CYBEXIS

WHITE PAPER | PAYMENT SECURITY

Securing Payment Ecosystems in an Era of Advancing Technology

How agentic commerce, front-end attacks, real-time payments and post-quantum cryptography are reshaping payment risk, and what to prioritise

October 2026

Clarity in complexity. Confidence in every decision.

At a glance

- UK payment fraud losses reached £1.28 billion in 2025, with authorised push payment (APP) fraud up 19% to £576.4 million as criminals target people rather than systems.
- Front-end attacks on checkout pages remain persistent and inventive, now hiding skimmers behind trusted services such as tag managers and payment APIs.
- AI agents are starting to make purchases on consumers' behalf. Card networks have launched agent authentication frameworks, but merchants must still decide how much to trust an agent-initiated transaction.
- Scope reduction, third-party oversight, script integrity and crypto agility are the four priorities that protect both compliance and customers as the ecosystem changes.

Who this is for: Payment, fraud and security leaders at merchants, payment service providers, fintechs and service providers handling cardholder or account-to-account payments.

Information correct as of October 2026. Free to share with attribution to Cybexis.

1. A payment ecosystem under pressure

Payments have never been more distributed. A single online purchase may now involve a merchant website, a dozen third-party scripts, a hosted payment page, a gateway, an acquirer, a token service, a 3-D Secure server, a fraud engine and, increasingly, an AI agent acting for the customer. Each link is an opportunity for an attacker, and each sits with a different organisation.

The fraud data shows where criminals are concentrating. UK Finance's Annual Fraud Report 2026 recorded **£1.28 billion** stolen through payment fraud in 2025, up 4%, with a record 4.06 million confirmed cases. Unauthorised fraud accounted for £703.4 million, while **APP fraud rose 19% to £576.4 million**. Two-thirds of APP cases began online and a further 17% through telecommunications [1][2]. Banks are getting better at stopping unauthorised transactions, so attackers are shifting to persuading victims to pay them directly, using increasingly convincing AI-generated content.

Meanwhile, attacks on the payment journey itself continue. In January 2026 researchers exposed a web-skimming network active since at least 2022 that targeted checkout pages accepting six major card brands [3]. In June 2026 another campaign was found injecting a skimmer through Google Tag Manager on Magento and Adobe Commerce stores and using a legitimate payment provider's API to store stolen card data, so that exfiltration blended into normal traffic [4].

2. Technologies reshaping payment risk

Agentic commerce

AI agents that search, compare and buy on a consumer's behalf moved from concept to pilot in 2025 and into early production in 2026. Visa launched its Trusted Agent Protocol in October 2025, using cryptographic signatures to let merchants verify an agent and its intent, and Mastercard has introduced Agent Pay with an acceptance framework built on tokenisation and strong authentication [5][6]. Large processors announced support for both in 2026 [7], and the PCI Security Standards Council's 2026 community meeting included sessions on attack surfaces in agentic payment flows and whether PCI DSS requirements apply differently to agents [8].

The security questions are new: how a merchant distinguishes a legitimate agent from a malicious bot, how consumer intent and spending limits are bound to a credential, who is liable when an agent is manipulated by a prompt injection on a product page, and how disputes are evidenced when no human clicked "pay".

Real-time and account-to-account payments

Faster Payments, open banking and variable recurring payments make money movement instant and irrevocable. That is good for customers and for criminals. The UK's mandatory APP reimbursement regime, in force since October 2024 with a cap of £85,000 per claim, has shifted cost onto payment service providers and sharpened incentives for real-time behavioural fraud detection and confirmation-of-payee controls. Regulatory oversight is also changing as the Payment Systems Regulator's functions are consolidated into the FCA.

Tokenisation, passkeys and new acceptance channels

Network tokens, device-bound wallets and passkeys are reducing the value of stolen card numbers and passwords. Software-based acceptance on commercial phones (PCI MPoC) is bringing card acceptance to small merchants without dedicated terminals. These are net positives, but they move risk rather than remove it: towards token provisioning and account takeover, device integrity and the identity checks that bind a token to a person.

AI on both sides of the fraud equation

Attackers use generative AI for synthetic identities, deepfake voice in impersonation scams and automated testing of stolen cards. Defenders use machine learning for transaction scoring and behavioural biometrics. The advantage goes to whoever iterates faster, which favours organisations that bring fraud, security and data teams together.

Post-quantum cryptography

Payments rely heavily on public-key cryptography for TLS, card authentication, key exchange and token services. The NCSC has set out a migration timeline: discovery and planning by 2028, priority migrations by 2031, and completion by 2035. Payment hardware and schemes have long replacement cycles, so organisations need to understand where cryptography sits in their estate now, even though the threat is not yet immediate.

3. The compliance baseline: PCI DSS v4.0.1 and beyond

Since 31 March 2025 all of the future-dated requirements in PCI DSS v4.0.1 have been mandatory. Several respond directly to the threats above:

Requirement	What it addresses	Common implementation gap
6.4.3	Inventory, authorisation and integrity of scripts on payment pages	Tag managers and marketing scripts added outside change control; no justification recorded per script
11.6.1	Detection of unauthorised changes to payment page content and HTTP headers	Monitoring checks only the merchant's own server, not what the browser actually loads
8.4.2	MFA for all access into the cardholder data environment	Service and break-glass accounts excluded; MFA not phishing-resistant
12.5.2	Scope confirmed at least annually and on significant change	New integrations, agents or cloud services not reflected in scope
12.8 / 12.9	Management of third-party service providers and responsibility matrices	Contracts and attestations not mapped to specific requirements; no ongoing monitoring
5.4.1 / 12.6.3.1	Anti-phishing mechanisms and awareness of phishing and social engineering	Training not updated for deepfake and AI-assisted pretexting

Table 1. PCI DSS v4.0.1 requirements most relevant to current threats.

The Council has signalled continued evolution: an e-commerce guidance task force on implementing the newest requirements, possible alignment of 3-D Secure core requirements into PCI DSS, consolidation of mobile acceptance standards under MPoC, and guidance on AI in assessments [9]. AI is not yet codified in PCI DSS, but assessors increasingly expect governance and control design around any AI that touches payment data or decisions.

> **Compliance is the floor**
>
> PCI DSS defines a minimum for protecting card data. It does not address APP fraud, agent manipulation or operational resilience across the wider payment chain. Organisations that treat a clean Report on Compliance as the end state tend to be surprised by the attacks that matter most to their customers.

4. Key challenges

- **Fragmented accountability.** Responsibility for a single transaction is split across merchants, service providers and schemes. Gaps appear at the handoffs, particularly in responsibility matrices that were never revisited after a platform change.
- **The browser is outside your control.** Skimmers run in the customer's browser, beyond server-side controls. Even merchants using iframes or hosted fields can be exposed if the parent page is compromised.
- **Trusting non-human customers.** Existing fraud models assume a person at a device. Agentic transactions break signals such as device fingerprinting and behavioural biometrics, while legitimate agents may look like bots.

- **Fraud and security in separate silos.** APP fraud, account takeover and data breaches share root causes but are often owned by different teams with different tools and metrics.
- **Legacy cryptography and hardware.** Terminals, HSMs and scheme interfaces have long lifecycles, making crypto agility slow and expensive.
- **Scope creep.** New integrations, analytics and AI services can quietly pull systems into the cardholder data environment.

5. Priorities

1. **Reduce scope deliberately.** Use network tokenisation, hosted payment pages or validated P2PE so that as few of your systems as possible ever see card data. Revalidate scope whenever architecture changes.
2. **Control what runs on payment pages.** Maintain an authorised script inventory, enforce a strict Content Security Policy and Subresource Integrity, remove tag managers from payment pages, and use client-side monitoring that sees what the browser loads.
3. **Map and monitor the third-party chain.** Maintain a living responsibility matrix for each service provider, link it to contract clauses, and monitor providers continuously rather than relying on annual attestations.
4. **Prepare for agent-initiated payments.** Decide your policy now: which agent protocols you will accept, what verification and spending limits apply, how intent is captured, and how you will evidence disputes. Threat model product and checkout pages for prompt injection targeted at shopping agents.
5. **Converge fraud and security operations.** Share intelligence, telemetry and incident playbooks between fraud and cyber teams, particularly for account takeover, mule activity and impersonation scams.
6. **Harden human processes against AI-enabled deception.** Out-of-band verification for payment changes and refunds, phishing-resistant MFA for staff with payment authority, and updated training on deepfakes.
7. **Start the cryptographic inventory.** Identify where public-key cryptography is used across payment flows, which components are hardware-bound, and what your providers' post-quantum roadmaps are.
8. **Test resilience across the chain.** Exercise the failure of a key provider, a skimming incident and a mass APP scam campaign, including customer communications and regulator notification.

Technology	Opportunity	Primary risk	First control to put in place
Agentic commerce	Conversion, convenience	Manipulated or impersonated agents	Verified agent protocols with scoped, tokenised credentials
Real-time A2A payments	Speed, lower cost	Irrevocable APP fraud	Behavioural risk scoring and payee confirmation
Network tokens and passkeys	Lower card-not-present fraud	Account takeover at provisioning	Strong identity checks on enrolment
Software POS (MPoC)	Cheap acceptance	Device compromise	Validated MPoC solutions and attestation
AI fraud analytics	Better detection	Model evasion and bias	Monitored models with human review of edge cases
Post-quantum cryptography	Long-term confidentiality	Delayed, costly migration	Cryptographic inventory and vendor roadmaps

Table 2. Advancing payment technologies at a glance.

The payment ecosystem is becoming faster, more automated and more interconnected, and the attackers who target it are following the same path. The organisations that will cope best are those that keep card data out of their environments wherever possible, take ownership of the customer-facing edge they cannot fully control, and treat fraud, security and resilience as one problem rather than three.

About Cybexis

Cybexis is an independent UK cyber security advisory, assurance and risk management practice based in Reading. Its insights series shares practitioner perspectives on the frameworks, regulation and threats facing regulated and high-risk organisations. www.cybexis.co.uk | hello@cybexis.co.uk

This paper is for general information only and does not constitute legal or regulatory advice. Requirements, deadlines and threat activity change; always confirm current obligations with your regulator, contracting authority or certification body.

Sources and further reading

[1] UK Finance, Annual Fraud Report 2026. https://www.ukfinance.org.uk/system/files/2026-06/UK%20Finance%20Fraud%20Report%202026.pdf

[2] Payment Expert, UK Finance: fraud losses hit £1.28bn as criminals exploit human trust (June 2026). https://paymentexpert.com/2026/06/15/uk-finance-fraud-report-2026/

[3] Malwarebytes, Online shoppers at risk as Magecart skimming hits major payment networks (Jan 2026). https://www.malwarebytes.com/blog/news/2026/01/online-shoppers-at-risk-as-magecart-skimming-hits-major-payment-networks

[4] ThreatCluster, Magecart campaign exploits Stripe for credit card theft (summary of Sansec research, June 2026). https://threatcluster.io/cluster/magecart-campaign-exploits-stripe-for-credit-card-theft-001a0df6

[5] eCommerceNews, Visa expands AI commerce framework with new security protocols (Nov 2025). https://ecommercenews.co.nz/story/visa-expands-ai-commerce-framework-with-new-security-protocols

[6] AiNews, Visa and Mastercard launch AI agent payments. https://www.ainews.com/p/visa-and-mastercard-launch-ai-agent-payments-for-smarter-commerce

[7] Digital Transactions, Fiserv adopts agentic commerce protocols from Visa and Mastercard (June 2026). https://www.digitaltransactions.net/fiserv-adopts-agentic-commerce-protocols-from-visa-and-mastercard/

[8] PCI SSC, Council celebrates 20 years at North America Community Meeting (Aug 2026). https://www.pcisecuritystandards.org/about_us/press_releases/pci-security-standards-council-celebrates-20-years-brings-north-america-community-meeting-to-vancouver/

[9] CompliancePoint, What PCI SSC's 2025 Annual Report means for our clients. https://www.compliancepoint.com/assurance/what-pci-sscs-2025-annual-report-means-for-our-clients-a-qsa-perspective/