

European
Community Meeting

EDINBURGH | 2026



The Checkout Blind Spot: Payment-Frame Risk in Retail

PRESENTED BY

reflectiz

Isaac Moddel

VP Sales, EMEA & APAC, Reflectiz



Isaac works with payment providers, QSAs and merchant security teams across EMEA and APAC on third-party and supply-chain script risk, and contributed to the research behind the State of Web Exposure 2026 study referenced in this session.

Agenda

- About the Data: 4,700 sites, 12 months
- The 2026 Headline: A Surge in Unjustified Apps on Payment Pages
- Why the Payment Frame: PCI DSS v4.x requirements 6.4.3 and 11.6.1
- Inside the Payment Frame & the Volume Illusion
- Benchmark by Vertical and Shadow Code risk
- The Priority-Action Gap & What Good Looks Like
- Take It Home: the 5-step checkout audit
- Key Takeaways

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

ABOUT THE DATA

How this study was built

Findings come from the State of Web Exposure 2026 study: 4,700 leading websites across 10 industries, monitored continuously for 12 months.

Scripts, pixels and tags were observed executing in the live browser — the consumer's vantage point — rather than inferred from code repositories.

A separate “leaders” cohort of 429 sites was benchmarked against 8 hygiene metrics.

Study by Reflectiz. All figures in this session are from this dataset unless noted.

THE 2026 HEADLINE

A Surge in Unjustified Third-Party Apps on Checkout Pages Despite Cleanup Efforts

-40%

Apps in payment frames — average fell from ~7.5 to ~4.5 per site.

47%

Unjustified at checkout — up from 36%, no business reason to be there.

8%

Deploy client-side protection — on payment pages, across the whole study.

Retail proves the paradox: apps per site fell 29% — yet the share of retail sites with third-party code in the payment frame rose from 10% to 14%.

WHY THE PAYMENT FRAME

Every script by the card field must be inventoried — and justified

"Unjustified" = a script present in the payment frame with no business reason to be there. PCI DSS v4.x makes finding and explaining these mandatory.

6.4.3

Manage payment-page scripts

Authorize every script, assure its integrity, and keep a written inventory with a justification for each one.

11.6.1

Detect unauthorized change

Monitor the payment page for tampering and unexpected script changes — and alert when the HTTP headers or content shift.

INSIDE THE PAYMENT FRAME

What's actually running next to the card field

CATEGORY	2024	2025
Advertising analytics	10%	**13%**
General analytics	15%	**11%**
Tag-management platforms	9%	**9%**
E-commerce platforms	2%	**7%**
Social-media pixels	5%	**4%**
Total unjustified	36%	**47%**

TOP NAMED OFFENDERS

Google Tag Manager 5%
Shopify 5%
Google Analytics 2%
Facebook Pixel 2%
TikTok Pixel 1%

Unjustified presence in payment frames — share of all payment-frame apps. Marketing tooling — not payment tooling — dominates the checkout frame. PCI DSS v4.x requires everyone to be inventoried and justified.

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

THE VOLUME ILLUSION

Volume fell. Reach grew.

Averages hide the story: fewer apps per site, but sitting on more sites than before.

WHAT WENT DOWN

7.5 → 4.5 apps/site

Average apps in the payment frame — a 40% cut across the study.

-29% apps per site in online retail specifically.

WHAT WENT UP

10% → 14%

Share of retail sites with third-party code inside the payment frame.

+6pp Finance, +11pp Travel, +12pp Government.

BENCHMARK BY VERTICAL

Where does your sector stand?

Third-party apps running in payment frames — average per site, 2025.

Leader benchmark: ≤2 apps per site in the payment frame.

Only Healthcare and Education clear it. Government runs +70% the wrong way, ~5 → 8.5 apps.



20 YEARS OF SECURING PAYMENT DATA

SHADOW CODE

The code you never approved

A tag manager loads a vendor, which loads another vendor — fourth-party chains executing on your page that no one authorized and no repo shows.

15%

of improper PII access now flows through tag managers.

39%

of public-CDN loads are cloud services you don't control.

3.8×

more often, recently-registered domains appear on compromised sites — the strongest single predictor we found.

Case in point: the Polyfill.io supply-chain attack reached 100,000+ sites through exactly this path.

Polyfill.io: Sansec, June 2024 — 100,000+ sites affected.

SURVEY · 128 SECURITY LEADERS

Feared more than the cause

95% at organizations with 1,000+ employees

81 / 39

The priority-action gap. 81% rank web attacks a top priority — but only 39% own a dedicated solution.

Last

Skimming ranks last — behind breaches and compliance violations. The penalty is feared more than the cause.

24%

Rely on general security tools that cannot see what executes in the browser.

43%

Of third-party risk originates in Marketing & Digital — Marketing alone (26%) outweighs IT (18%).

Survey: n=128 security leaders; 95% at organizations with 1,000+ employees.

WHAT GOOD LOOKS LIKE

Leaders aren't exotic — they're measured

METRIC	LEADERS	STUDY AVERAGE
Apps in payment frames	**< 2**	5–8
Justified payment-frame apps	**100%**	40–60%
Third-party apps (total)	**< 8**	15–25
External domain connections	**< 18**	30–50
Apps accessing PII	**< 1**	2–4

1

1 of the 429 sites in the leaders analysis met all 8 benchmarks (5 shown here).

Just 18% fully justified their payment-frame apps.

20 YEARS OF SECURING PAYMENT DATA PCI Security Standards Council

TAKE IT HOME

The 5-step checkout audit

What you can measure your own checkout against this week.

1. Inventory every script executing on the payment page — from the browser, not the repo.
2. Name a business owner and justification for each one; remove what fails.
3. Expand the tag-manager container to its fourth-party children.
4. Flag public-CDN loads and recently-registered domains as high priority.
5. Monitor continuously — the inventory changes without a release.

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Key Takeaways
You Can't Justify What You Can't See



- Cleanup is real, but unjustified presence at checkout grew from 36% to 47% year over year.
- Marketing tooling, not payment tooling, dominates the payment frame.
- PCI DSS v4.x (6.4.3 and 11.6.1) makes justification a requirement, not a nice-to-have.
- Benchmark your own checkout against the leader numbers this week.
- Data: State of Web Exposure 2026 (Reflectiz) — 4,700 sites, 10 industries, 12 months.

Thank You

Questions? Visit Reflectiz booth #6

Scan to download the full report

reflectiz.com/learning-hub/web-exposure-2026-research

State of Web Exposure 2026 — 4,700 sites, 10 industries, 12 months.