

20 Years in the Trenches: How the Threat Landscape Shaped PCI DSS — and What's Coming Next

Raymond Simpson

Foregenix PCI QSA | 20 Years the Payment Card Security



Session Agenda

Four parts — from 2004 to 2030 and beyond

01 Where It All Began — the 2002–2004 landscape and why PCI DSS was born

02 A Decade of Escalation — breaches, skimmers and the standards that responded

03 The Modern Threat Era — AI and quantum: What's coming and why it matters now

04 Six Predictions — how PCI DSS and the QSA evolve from here

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Part 01
Where It All Began

2002–2006: The Pre-Council Era and the Birth of PCI DSS



Before the Standard, There Was Chaos

Three catalysts that forced the card brands to unite

2002–2004

Shadowcrew

Organised carding forums traded millions of stolen cards. Separate brand programs could not stop syndicates operating at this scale.

February 2003

Payment Processor

Up to 8 million card numbers stolen from a third-party processor. Card Schemes pushed for one rulebook and a firm timeline.

Early 2004

Warehouse Chain

Card data stolen from in-store POS. Full track data was kept long after authorisation, reinforcing the ban on storing SAD.

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Part 02
A Decade of Escalation and Response

2007–2018: Breaches That Changed Everything



The Breaches That Changed Everything

Real organisations, real cardholder data, real consequences

Off-price Retailer (2007) — 45M records. The first mega-breach; wireless network compromise

Global Processor (2008–09) — 134M records. SQL injection at processor scale

Department Store Chain (2013) — 110M records. RAM-scraping malware via an HVAC vendor pivot

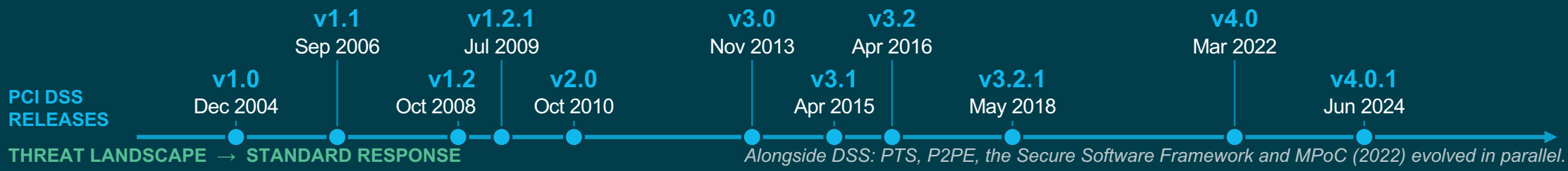
EU Airline (2018) — ~430K cards. The definitive Magecart e-skimming case

APAC Airline (2018) — 9.4M passenger profiles, ~430 cards. The APAC wake-up call on identity data

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Standard Evolution Timeline

The standard has always been reactive to an ever-changing threat landscape



Alongside DSS: PTS, P2PE, the Secure Software Framework and MPoC (2022) evolved in parallel.

v1.1 · 2006
SQL injection & weak credentials
Req 6.6 code review or WAF; Req 6 and 8 hardened

v1.2 · 2008
Wireless cracking (WEP)
WEP banned: no new use after Mar 2009, none after Jun 2010

v2.0 · 2010
CHD sprawl & virtualisation
Data-discovery scoping; virtualisation; risk-ranked vulns

v3.0 · 2013
RAM-scraping & vendor pivot
Pen-test methodology; segmentation testing; service provider duties

v3.0 · 2013
POS skimming & tampering
Req 9.9: inventory and inspect POS devices; train staff

v3.1 · 2015
SSL / early TLS exploits
SSL/early TLS out; due Jun 2016, extended to Jun 2018

v3.2 · 2016
EMV bypass & CNP fraud surge
MFA for non-console admin; TLS 1.0 deprecated

v3.2 · 2016
Weak service provider oversight
Segmentation tests every 6 months; control monitoring

Industry · 2014+
PAN sprawl in merchant systems
Network tokens; RBI bans merchant PAN storage (2021)

v4.0 · 2022
Phishing & credential stuffing
MFA for all CDE access; anti-phishing; 12-char passwords

v4.0 · 2022
Magecart / JS e-skimming
Req 6.4.3 & 11.6.1: script inventory, payment-page integrity

v4.0 / v4.0.1
Ransomware targeting CHD
Targeted risk analysis; authenticated scans; segmentation checks

20 YEARS OF SECURING PAYMENT DATA

Field Reality: 20 Years on the Ground

Observations from patterns that repeat

PCI fatigue — mental exhaustion, operational burnout and compliance drift

No one knows everything — leverage professional expertise or be left behind

“QSA audits of no value whatsoever” — value matches the importance given to it

Do the right thing — it’s a small industry and we all depend on one another

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Part 03
The Modern Threat Era - AI & Quantum

The Threats We Can See — and the Ones We Can’t Yet



AI: The Double-Edged Sword

The AI arms race is re-drawing the battle lines

In attackers' hands:

Hyper-personalised phishing at scale • automated CVE discovery and chaining • deepfake fraud bypassing identity checks • adversarial ML probing fraud models

In defenders' hands:

Real-time behavioural analytics • LLM-assisted threat modelling • natural-language compliance mapping • adaptive fraud scoring without rule changes

Ripple-effect:

Cognitive Offloading and Automation Bias threaten the critical thinking required to stay ahead

The Council has already moved:

AI Assessment Guidelines (Mar 2025), AI Principles incl. agentic AI (Sep 2025)

Since then: new Information Supplement, Security Considerations for AI Systems (press release, 7 Oct 2026)

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Agentic AI: Machine Speed and Trust

Attack speed has outrun human limits; payment networks are responding

IN ATTACKERS' HANDS

Machine-speed operations

~37×

faster operational tempo

- 1,500+ commands per hour, against up to 40 for human operators
- State-backed APT paired an open-source agentic pen-test framework with a frontier reasoning model
- 200+ organisations in 14+ countries; financial services hit hardest

IN ATTACKERS' HANDS

Financial sector case study

9 banks

in one regional hub, over weeks

- Same agentic framework behind the campaign
- Commercial agentic coding assistants plus autonomous recon
- Framework went closed source; regulators and law enforcement investigating

INDUSTRY RESPONSE

Agentic commerce trust layer

Verified intent

for agent-initiated payments

- Network A: cryptographic proof of user intent for each transaction
- Network B: open trusted-agent standard for agent identity and mandate limits
- Goal: close the trust gap before agentic commerce scales

Sources: independent threat intelligence reporting; sector cyber authority and incident response findings; payment network announcements (2026)

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Quantum I: Harvest Now, Decrypt Later

Adversaries are collecting encrypted payment data today, to decrypt once quantum arrives

What quantum breaks:

Asymmetric - RSA and ECC public-key encryption, TLS handshakes, HSM key wrapping — Shor's Algorithm defeats RSA-2048 in hours to days, not years

What it weakens:

Symmetric crypto at risk? Grover's Algorithm halves effective key length — e.g. AES-128 falls to ~64-bit and is migration-bound; AES-256 keeps a 128-bit post-quantum margin. Thus, the **asymmetric** layer is the emergency

The timeline is accelerating: Q-Day estimates are moving earlier

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Quantum Reality Check: A Builder's View

Diraq, a Sydney silicon-quantum builder, on timelines, hardware and Q-Day

TODAY

8 qubits

Diraq's silicon CMOS chip, running in a Sydney data centre

2029 TARGET

150K qubits

Physical qubits, giving ~1,000 logical. Best published RSA-2048 estimate: ~1,400 logical, <1M physical (2025)

2031 TARGET

Utility scale

Fault-tolerant machine whose output is worth more than its running cost

Q-Day will be gradual

Early machines may take weeks or months per key. Checking a cracked key is instant; each new key needs its own long run, so mass decryption builds slowly.

Silicon is a contender

CMOS-based silicon-spin chips are energy-efficient and use standard chip manufacturing. Rivals face cost, complexity and energy limits.

Expect no warning

Well-funded nation-states could reach utility scale unnoticed. Four vendors, including Diraq, have qualified for DARPA Stage C verification.



Image: Diraq

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Quantum II: The Post-Quantum Response

The standards exist and the Council has made its first move — certified hardware is the missing piece

NIST PQC standards (Aug 2024): ML-KEM / FIPS 203, ML-DSA / FIPS 204, SLH-DSA / FIPS 205; HQC added Mar 2025, FIPS due 2027

The hardware gap: no payment-ecosystem HSM vendor yet holds FIPS 140-3 Level 3 validation including these algorithms — earliest window 2027

Crypto inventory is now mandatory: Requirement 12.3.3 fully enforceable since 31 March 2025 — QSAs are running second-cycle reviews

PTS HSM v5.0 (May 2026): the Council's first formal PQC move — the HSM standard now embeds post-quantum considerations and a 128-bit minimum key strength for device security (no TDES)

Regulatory pressure is external too: US Executive Order on PQC signed June 2026; DSS-level PQC migration guidance still pending

Act now: two-track strategy — non-production PQC testing today, certified migration when validations land; HSM vendor conversations this year

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Part 04
Six Predictions

What the Next Decade Demands From Practitioners and Standards Alike



Predictions: The Near Horizon

One of these has already started coming true

1. AI governance: guidance to requirement (brands 2026–27; PCI DSS 2028+). Card brand rules bind agentic payments first; native DSS controls follow

2. Continuous evidence, periodic attestation (2026–27). Evidence is collected automatically all year; the AoC stays a point-in-time sign-off

3. PCI PQC guidance issued (2027–28). 12.3.3 inventories and the June 2026 Executive Order force a formal migration roadmap

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Predictions: The Far Horizon

Where the standard — and the profession — land by 2030

4. Regulatory harmonisation (2028–30). Regulators keep their own rules; cross-trained QSAs map them into one control set

5. The customised approach splits the market (2030+). Tech-native firms adopt it; many merchants stay with the defined approach

6. The abstracted CDE — and the evolving QSA (2030+). Scope moves from the PAN to tokens, APIs and AI agent authority; the QSA becomes a systems auditor

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Three Key Takeaways

What to carry out of this room

1. Meet the intent and the rigour, and the Standard protects you. In 20 years, no breached company we investigated was compliant at the time – and none of the companies applied the Standard were breached

2. Speed is the new threat, so the basics matter more. AI agents attack at machine speed, so small gaps are found within hours. Keep the basics tight, monitor continually, and keep people exercising judgement

3. The quantum clock is already running. Payment data stolen today can be decrypted later. Your 12.3.3 inventory shows where you're exposed, so start there

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Thank You

Parting thought…

“The Standard evolves because threats evolve. After 20 years, the one constant remains: the attackers never stop.”

PCI SSC Community Meeting — Asia-Pacific | 2026

20 YEARS OF SECURING PAYMENT DATA