

Post event report



PCI London

21st January 2026, London

Strategic Sponsors



Education Seminar Sponsors



Networking Sponsors



Branding Sponsors



Executive Roundtable Sponsors



Inside this report:

Sponsors
Key themes
Who attended?
Speakers
Agenda
Education Seminars

Key themes

- Tackling PCI DSS v4.0's new requirements
- Aligning PCI with broader security frameworks
- From point-in-time to continuous compliance
- Reducing the cost of PCI DSS compliance
- New challenges in managing third-party risks
- Technology challenges in hybrid environments
- New technologies – a challenge to compliance?
- Automation, AI & continuous assurance
- Aligning PCI DSS, GDPR and broader GRC efforts
- Securing Cloud and other critical third-party dependencies
- Vulnerability management and remediation
- Technology investment decisions are getting harder

Who attended?



Speakers

- Simon Arazi, VP of Product
Reflectiz
- Tim Ayling,
VP EMEA Cyber Security Specialists
Thales
- John Bartholomew,
Senior VP, Strategic Relationships
SecurityMetrics
- Daniel Bond, Account Executive,
Payments & Fraud – EMEA
HUMAN Security
- Gareth Bowker, PCI Technical Advisor,
Jscrambler
- Katie Cowman,
Senior PCI Assurance Manager
Barclaycard
- Úna Dillon, Regional Director Europe
PCI Security Standards Council
- Jason Donegan,
Chief Operating Officer
ComplyB4
- Adaora Ezennia, GRC Lead
THG PLC
- Michelle Griffey, GRC Director
Paragon
- Mohamed Inshaff,
Principal
Sales Engineer, EMEA
HUMAN Security
- Muhammad Emal Khan,
Senior Information Security Consultant
Lidl
- Parminder Lall, CEO and Founder
1 Cyber Valley
- Carol Lloyd,
PCI Compliance Consultant
Stonegate Group
- Kris Olejniczak, CEO
Patronusec
- James Richardson,
Information Security Officer
Specsavers
- Matt Taylor,
Head of Solution Consulting,
IP Integration
- Ronak Topiwala, Global Information
Security GRC Lead
Checkout.com
- Simon Turner, Head of Security
Governance and Compliance
BT Group
- Jo Vane, Director – Information Security
Checkout.com

Agenda		
08:30	Breakfast & networking break	
09:30	Chairman's welcome	
09:40	What's new in PCI security: Updates and insights from the Council Úna Dillon , Regional Director Europe, PCI Security Standards Council <ul style="list-style-type: none"> The PCI Council's latest initiatives and effective ways to engage with the Council Recent updates to the PCI Security Standards and how they impact your compliance strategy 	
10:00	Beyond compliance: Protecting the payment journey in a machine-driven world Daniel Bond , Account Executive, Payments & Fraud – EMEA, HUMAN Security; Mohamed Inshaff , Principal Sales Engineer, EMEA, HUMAN Security <ul style="list-style-type: none"> The rise of agentic AI and its implications for payment security Why protecting payments now requires a zero-trust approach built on continuous visibility and verified intent What recent third-party platform abuse reveals about modern payment-journey risk 	
10:20	Education Seminars Session 1	
	IP Integration The art of the possible: Why forcing customers to change channel to pay is breaking your CX Matt Taylor , Head of Solution Consulting, IP Integration	Reflectiz The next wave: How AI will reshape retail security threats Simon Arazi , VP of Product, Reflectiz
		SecurityMetrics The uncomfortable truth about e-commerce payment security & PCI 4.0 compliance John Bartholomew , Senior VP, Strategic Relationships, SecurityMetrics
11:00	Networking break	
11:30	The great de-scope: Using tokenisation to slash your PCI DSS burden (a GRC perspective on strategic scope reduction and multi-framework benefits) Adaora Ezennia , GRC Lead, THG PLC <ul style="list-style-type: none"> Strategic scope reduction – How tokenisation slashes PCI requirements from 300+ to dozens by eliminating cardholder data from your environment Multi-framework ROI – Delivering simultaneous compliance benefits across PCI DSS, GDPR data minimisation, and ISO 27001/27701 controls Audit advantage & implementation – Why demonstrating compliance becomes 40–50% faster, plus actionable evaluation framework and next steps 	
11:50	Using an AI assistant to simplify third-party script authorisation for PCI DSS Requirement 6.4.3 Gareth Bowker , PCI Technical Advisor, Jscrambler <ul style="list-style-type: none"> The problem: PCI DSS 6.4.3 requires managing undecipherable third-party scripts that vendors can update without notice – manual review doesn't scale The risk: Single malicious script change could compromise payment data, yet security teams must vouch for code they can't read The solution: Jscrambler's AI-assisted authorisation combines LLM analysis with deterministic checks and behavioural baselines – proving AI can be used safely for security-critical decisions The result: Auditable decision trails that satisfy assessors and transform 'which wire do I cut?' moments into documented, defensible authorisations 	

Agenda

12:10	Beyond the playbook: The Human side of managing major incidents			
	<p>Michelle Griffey, GRC Director, Paragon</p> <ul style="list-style-type: none">From procedure to performance – How to turn documented PCI DSS response plans into confident, real-world action under pressureCollaboration as a control – How cross-functional coordination between IT, compliance, forensics, and business leaders strengthens response effectivenessPreparedness through culture – How regular training and simulations build an instinctive, empowered 'response culture' across the organisation			
12:30	Education Seminars Session 2			
	<p>1 Cyber Valley Choosing a QSA: Life is like a box of assessors – you need to know what you're going to get Parminder Lall, CEO and Founder, 1 Cyber Valley</p>	<p>ComplyB4 How to avoid PCI DSS assessment anxiety Jason Donegan, Chief Operating Officer, ComplyB4</p>	<p>Patronusec From annual panic to continuous control: 5 practical steps to build a continuous PCI DSS compliance model Kris Olejniczak, CEO, Patronusec</p>	<p>Thales Fighting against the AI bot threat Tim Ayling, VP EMEA Cyber Security Specialists, Thales</p>
13:10	Lunch networking break			
14:10	Getting through the PCI audit: Building confidence and compliance			
	<p>Carol Lloyd, PCI Compliance Consultant, Stonegate Group</p> <ul style="list-style-type: none">Demystifying the PCI audit – what auditors expect, key requirements, and how PCI DSS fits into the broader compliance landscapePreparation and readiness – documentation, system evidence, and process reviews to avoid last-minute surprisesWorking with your auditor – effective communication, handling requests, and demonstrating control ownershipBeyond compliance – turning audit outcomes into opportunities to strengthen security posture and reduce risk			
14:30	Third-party management at scale: From compliance burden to business enabler			
	<p>Simon Turner, Head of Security Governance and Compliance, BT Group</p> <ul style="list-style-type: none">Evolving landscape: Understand how changing service delivery models, cloud adoption, and outsourced payment solutions reshape third-party PCI obligationsRisk-based approach: Learn how to categorise suppliers ethically and apply assurance proportional to risk, ensuring PCI DSS controls remain practical and scalableStrengthening governance: Explore how structured governance frameworks, standardised assurance processes, and right-to-audit provisions can drive supplier accountability and consistencyCompliance as a consequence: Discover how embedding PCI DSS into business-as-usual activities transforms compliance from a costly requirement into a driver of trust, resilience, and business value			
14:50	From checkbox to continuous: How PCI DSS 4.0 transforms compliance into living governance			
	<p>Ronak Topiwala, Global Information Security GRC Lead, Checkout.com</p> <ul style="list-style-type: none">Applying the Customised Approach to align PCI controls with real engineering and business outcomesUsing Targeted Risk Analysis to drive smarter, evidence-based security decisionsImplementing Continuous Control Monitoring with real-time data and automationReducing audit fatigue, accelerating delivery, and strengthening organisational trust through outcome-based governance			
15:10	Networking break			
15:40	PANEL DISCUSSION	20 Years of PCI: Powering the next generation of secure payments		
	<p>Simon Turner, Head of Security Governance and Compliance, BT Group (Moderator); James Richardson, Information Security Officer, Specsavers; Jo Vane, Director – Information Security, Checkout.com Katie Cowman, Senior PCI Assurance Manager, Barclaycard; Muhammad Emal Khan, Senior Information Security Consultant, Lidl; Úna Dillon, Regional Director Europe, PCI Security Standards Council</p> <ul style="list-style-type: none">How can PCI requirements stay relevant as payments move into API-driven, serverless, and decentralised systems?Should PCI evolve toward a more outcomes-based or risk-based framework?What role will automation and real-time monitoring play in compliance?The next generation of standards and what the ecosystem needs to thriveWhat industry collaboration looks like in the next 20 years			
16:20	Chairman's closing remarks			
16:30	Drinks reception		17:30 End of conference	

Education Seminars

1 Cyber Valley

Choosing a QSA: Life is like a box of assessors – you need to know what you're going to get

Parminder Lall, CEO and Founder, 1 Cyber Valley

In this presentation, Parminder will explain and describe to the audience what their thought processes should be like when selecting and working with a QSA. When presenting, Parminder will outline what a QSA's job asks of them to deliver, What a QSA is and who in the audience needs a QSA. We believe this is important for the audience to learn further on as PCI may still be seen as a niche in the cybersecurity world. Having done two previous presentations at the AKJ event in past years, we have seen that the audience's experience scale varies at the event and we also want to accommodate for those who have been in the industry for many years, like Parminder. To accommodate for these said individuals, our presentation will be highly interactive, where we will ask them to also provide their input and experience of the matter.

We will also explore 'cost considerations' and how pricing scales vary for all companies looking into PCI DSS QSAs. We feel this is important as it is a barrier we are consistently confronted with in our work and feel the need to justify/clarify what it is we do that requires such costs. This will be highly educational as it is something we deem very important for all involved parties. Parminder will inclusively also discuss the differences between 'Value Added QSAs' and 'Cost Leader QSAs', and how it is important for CISOs to actively discuss which is a better option for themselves when selecting a QSA.

Attendees will learn:

- What is a QSA?
- Who needs a QSA?
- Value-Added QSAs vs Cost Leader QSAs
- Cost considerations
- Tips for when choosing a QSA

ComplyBe4

How to avoid PCI DSS assessment anxiety

Jason Donegan, Chief Operating Officer, ComplyB4

This talk will look at why PCI DSS assessments can feel stressful for both the assessor and assessee. Focusing on PCI DSS v4.0.1 it will explain what can cause this stress, such as unclear boundaries, procrastination, leaving things until the last minute, confusion about what's expected, and other assumptions on both sides and how that plays out during the process.

The goal is to make reviews more efficient, more consistent, and less painful by treating it as something you stay on top of all year, not just a once-a-year scramble and how to remove assessment anxiety.

Attendees will learn:

- Simple and practical ways to make the assessment smoother and easier
- How to prepare early
- How to agree what good looks like
- How to check you're ready and being organised

Education Seminars

IP Integration

The art of the possible: Why forcing customers to change channel to pay is breaking your CX

Matt Taylor, Head of Solution Consulting, IP Integration

For many organisations, customer journeys don't fail at discovery, engagement, or service. They fail at the moment a payment is required. As customer contact strategies expand across voice, digital, automation, AI, and hybrid channels, payments are still too often treated as a separate problem. Customers are asked to change channel, repeat information, or wait while compliance processes catch up. The result is broken journeys, abandoned transactions, and unnecessary friction at the point where trust matters most.

This session explores the art of the possible when PCI compliance is designed to enable customer experience rather than restrict it. Through the lens of Practical Intelligence, we will look at how organisations can embed secure payments directly into the channels customers are already using. Voice agent, IVR, speech, and pay-by-link. Without forcing channel shifts, bolted-on compliance, or fragmented hand-offs. We will challenge a long-standing industry assumption. If a customer has to change channel to pay, the CX design has already failed.

Attendees will see how a modern, channel-agnostic PCI approach allows organisations to payment-enable every customer contact strategy by design. Not as an afterthought. Whether deploying new digital journeys, introducing AI and automation, or modernising voice interactions, payments must be built in from day one. The session will also highlight where organisations typically get stuck today. Where CX ambition collides with regulatory reality. And what 'good' actually looks like as we move into 2026. Practical, scalable, and designed for real-world delivery.

Attendees will learn:

- Understand why channel shifting at the point of payment is one of the biggest hidden causes of CX failure
- Learn how to enable secure payments across voice, IVR, speech, and digital channels without fragmenting the customer journey
- See how Practical Intelligence can be applied to PCI compliance to accelerate CX rather than slow it down
- Identify common design mistakes organisations make when introducing new customer contact channels without payment enablement
- Define what a modern, future-ready PCI payment architecture looks like in 2026

Patronusec

From annual panic to continuous control: 5 practical steps to build a continuous PCI DSS compliance model

Kris Olejniczak, CEO, Patronusec

Continuous compliance is often described as the holy grail of the security and compliance world – widely discussed, frequently promised, but in reality achieved by very few organisations. For many companies, PCI DSS still remains an annual exercise driven by audit pressure rather than a sustainable security operating model. This session demystifies continuous PCI DSS compliance by breaking it down into five practical and achievable steps. Instead of abstract frameworks or theoretical maturity models, the presentation focuses on real-world practices that security and compliance teams can apply immediately within their existing environments.

Attendees will learn:

- Why treating PCI DSS as an annual event creates unnecessary risk, cost, and operational friction
- What 'continuous compliance' really means in the context of PCI DSS 4.x – beyond marketing buzzwords
- What is step 1 in the continuous compliance journey
- What are other 4 actionable steps that you can implement in your organisation to stop experiencing annual panic

Reflectiz

The next wave: How AI will reshape retail security threats

Simon Arazi, VP of Product, Reflectiz

Our presentation, 'The next wave: How AI will reshape retail security threats', will examine the 2026 retail threat landscape, focusing on AI's impact – from personalised shopping to autonomous checkout. We'll highlight how these innovations are creating new security risks and forecast the emerging threats that are currently flying under the radar.

Attendees will learn:

- 2026 web exposure reality check: A data-driven look at today's retail threat landscape
- AI-powered retail – The double-edged sword: How AI is transforming online shopping experiences, from personalised recommendations to autonomous checkout
- Threat forecast – What's coming next: Why these same capabilities are creating a new set of threats currently are off radar

Education Seminars

SecurityMetrics**The uncomfortable truth about e-commerce payment security & PCI 4.0 compliance**

John Bartholomew, Senior VP, Strategic Relationships, SecurityMetrics

In 2020, a new kind of cyber-attack was discovered that targets e-commerce secure payment iframes in a way that hadn't been seen before. There are now multiple successful tactics to circumvent iFrames and their use is growing. Protecting e-commerce data needed an improved security approach. The industry response is PCI DSS 4.0 with new security controls specifically for e-commerce. While the transition to improved e-commerce security has begun, it's far from over and ultimate success as currently functioning may be questionable. Join SecurityMetrics Sr. VP, John Bartholomew as he guides you through the evolving landscape of e-commerce website attacks, what attackers are focusing on in 2026, and how acquirers can help their merchants stay safe. He will also explore some challenging realities of our industry's current approach to protecting e-commerce payment data and how to improve.

Attendees will learn:

- Key attributes of current hacker methodologies
- Challenges for merchants, acquirers and forensics experts
- Key criteria for simplified & effective solutions for 6.4.3 and 11.6.1
- Risk-based practical & realistic options for reducing e-commerce merchant risk

Thales**Fighting against the AI bot threat**

Tim Ayling, VP EMEA Cyber Security Specialists, Thales

In this session, Thales' expert Tim will guide attendees through the dynamic and increasingly complex world of bots and automated threats, focusing on the latest transformations in the cybersecurity landscape. As digital environments grow more sophisticated, so do the tactics deployed by malicious actors seeking to exploit vulnerabilities. Tim will illuminate the ways in which these bad actors are now harnessing artificial intelligence to supercharge their bot attacks, shifting the focus from rudimentary automated scripts to highly adaptive, intelligent threats capable of bypassing traditional defences.

Drawing upon Thales' extensive expertise in advanced security solutions, Tim will dissect recent bot-based threats and showcase the innovative methods attackers now deploy – covering everything from account takeover to fraud and data exfiltration. Through detailed, real-world examples, participants will gain a clear picture of these evolving threats and the practical challenges they pose to organisations of all sizes. Importantly, the session will not only depict the risks but will also equip attendees with actionable strategies and cutting-edge approaches to bolster their defences. Tim will also highlight collaboration opportunities with industry leaders like Thales, illustrating how multilayered security frameworks and threat intelligence sharing are essential for staying resilient.

Attendees will learn:

- In-depth understanding of how AI is revolutionising both bot attacks and defences in today's cyber-landscape
- Practical, real-world strategies for identifying and mitigating advanced, automated threats targeting organisations
- Insights into leveraging Thales solutions to deploy multilayered security frameworks and harness threat intelligence for ongoing protection
- Knowledge of emerging collaboration techniques that strengthen organisational resilience against evolving bot-driven risks