Ian Butler

VP Global Enterprise Product
Elavon Merchant Payment Services

Candice Pressinger

AVP Customer Data Security,
Elavon Merchant Payment Services





20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council



When Machines Start Paying: Securing the Agents!

October 2026

Agenda

Emerging Fraud Challenges

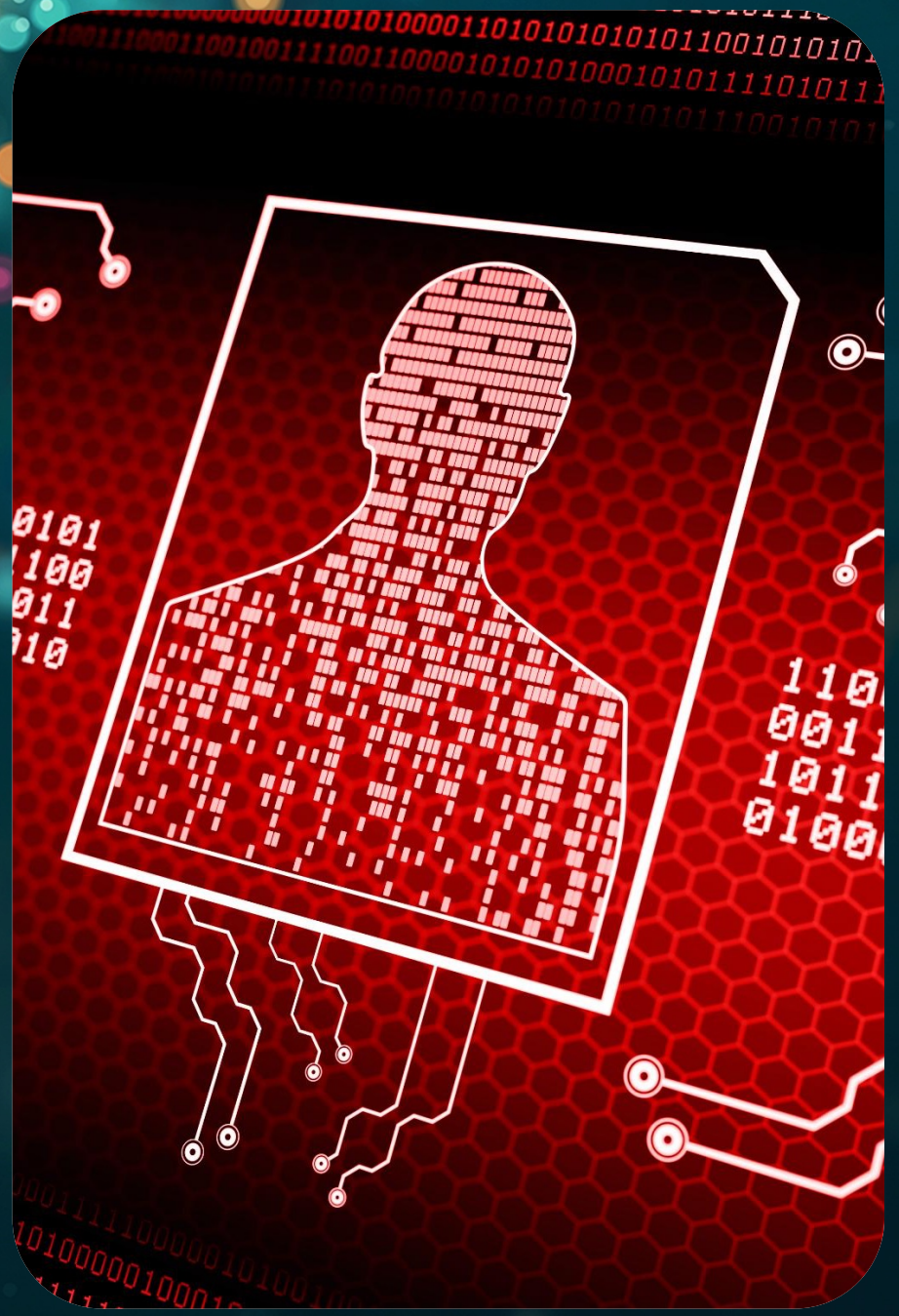
- Fraud now begins before a user enters the transaction flow, increasing security risks.

Evolution of Fraud Prevention

- Previous focus was on stopping fraud at pre-authorisation stages, now shifted earlier.

Importance of Securing Agents

- Machines acting as agents require enhanced security measures to prevent unauthorised activity.



Fraud Has Been Moving Upstream For Years

Each shift made the previous controls less effective.



Post-auth detection	Pre-auth screening	Bot & session controls	Synthetic ID & ATO	Pre-user, machine-driven

Every control layer we built assumed the attacker came later.
That assumption is now wrong.

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

THE DECISION HAS MOVED

Merchants set rules. Agents act. Payments execute.



DECISION LAYER = NEW RISK SURFACE

EXECUTION LAYER = WHAT PCI COVERS TODAY

We’re authenticating execution. Fraud has moved to decisioning.

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

THE ZOMBIE AGENT PROBLEM



The agent is not broken. It's controlled.

Looks legitimate

The host appears clean

Passes controls

Execution checks still succeed

Acts at scale

The decision was already influenced

Fraud doesn't break the system. It controls the decision-maker.

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

BUILT FOR HUMANS. FAILS FOR AGENTS.

You're authenticating the host not the entity controlling it.

CONTROL	HUMAN ASSUMPTION	BREAK IN AGENTIC WORLD
Authentication / SCA	Human present	**No user in loop**
Tokenisation	Credentials are the risk	**Credentials are not the problem**
Behavioural models	Humans act predictably	**Agents act at machine speed**
Velocity / geo checks	Anomaly = fraud	**Normal agent behaviour**

We're authenticating the user, but the user is no longer making the decision

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

From Transactions to Trust Chains

PAYMENT
= Execution

DECISION
= Risk

Fraud becomes a decision problem,
not a payment problem.

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

A New Control Model

Identity. Intent. Behaviour. Execution.

Agent Identity
Who created it? What authority?

Intent + Policy Enforcement
What is it allowed to do?

Continuous Behavioural Validation
Is it still acting in pattern?

Execution Controls (Payments)
Last line of defence.

RISK CONCENTRATES HERE

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Designing For Agent Identity

Agents need first-party identity - not borrowed credentials.

AGENT IDENTITY	LIFECYCLE GOVERNANCE	DELEGATION CHAIN
• Unique, attestable identity	• Provisioning controls	• Who authorised it
• Bound to issuing entity	• Active monitoring	• What scope was granted
• Verifiable at runtime	• Revocation & rotation	• Time-bound expiry

If we can't identify the agent, we can't secure it.

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Intent + Policy Enforcement

What is it allowed to do?

CAPTURE INTENT	DEFINE POLICY	ENFORCE AT RUNTIME
• Digital user mandate	• Scope spend, merchant & time	• Verify agent + mandate
• Bind item, amount & payee	• Issue task-bound credentials	• Allow, deny or step up
• Reject changed checkout	• Step up above limits	• Create signed receipts

A prompt is not a control - bind intent, then enforce it at every step.

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Designing For Continuous Trust

Trust is not a moment. It's a stream.

BASELINE
Behavioural pattern

→

OBSERVE
Continuous signals

→

DETECT DRIFT
Deviation = risk

→

REVOKE / STEP-UP
Real-time response

Behaviour replaces authorisation as the trust signal

Trust decays - it must be re-earned continuously

Drift detection is the new fraud detection

Continuous trust replaces point-in-time authentication.

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Evolution of scope

The actor has changed. The standard hasn't.

PCI SECURES TODAY	PCI DOES NOT YET DEFINE
• Card data	• **Agent identity & lifecycle**
• Transactions	• **Intent and enforcement**
• Storage & transmission	• **Continuous trust and auditability**

Scope must extend from card data → to decision systems.
Without these, we will retrofit controls after the first major failure.

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

THREE ASKS FOR PCI SSC & THE COMMUNITY

Don’t wait for the first major agentic failure to retrofit controls.

01

TREAT AGENTS AS FIRST-PARTY ACTOR

Treat the agent as a controllable participant in the payment trust chain not as a borrowed user credential.

02

EXTEND PCI SCOPE LEFT OF THE PAYMENT

Cover identity, intent, delegation, lifecycle and auditability of automated decisions.

03

ALIGN EARLY ON AGENT TRUST MODELS

Create common language for policy-scoped consent, continuous validation and revocation.

DON’T JUST SECURE THE TRANSACTION.
SECURE THE DECISION.

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

Don’t just secure the transaction.
Secure the decision.