2025
EUROPE
COMMUNITY
MEETING

AI at the Gates:

Stopping Payment Fraud Before it Starts

PCI Security Standards Council

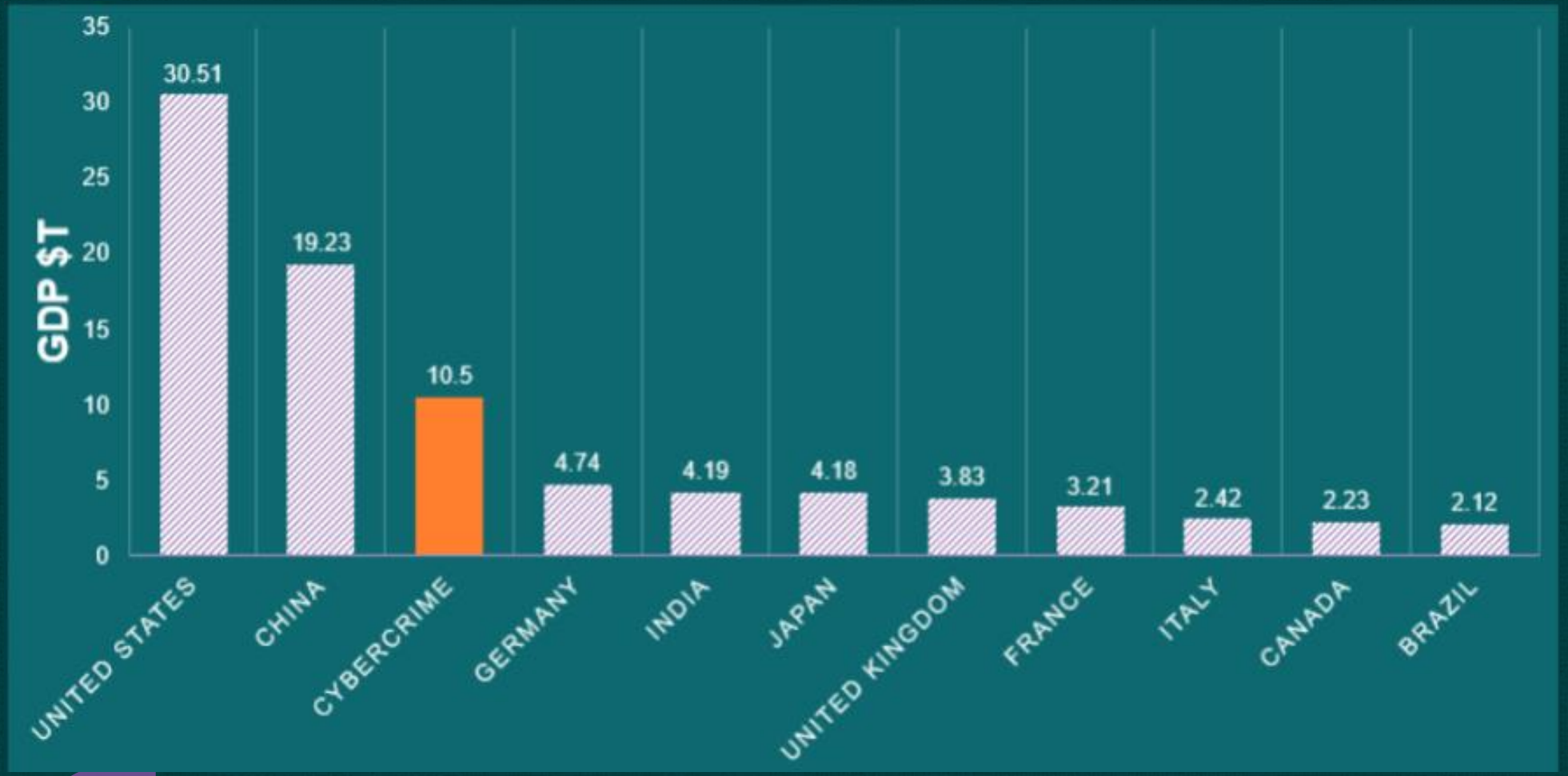
Candice Pressinger

Director Customer Data Security

Elavon Merchant Payment Services Europe

PCI Security Standards Council

World's top 10 economies + Cybercrime



PCI Security Standards Council

Truly organised and very lucrative crime
Well-positioned to take advantage of AI

Cybercrime professionals

New powerful tech and **AI taking fraud to new levels**

Cybercrime Trends

Fraud attempts with deepfakes have increased by **2,137%** over the last three years

The rising tide of bot attacks

Cybercrime costs

Predicted to hit **€11.9 trillion by 2028**.

Equivalent to GDP of world's third-largest economy

Card fraud

Card-based payment fraud transactions expected to reach **€34.5 billion by 2027**

Rising costs

Fraud Losses Hit $11m Per Company as Customer Abuse Soars

Fraud driving higher prices for consumers.

AI boosts organised crime, fraud costs rise, consumers impacted globally

What we see across industry

- Phishing and carding attacks
- Account takeovers and data breaches
- Bot Fighting is never ending
- Fake bookings and chargebacks
- Abuse of loyalty programmes
- Hard to tell fraudsters from good customers

Fraud signals are present throughout the merchant journey
Legacy fraud tools only kick in at checkout, which can be too late

Fraud Prevention Starts Too Late

Legacy systems

Based on the payment transaction

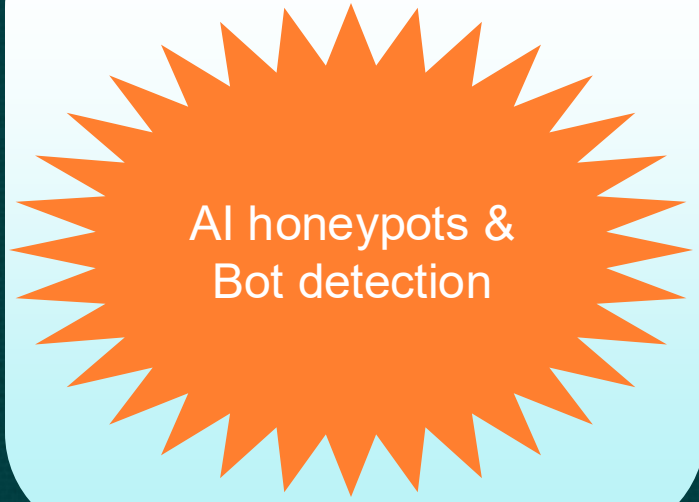
- **Focus on card number**
- Catching obvious fraud scenarios
- Rules based
- Huge manual effort
- Over-reliance on limited blacklists
- Multiple steps for good customers

Next Generation

AI oversight at all steps

- **AI inferences from whole journey**
- Data signals from all interactions
- Finding hidden correlations in data
- Real-time link analysis
- Blocks real fraud
- Frictionless for good customers

Cutting edge

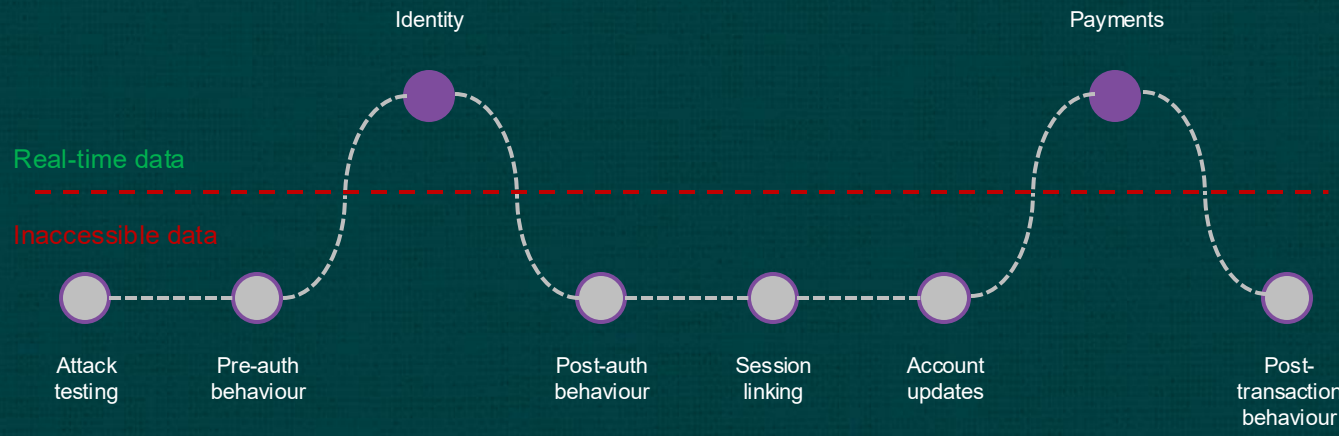


The game has changed. Criminals are using AI to steal high-value data
We need to fight AI fire with AI fire

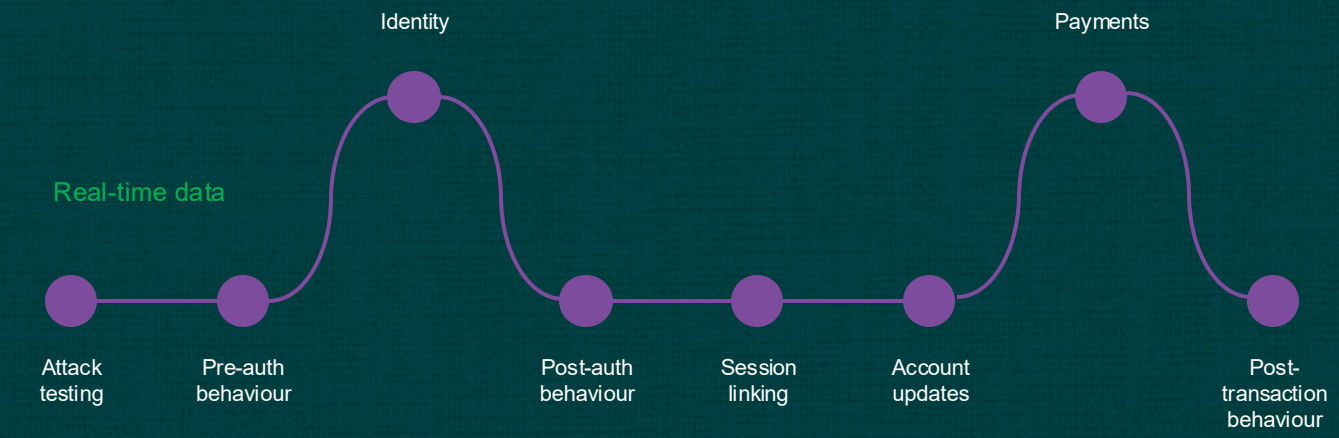
We need to see all the signals

Traditional methods have limited visibility of the wide range of fraud signals available.

Processing is analytical and rule-based.



To stay ahead, we require visibility across the entire range of signals to support AI-powered detection, allowing for fast feedback loops that provide low-latency, real-time corrections.



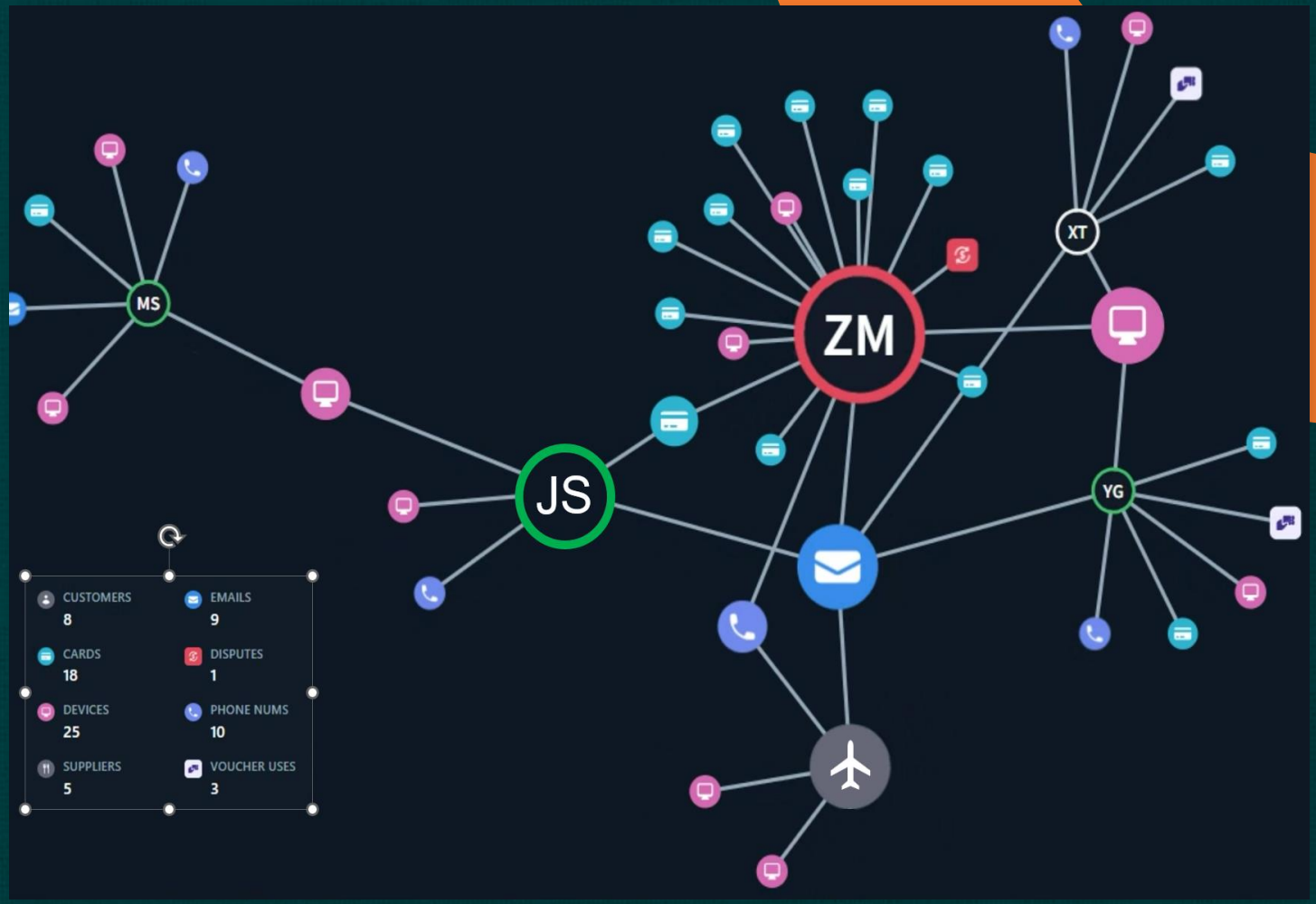
Adapts instantly as fraudsters change their tactics

PCI Security Standards Council

Instant link analysis
(170ms)

Thousand of signals analysed

AI models have access to the latest data and rapidly adapt their behaviours.

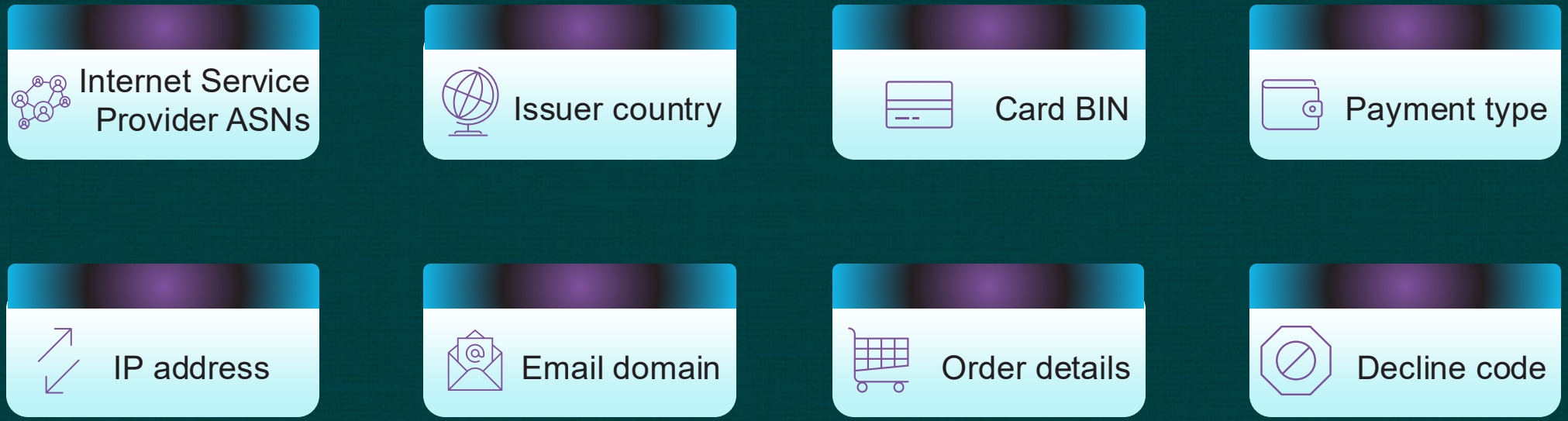


Fraud is web that AI maps instantly

PCI Security Standards Council

Consortium data

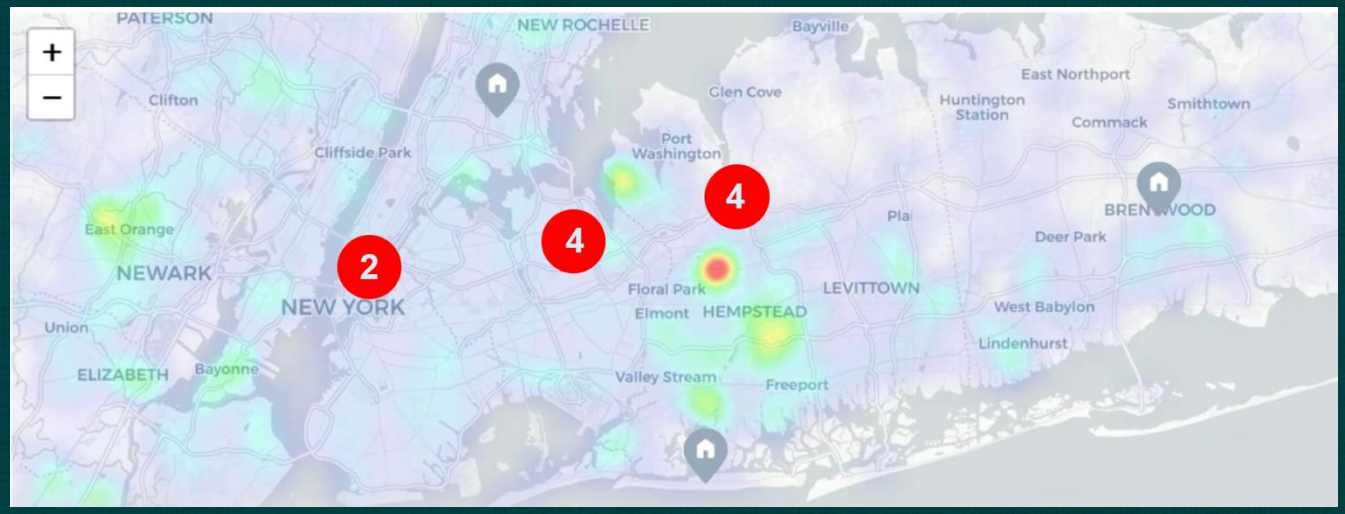
We use consortium data to generate **fraud rate** features. These features represent how much fraud has been associated with a particular entity in the past. These are calculated at **global** level (i.e. using consortium data) and at a **merchant** level.



Consortium data sharing strengthens industry-wide fraud defences

Fraud is both local and global

- Fraud is borderless. Activity can bounce between continents in minutes.
- The same fraud network can test stolen cards in Asia, Europe, and North America in under an hour.
- Fraud hotspots light up in real-time, revealing where criminals are active right now.



Fraud networks operate globally, evading borders and laws

PCI Security Standards Council

False Declines cost merchants more than fraud

- AI-driven fraud detection reduces both fraud losses and operational costs by catching threats earlier and more accurately.
- Advanced AI tools minimise friction for genuine customers while blocking bad actors before they reach checkout.
- Investing in AI means fewer manual reviews and lower false positives, protecting revenue and customer experience.
- The right AI solution balances security and efficiency, ensuring merchants don't sacrifice good customers to stop fraud.

Approve the bad and lose:

$362b

Estimated losses due to Online payment fraud between 2023 to 2028[1].

Decline the good and lose:

$645b

Estimated scope of false decline loss to merchants[2].

Blocking good customers costs twice as much as letting the fraud through

PCI Security Standards Council

Governance, not gloss

- Governance, transparency, and explainability are essential for secure, scalable AI systems.
- The EU AI Act enforces strict rules for high-risk AI in payments and fraud prevention.
- Dual compliance: AI accountability and GDPR compatibility are now mandatory for personal data use.
- Organisations must conduct AI Impact Assessments and Data Protection Impact Assessments.
- Build systems with clear governance, ready for boardroom and courtroom scrutiny.
- Start with governance, embed human oversight, and continuously monitor for model drift.

Boundaries shape trust and truth, Accountable dawn

3 Key Takeaways…

AI is redefining fraud prevention
shifting from static rules to adaptive, self-learning defence

The threat is
Global and always evolving
fraud networks adapt in minutes, so defences must too

Precision matters
as much as protection, reducing false positives protects more revenue than stopping fraud alone

AI is rewriting the rules of fraud, we must adapt or lose

PCI Security Standards Council

Thank you

Bio: As an award-winning Data Security leader at Elavon/U.S Bank, I deliver AI-driven fraud and security solutions. Previously, I secured 80 million transactions annually at BT Group, leading a team of 100 security professionals

LinkedIn: Candice Pressinger | LinkedIn

Blogs: PCI SSC – blog on AI governance

Paving the Way: Inspiring Women in Payments - A Podcast Featuring Candice Pressinger

PCI Security Standards Council®

2025 EUROPE COMMUNITY MEETING