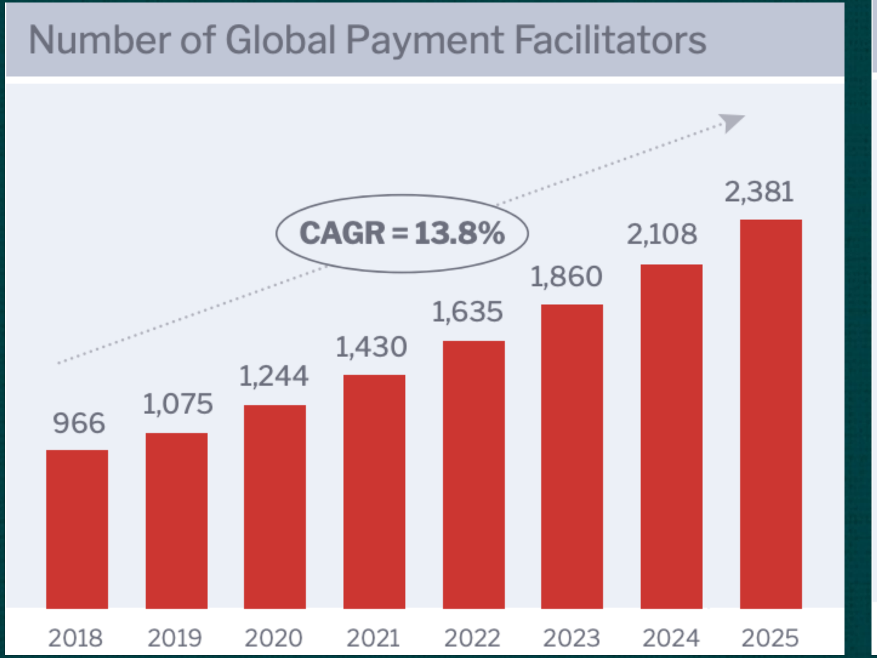
PayFac PCI DSS Strategies

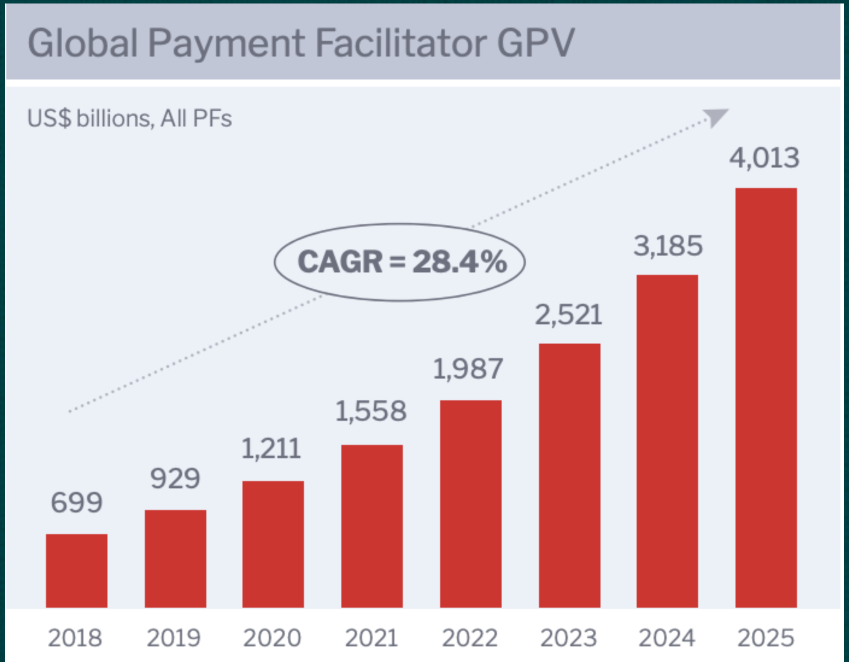
PayFac Overview

Overview - PayFacs and PCI DSS Compliance

Why this topic is timely and important?

- Growth of the PayFac Model
- Compliance and Security responsibility
- Data breaches, fraud, and non-compliance
- Complexity of modern payments and increasing relevance of the PayFac model

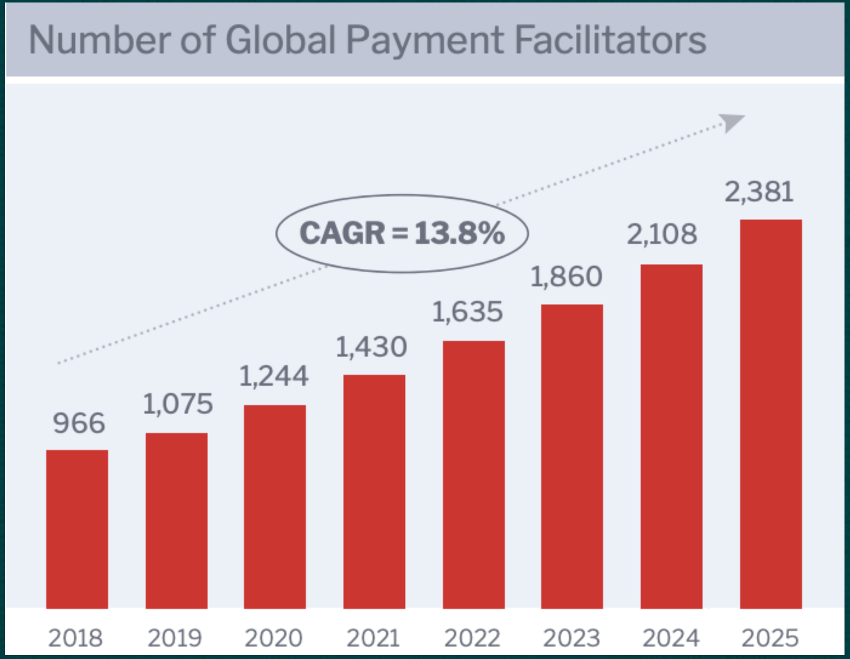


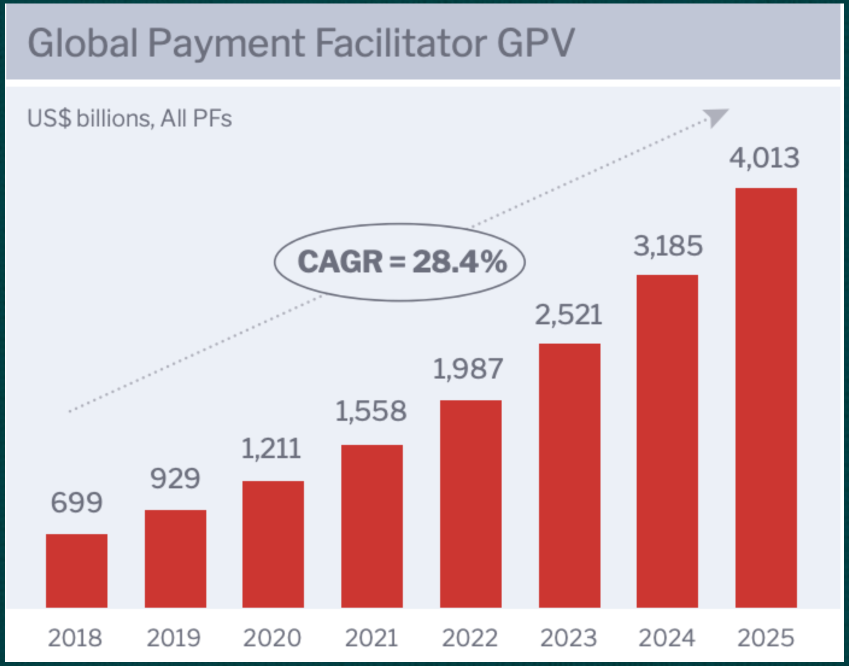


Overview - PayFacs and PCI DSS Compliance

Why this topic is timely and important?

- Growth of the PayFac Model
- Compliance and Security responsibility
- Data breaches, fraud, and non-compliance
- Complexity of modern payments and increasing relevance of the PayFac model





Evolution of the PayFac Model

Introduction of the PayFac model

- Card networks formalized the PayFac model in their rules in the early 2000’s

Examples of PayFacs

- Toast
- Paypal
- SumUp
- Square
- Stripe

PayFac Model vs. Traditional Acquiring Model

PayFac Model

- Enables SMEs to accept payments
- Handle the technical, financial, risk and compliance complexities

Traditional Acquiring Model

- Direct relationship with (sub) merchants, friction for SMEs
- **Key characteristics:** Lengthy onboarding, high compliance burden, complex integrations

Evolution of the PayFac Model

Introduction of the PayFac model

- Card networks formalized the PayFac model in their rules in the early 2000’s

Examples of PayFacs

- Toast
- Paypal
- SumUp
- Square
- Stripe
- Shopify

PayFac Model vs. Traditional Acquiring Model

PayFac Model

- Enables SMEs to accept payments
- Handle the technical, financial, risk and compliance complexities

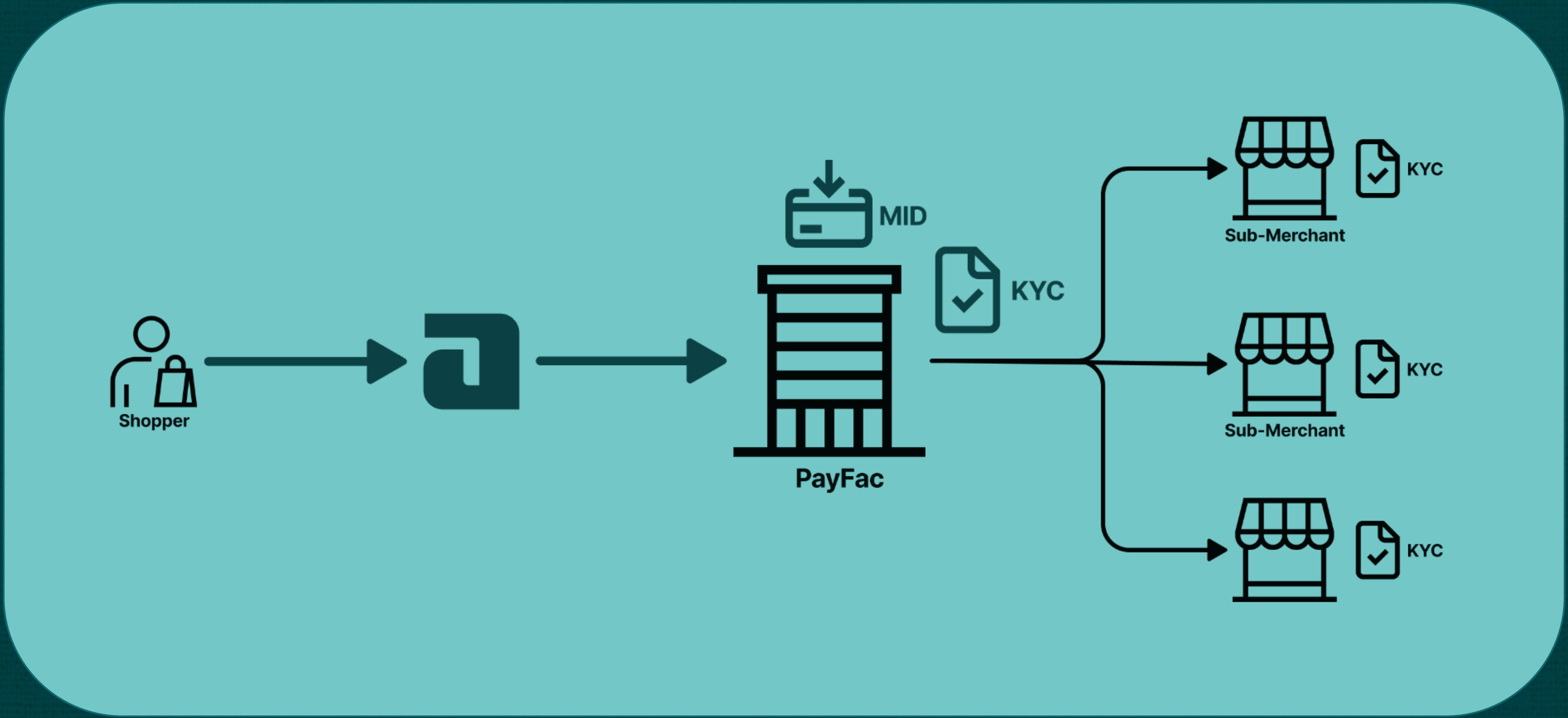
Traditional Acquiring Model

- Direct relationship with (sub) merchants, friction for SMEs
- **Key characteristics:** Lengthy onboarding, high compliance burden, complex integrations

Entities & Roles

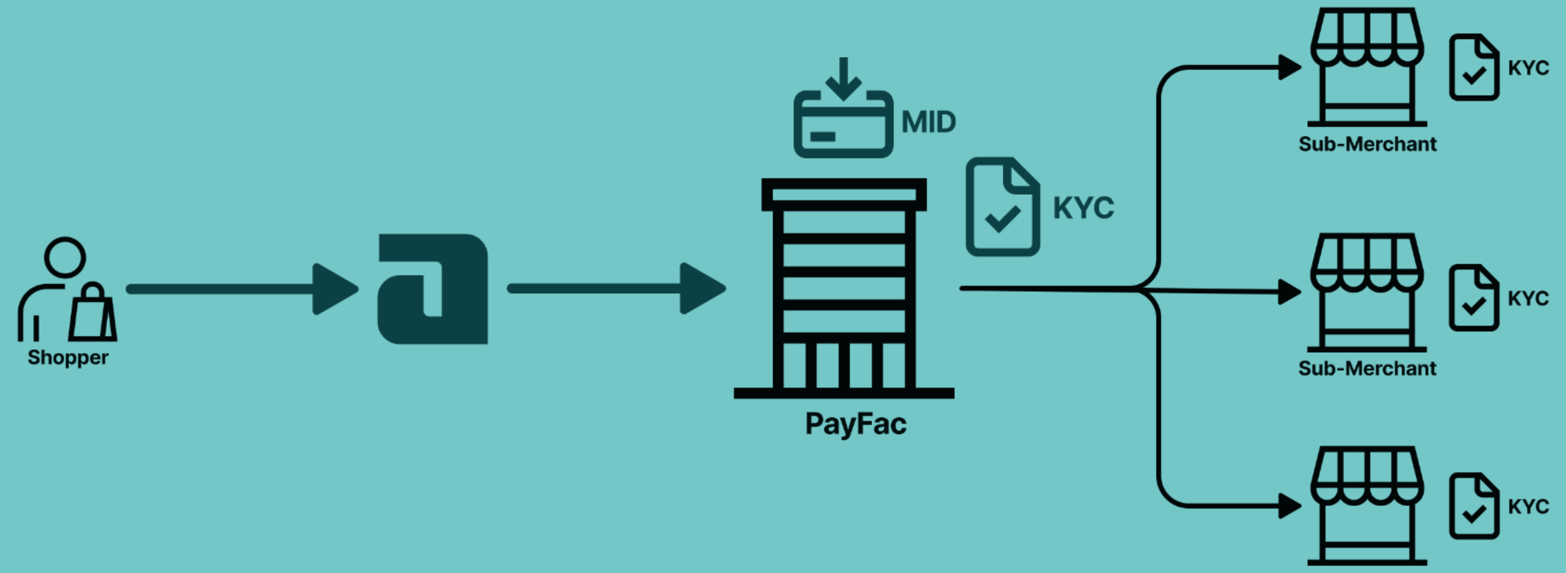
PayFac Ecosystem Relationship Diagram

Cardholder, Acquiring Banks, PayFac, and Sub-merchants



PayFac Ecosystem Relationship Diagram

Cardholder, Acquiring Banks, PayFac, and Sub-merchants



Will the Real “Merchant” Please Stand Up?

Merchant, Master Merchant, Sub-Merchant, Platform Merchant, Original Merchant, Merchant Business, Sponsored Merchant, Direct Merchant, Primary Merchant, Merchant-of-Record (MoR)

- Different meanings in different contexts (banking regulations, PCI, acquirer, individual brands)
- For PCI DSS:
  - Identifying responsibilities is key (12.8, 12.9)
  - Merchant can also be a Service Provider (FAQ 1079)
  - Consult with acquirer and/or brands (FAQ 1473)
- Other PCI programs which defined Merchant (e.g., P2PE) may wish to review glossary definition to reduce confusion

Marketplaces vs. PayFac

Feature	Marketplace Facilitators	Payment Facilitator
Core Purpose	Platform that enables buyers to transact with multiple sellers.	Entity that enables sub-merchants to accept payments under its master merchant account.
Compliance Responsibility	Varies; may shift PCI DSS and KYC responsibilities to a processor or PayFac.	Directly responsible for PCI DSS, KYC/AML, fraud, and onboarding.
PCI Scope	May be reduced or offloaded if payments are handled by the processor or acquirer.	Full PCI DSS responsibility for its own systems; may reduce sub-merchant scope via hosted integrations.
Examples	Amazon, Etsy, Airbnb, eBay, Uber	Toast, SumUp, Square, Shopify Payments

Marketplaces vs. PayFac

Feature	Marketplace Facilitators	Payment Facilitator
Core Purpose	Platform that enables buyers to transact with multiple sellers.	Entity that enables sub-merchants to accept payments under its master merchant account.
Compliance Responsibility	Varies; may shift PCI DSS and KYC responsibilities to a processor or PayFac.	Directly responsible for PCI DSS, KYC/AML, fraud, and onboarding.
PCI Scope	May be reduced or offloaded if payments are handled by the processor or acquirer.	Full PCI DSS responsibility for its own systems; may reduce sub-merchant scope via hosted integrations.
Examples	Amazon, Etsy, Airbnb, eBay, Uber	Toast, SumUp, Square, Shopify Payments

PayFac PCI DSS Strategies

PCI Peloton (“Follow the Leader”)

PCI SSC

- Manages Standards & Programs

Networks

- Enforce the Standards
- PayFacs register with networks

Acquirer

- Accountable to Networks for PCI DSS Compliance

Master Merchants

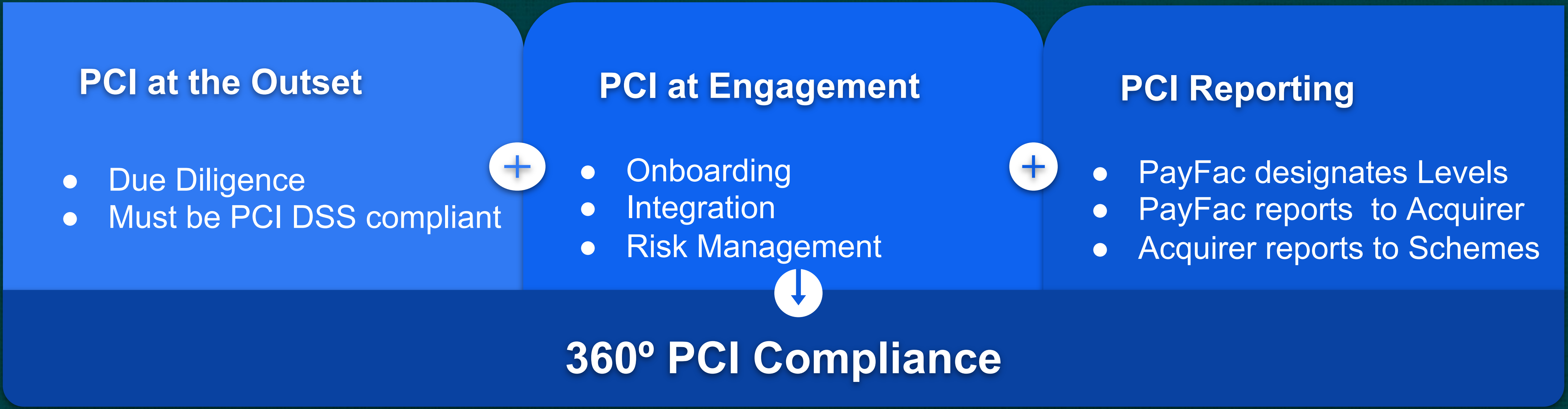
- Platform Provider
- PCI Solution Provider
- Sub-merchant Levels
- Accountable to Acquirer for PCI DSS Compliance

Sub Merchants

- Review PayFac AOC and RM
- Meet Applicable Compliance Requirements

PCI DSS Compliance in the PayFac model

PCI Lifecycle between the PayFac and Acquirer



PCI at the Outset

- Due Diligence
- Must be PCI DSS compliant

+

PCI at Engagement

- Onboarding
- Integration
- Risk Management

+

PCI Reporting

- PayFac designates Levels
- PayFac reports to Acquirer
- Acquirer reports to Schemes

360º PCI Compliance

PCI DSS Compliance Best Practices

Winning Together

- Collaborate Closely with Acquirer
  - Aligning on perspectives and risk mitigation
  - Understanding the unique business model
- Shared Responsibility
  - Take ownership of responsibilities for certain PCI requirements
  - Provide clear responsibility matrix
- Scope Impact
  - Toast as a closed ecosystem
  - Provides tools and services to facilitate compliance
  - Other guidance for sub-merchants

PCI DSS Compliance Best Practices

Winning Together

- Collaborate Closely with Acquirer
  - Aligning on perspectives and risk mitigation
  - Understanding the unique business model
- Shared Responsibility
  - Take ownership of responsibilities for certain PCI requirements
  - Provide clear responsibility matrix
- Scope Impact
  - Toast as a closed ecosystem
  - Provides tools and services to facilitate compliance
  - Other guidance for sub-merchants

Looking Ahead

The PayFac model will continue to evolve with the payments industry, not a static model.

- Evolution of PCI Standards
- Support for New Payment Models
- Changes to Consumer Payment Behaviors
- International Expansion

Looking Ahead

The PayFac model will continue to evolve with the payments industry, not a static model.

- Evolution of PCI Standards
- Support for New Payment Models
- Changes to Consumer Payment Behaviors
- International Expansion

Thank you

PCI Security Standards Council®

2025 NORTH AMERICA COMMUNITY MEETING