

North America
Community Meeting

VANCOUVER | 2026



Inside PCI 3DS

What It Protects, What It Requires, and Where It Connects

Raman Dhaliwal

Security Compliance
Block Inc.



AGENDA



01 Setting the Scene

The Risk, The Components, and How it Works

02 The Standard

Diving into the standard, scoping and data elements

03 Where It Connects

Square's implementation, EMVCo, SCA, and unified compliance

Setting the Scene

01 The Authentication Challenge

The World We're Protecting

THE WORLD WE'RE PROTECTING

Someone just bought a $2,000 laptop with your card.

THE FUNDAMENTAL GAP

In-Person Checkout

High security with physical presence verification.

Online Checkout

A static 16-digit number, expiry, and CVV code that anyone can copy.

THE SCALE OF FRAUD

$30B+

Global CNP fraud losses annually (2023)

73%

Of all credit card fraud is card-not-present

91%

Of e-commerce merchants targeted

THE CHALLENGE

Closing the Loop

The global payment industry built **3D Secure (3DS)** protocols to bridge this gap.

The Real Question

Who secures the complex, multi-hop infrastructure that does the securing?

20 YEARS OF SECURING PAYMENT DATA PCI

The Components

3DSS
Merchant Side

DS
Network Router

ACS
Issuer Side

The important thing is not one component — it is the chain of trust between them.

How They Connect

3DSS		DS		ACS
Merchant Side	→ hop	Network Router	→ hop	Issuer Side
Starts **authentication**		Routes **request**		Evaluates **risk**

Each Hop Carries the Authentication Decision

What Keeps Us Up at Night

3DSS
Merchant Side

Bypass attacks
Skipping authentication entirely

DS
Network Router

Interception
Auth messages captured in transit

Spoofing
Fake responses injected into flow

Infrastructure compromise
The servers themselves become targets

ACS
Issuer Side

Credential theft
Cryptographic keys compromised

Data leakage
Auth values or cryptograms exposed

The system that protects cardholders... needs protection itself.

The question isn't IF these risks exist, it's WHO is responsible for securing against them.

02

The Standard

Enter PCI 3DS

Purpose-built security for authentication infrastructure.

DEFINITION

PCI 3DS: Purpose-built security for authentication infrastructure

Scope & Applicability

PCI SSC standard for 3DS functions

- Applies directly to ACS, DS, and 3DSS operators

Core Objective

Secure the infrastructure that authenticates consumers

Co-existence

Separate but complementary

- Works in tandem with traditional DSS requirements

SCOPE & DEPLOYMENT

Scope is driven by where 3DS data lives and how you deploy

In Scope

- Systems processing, storing, or transmitting 3DS data
- Supporting infra: HSMs, key mgmt, logs
- Connected systems impacting 3DS security
    - 3DS components: ACS, DS, 3DSS

Deployment Models

- Self-hosted → you own full scope
- Third-party → shared responsibility
- Hybrid → careful boundary definition

Deployment Model Shapes Your Compliance Scope

SENSITIVE DATA

PCI 3DS Data

Authentication Values

Cardholder credentials, PINs, or biometric templates used for identity verification.

Cryptograms

Dynamically generated transaction values securing payment authorization paths.

Cryptographic Keys

Keys utilized for encryption, signing, and decryption of critical 3DS components.

DS Data

Directory Server metadata, routing maps, and core transaction flow records.

3DS Messages

Standard protocol request/response packets transmitted between active endpoints.

Device Data

SDK-collected platform details and browser headers used for risk evaluations.

REQUIREMENTS

Part 1 is familiar. Part 2 is the 3DS-specific work.

Part 1 — Baseline Security

Covered by your PCI DSS ROC

- Network security & segmentation
- Access control & authentication
- Encryption & key management
- Vulnerability management & patching
- Monitoring, logging & incident response
- Physical security

Part 2 — 3DS-Specific Controls

- 3DS component validation & integrity
- Protocol-specific data protection
- HSM & cryptographic operation controls (FIPS 140-2 Level 3+)
- 3DS environment isolation requirements
- Security governance specific to 3DS operations

Compliance with PCI DSS can Cover Part 1 Requirements

03

The Bigger Picture

Where it Connects

BUILD DECISION

Why Square Built a 3DS Server In-House

In-House 3DS Server

Full Control & Protection

Square manages risk & disputes on behalf of our sellers. 3DS is vital to protect our merchants and ourselves from CNP fraud.

The Business Case

Why Not Use a Vendor?

01. Eliminate Fees

02. Enable Innovation

03. Scale Globally

VALIDATION STANDARDS

3D Secure Is an EMVCo Protocol. PCI 3DS Secures Its

EMVCo Certification

"You built it right"

3DS is owned & maintained by EMVCo [cite: 17]

- **Tests:** functional correctness, interoperability, protocol conformance
- **Produces:** Letter of Approval
- **Scope:** The Software Protocol

PCI 3DS Assessment

"You're running it securely"

Validates the active environment

- **Tests:** environment security, crypto controls, access, monitoring
- **Produces:** ROC + AOC
- **Scope:** the infrastructure

Note: Technically independent — but the AOC asks for your LOA details. Payment brands may expect both.

REGULATORY CONTEXT

3DS2 Delivers SCA — PCI 3DS Secures the Delivery Mechanism

STRONG CUSTOMER AUTHENTICATION

SCA Mandates & 3DS2

- **PSD2 (EU) Mandate:** Requires 2 of 3 factors — knowledge, possession, and inherence.
- **Primary Protocol:** 3DS2 is the industry standard for delivering SCA in online payments.
- **Global Expansion:** Similar mandates are actively emerging in the UK, Australia, and India.

COMPLIANCE & SECURITY

Securing Infrastructure

- **PCI 3DS Security:** Specifically secures the underlying infrastructure that makes SCA possible.
- **Global Acceleration:** Adoption of the 3DS2 standard is accelerating rapidly worldwide.
- **Mandatory Compliance:** Meeting these standards is no longer optional for global commerce.

Takeaway: As SCA-style mandates expand globally, 3DS infrastructure becomes a critical compliance dependency.

KEY TAKEAWAYS

Some takeaways for your 3DS security strategy

01. UNDERSTAND RISK

Understand Risk

- CNP fraud demands auth security
- Know your components — ACS, DS, 3DSS define scope

02. THE COMPLIANCE STANDARD

Know the Standard

- Part 1 = your DSS ROC
- Part 2 = new 3DS-specific work
- EMVCo certifies product; PCI 3DS secures environment

03. NEXT STEPS

Take Action

- Map your 3DS components and data flows
- Identify gaps vs. PCI 3DS Part 2
- Build an integrated assessment plan

Thank You!

If you want to continue this conversation,

I'll be by the **coffee station**.

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council