

Simple & Complex Environments: A Service Provider's Perspective

Brendan Cleary

Head of Infrastructure Compliance Engineering

stripe

Vincent Passaro

Head of Attacker Engineering

stripe

20 YEARS OF SECURING PAYMENT DATA

PCI Security Standards Council





The Evolution of the Merchant Environment

Phase 1

- Self Hosting
- Direct Access to Card Data
- High Technical Complexity and Risk

Phase 2

- Outsourced Cloud Hosting
- Outsourcing Card Data Environments
- Some Technical Complexity can be Outsourced

Phase 3

- Widespread Platformization
- Tokenization, Card on Account, Low Code/ No Code solutions
- Limited Technical Capability Required

PCI DSS

20 YEARS OF SECURING PAYMENT DATA

Celebrate the Success

PCI DSS Has Delivered for Merchants and Card Holders

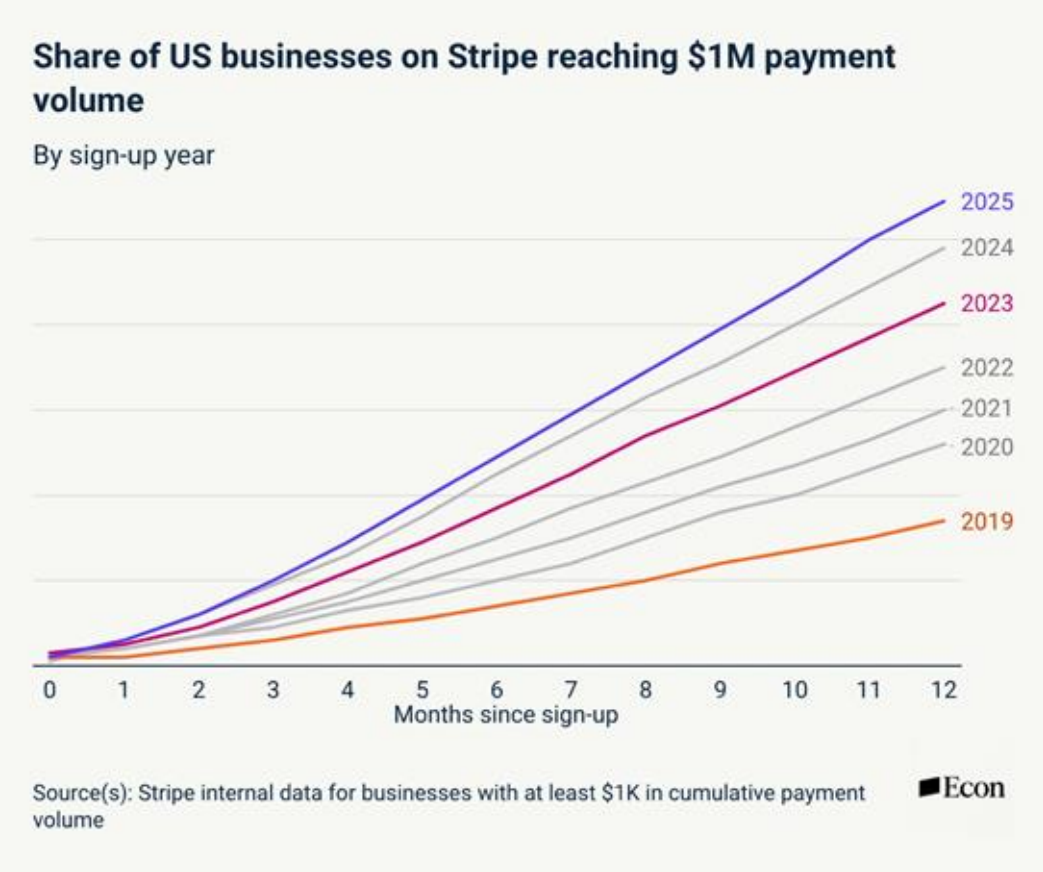
More Merchants: More people can become merchants more easily

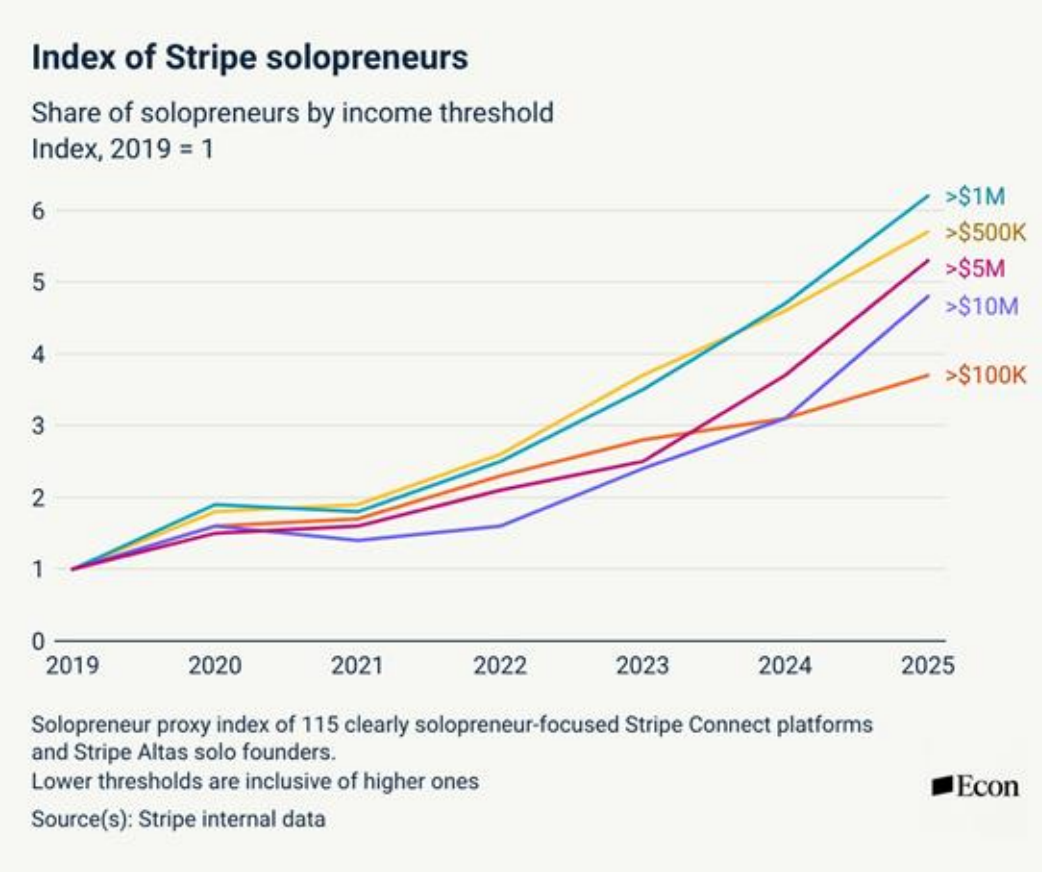
More Secure: More merchants can be more secure by default

Risk Centralization: More risks are able to be centralized

Whats Next?

What's Next - AI Enabled Rapid Scaling & Solopreneurs





20 YEARS OF SECURING PAYMENT DATA PCI



1 Service Provider
Offers cardholder data environment outsourcing to multiple merchants or other service providers and platforms. Dedicated developer and security teams

2 Integrated API Merchant
Develops own website/app, cloud hosted, owns the backend, direct API integration with PSP API. May act as a platform for other merchants

3 Hosted or Redirect Checkout
Develops own website/app, cloud hosted, integrates iframe or redirects for checkout to PSP

4 Low-Code Integration
Writes some code to customize platform provided catalog, redirects to PSP provided hosted checkout.

5 Platformized Merchant
Merchant product catalog and checkout provided entirely by a platform, very limited customization capability. Limited or no technical capability

6 AI Enabled Small Team Merchant - Emerging
Merchant heavily enabled by AI to customize platforms or low code integrations. May have limited or no technical capability, may be solopreneur.

20 YEARS OF SECURING PAYMENT DATA PCI

Trends & Challenges

Operational & Compliance Realities

Merchant Complexity: More types of merchants and risk profiles

Rapid Scaling: Transaction volume is no longer a reliable proxy for capability

AI Impact: Enabling non-technical merchants

Whats does this mean for PCI DSS?

Simple and Complex Merchant Environments

Complex Merchant Environments

Direct APIs, PSPs, and custom clouds

- Custom code requiring dedicated developers
- Direct API integration managing raw transaction flows
- Can be expected to have developer and often security teams
- More able to understand and implement PCI DSS requirements



Simple Merchant Environments

Platform-hosted, low-code architecture, AI enabled

- Redirected checkout and hosted checkout
- Zero card data exposure within internal networks (or no internal networks)
- Web and mobile platforms with limited customization
- Limited ability to interpret or implement security requirements

20 YEARS OF SECURING PAYMENT DATA PCI

Protecting Payments in a Simple-Complex World

DSS Importance: As before DSS will evolve, adapt and shape the ecosystem

Service Providers: Will need to play a bigger role

How do Service Providers Protect Payments?

Protecting the Modern Merchant Ecosystem

Protecting modern merchants with proactive global defense mechanisms



The Modern Payment Threat Landscape

Core Attack Categories by Operational Impact

Credential & Account Abuse

Tactics: Credential stuffing, ATO, session hijacking

Target: Merchant storefronts & customer accounts

Automated Testing

Tactics: Carding, BIN attacks, account enumeration

Target: Payment authorization endpoints & APIs

Data Interception

Tactics: Formjacking, Magecart, API manipulation

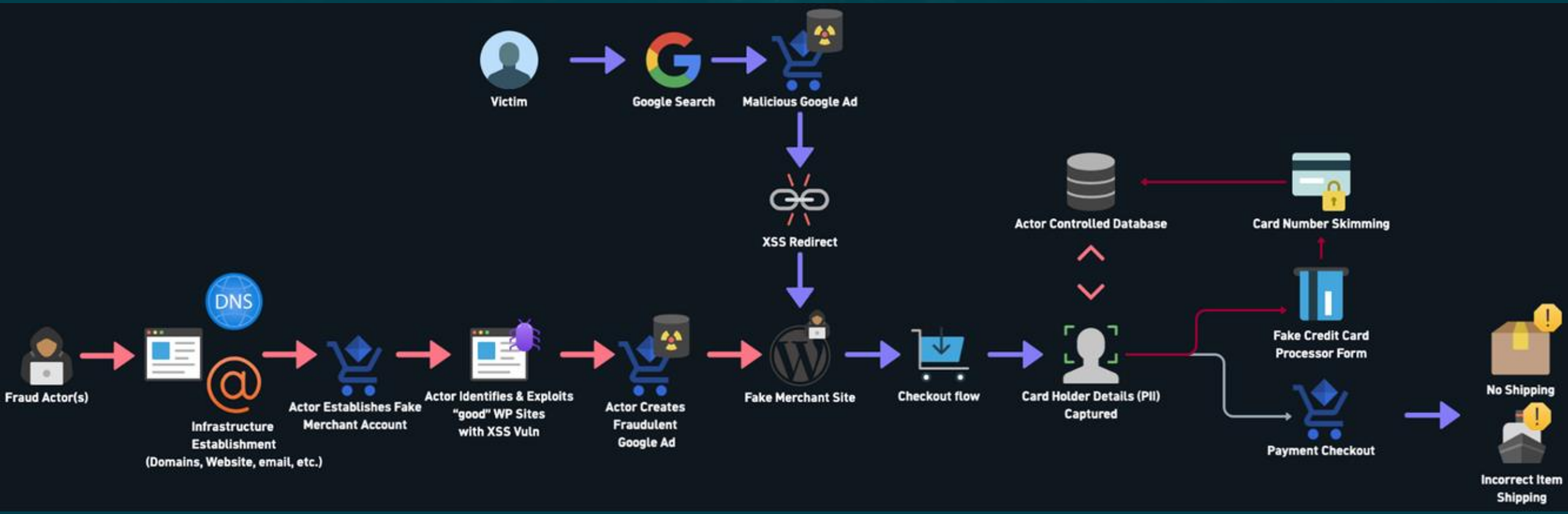
Target: In-flight payment data & checkout flows

Identity & Scheme Exploitation

Tactics: Synthetic identities, triangulation fraud, friendly fraud

Target: Settlement systems, dispute mechanisms & risk limits

Fraud Challenges at Scale



20 YEARS OF SECURING PAYMENT DATA PCI

Address Fraud at Scale - The Workflow

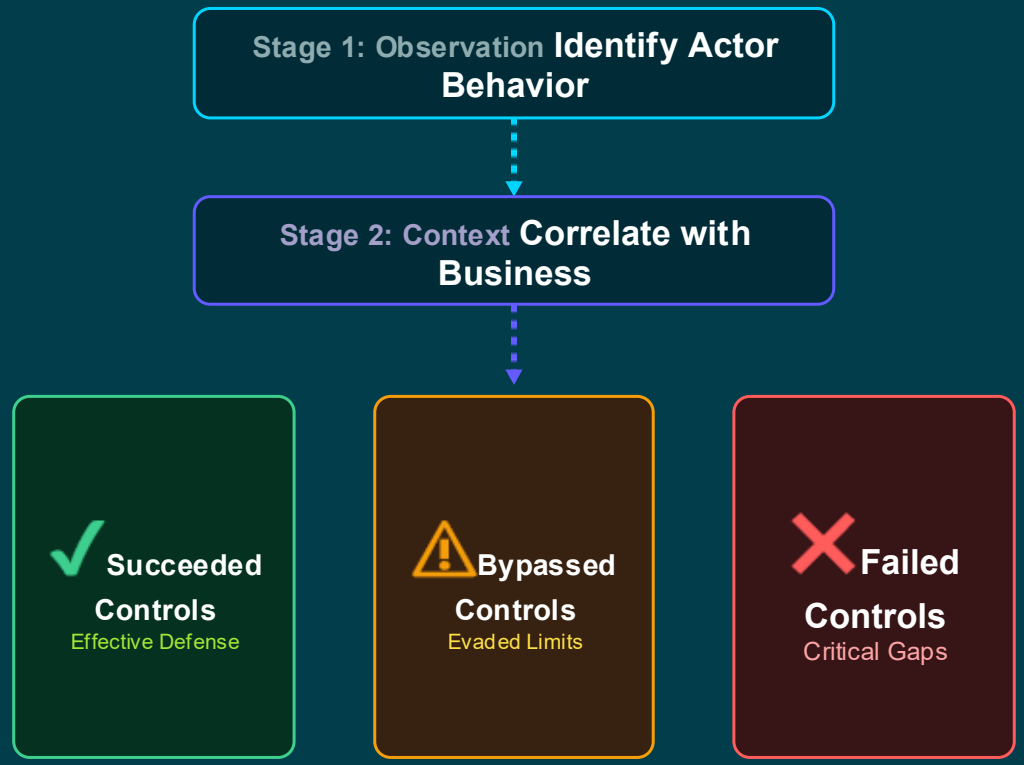
Identifying what the actor is doing (inside and outside the organization)

Correlating ‘what’ the actor is doing against what aspect of the business.

Determining which controls succeeded

Determining which controls were ‘bypassed’

Determining which controls failed



20 YEARS OF SECURING PAYMENT DATA PCI

Guardians of the Financial Ecosystem

Protecting the integrity of the global financial system.

FT3: Fraud Tools, Tactics & Techniques

- A structured knowledge base that maps the tools, tactics, and techniques used by fraudsters against financial systems.

- Gives compliance teams a direct way to map observed fraud behavior against control frameworks and PCI DSS requirements

Open Source & Publicly Shared

Freely available, reflecting Stripe's commitment to raising the security floor across the entire global ecosystem.

Standardized Threat Intel

Enables fraud & compliance teams everywhere to structure threat knowledge the same way security teams use MITRE ATT&CK.

Public on Github

github.com/stripe/ft3

ECOSYSTEM SECURITY **Stripe doesn't just protect its merchants. It protects the ecosystem everyone depends on.**

Modern Fraud Challenges

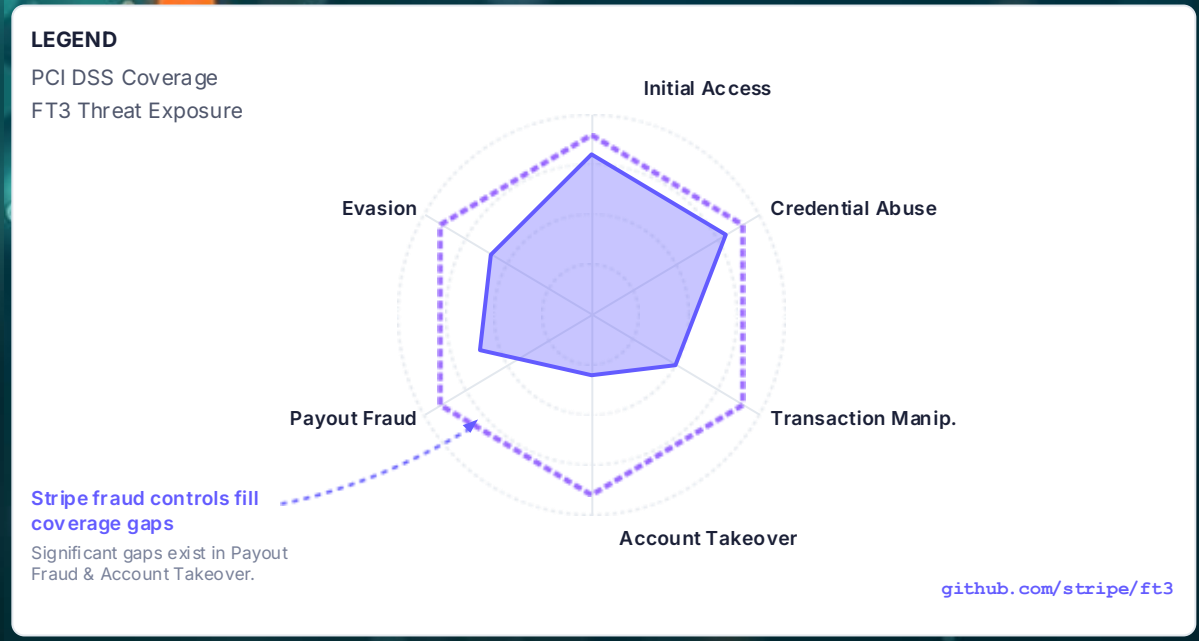


20 YEARS OF SECURING PAYMENT DATA PCI

PCI DSS Controls Mapped to the FT3 Framework

Bridging compliance and fraud defense into a unified security posture

By aligning regulatory baselines with real-world attacker techniques via matrices like FT3, provides the ability to establish a defense posture that satisfies auditors while actively stopping attacks.



20 YEARS OF SECURING PAYMENT DATA PCI

Auditing & Security Testing

Standardized taxonomies as a runtime playbook for controls verification

Unified Audit & Testing Posture

By mapping controls to explicit real-world behaviors, the FT3 matrix serves as an actionable playbook for both compliance assessors and active security teams.

Compliance Auditing & Mapping

Simplifies evidence collection by mapping specific control implementations to standardized, well-defined attacker behaviors.

Red Teaming & Security Testing

Provides a systematic blueprint for penetration testing, enabling operators to validate the effectiveness of specific control blocks against known threat vectors.

Agentic Validation

Translates seamlessly into structured schemas for autonomous LLM security agents, allowing them to dynamically probe, test, and report on control efficacy.



20 YEARS OF SECURING PAYMENT DATA PCI

PSP Level Protections

Future standards should secure global commerce by making robust, platform-level protection unseen yet foundational.

Adaptive Control Structure

- Modernize PCI DSS to encompass all merchant types from simple to complex.
- Structure controls to match actual risk profiles and technical limits of simple environments.

Invisible Platform Baselines

- Integrate invisible PSP-level baselines in future standards and service requirements.
- Baseline protection is essential: unseen infrastructure protects global payments at scale.

Aligning PCI DSS to the Modern Merchant Ecosystem

Reflect all Merchant Types

- PCI DSS must reflect the operational scale, risk profile, and architecture across diverse merchant environments.

Recognize Technical Limits

- Create realistic, achievable criteria that match merchant capabilities and priorities.

Recognizing Service Provider Safeguards

- Incorporate platform layers and service provider controls as valid mitigations for simpler merchant environments risks

20 YEARS OF SECURING PAYMENT DATA
PCI