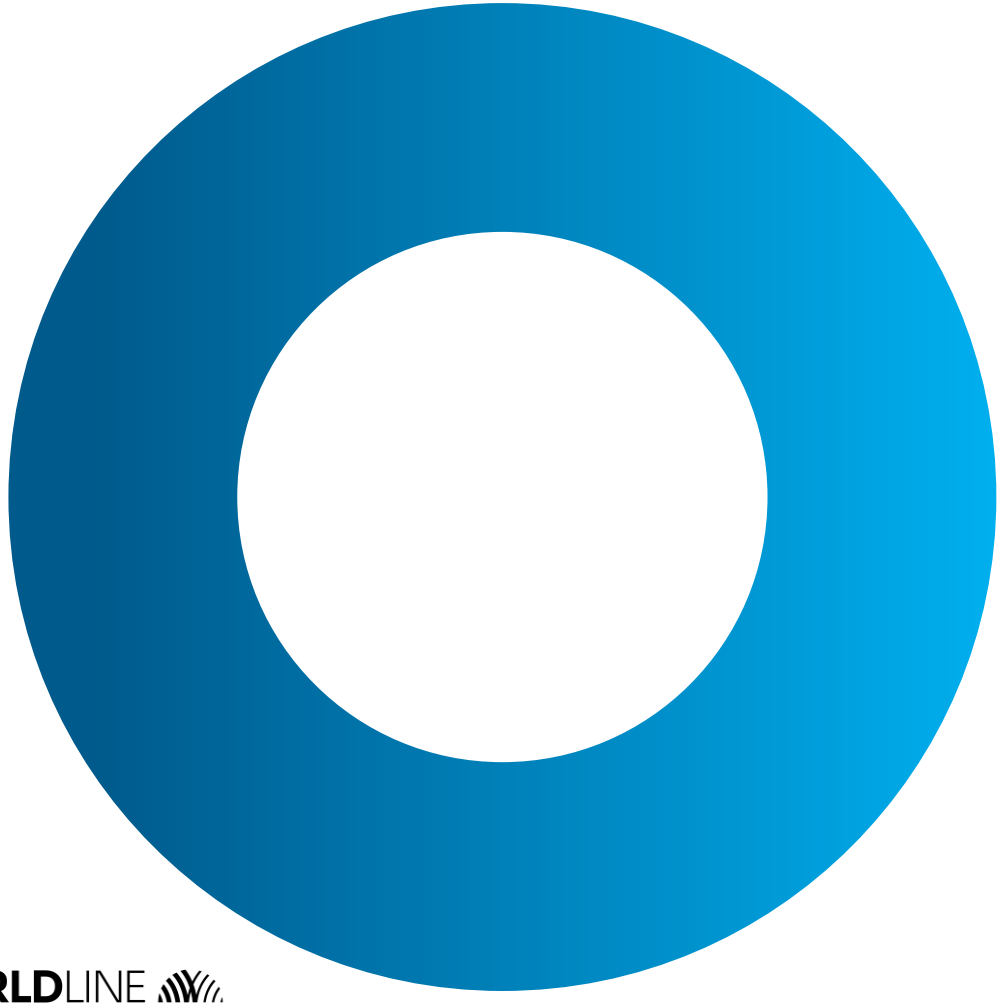

Data-driven defenses for payments

How data analytics, advanced identity verification, and secure payments work together to combat fraud in the evolving digital landscape.

WORLDLINE

The Stakes Have Never Been Higher

28%

of all fraud is now 'sophisticated AI-driven'

Up from 10% in 2024

2.8B+ EUR

projected APP fraud losses by 2027

Instant rails remove intervention windows

10,500+

active Magecart skimming attacks in 2025

23M transactions compromised

200/hr

invalid IDs flagged by banking systems

Identity fraud reaching critical volume

The Threat Landscape

SID

Synthetic Identity Fraud

Fabricated profiles blending real SSNs/IDs with invented data bypass traditional checks. Ghost accounts operate for months before busting out with maximum credit.

APP

Authorized Push Payment (APP) Scams

AI deepfakes and hyper-personalized phishing trick customers into voluntary transfers. Speed of instant rails eliminates intervention windows.

ATO

Account Takeover & Credential Attacks

Autonomous AI fraud agents execute attacks without human input. 10,500+ active Magecart skimming attacks compromised 23M transactions in 2025.

FaaS

Fraud-as-a-Service (FaaS)

Industrialized criminal rings reuse device fingerprints, IPs, and payment routes across banking, crypto, and e-commerce at industrial scale.

Data-Driven Detection Engines

Real-Time AI Risk Scoring

Every transaction scored in milliseconds. Behavioral profiles, device fingerprints, geolocation, and velocity signals fused into a single risk score.

300%
detection lift (Mastercard)

Behavioral Biometrics

Mouse cadence, keystroke timing, swipe pressure silently authenticate users continuously. Fraudsters can steal passwords — they cannot replicate how you type.

60%
false positive reduction (HSBC)

Graph Analytics & Network Detection

Graph neural networks expose criminal rings reusing devices, IPs, and addresses — invisible to rule-based systems. Relationships across accounts reveal hidden patterns.

4,9M EUR
fraud ring unraveled in 2 hours

Cross-Channel FRAML Fusion

Breaking silos between fraud and AML. Unified data across KYC, SAR filings, device IDs, and transaction behavior builds a 360° risk view.

360°
risk intelligence view

Advanced Identity Verification Framework

The evolution of identity

Before	Now
Check once at onboarding	Continuous assurance across lifecycle
Static document-based	Dynamic, behavioral + biometric
Single signal (ID doc)	Multi-layer signal fusion
Human review of edge cases	AI-driven adaptive step-up
Trust until proven otherwise	Zero-trust with risk-proportionate response

Multi-Layer Signal Fusion
Government records + digital footprints + device intel + behavioral biometrics + on-chain reputation

Frictionless Step-Up Auth
Risk proportionate responses — biometrics triggered only for high-risk events. Reduces abandonment.

Deepfake & Forgery Defense
Multi-modal verification (facial + liveness + behavioral) — biometrics alone unreliable by 2026.

Continuous Identity Assurance
Verification throughout the customer lifecycle — not just at onboarding or login.

Future Developments & Emerging Trends

AI NATIVE — 2026

AI-Native Fraud Platforms

Systems where AI autonomously runs detection, decisioning, and continuous learning loops — no human-defined rules. Self-service model development without data science teams.

PRIVACY — 2026-27

Federated Learning

Multiple institutions collaborate on AI training without sharing raw customer data. Intelligence shared industry-wide; personal data stays local. Meets GDPR and PCI constraints.

REGULATORY — 2027

EU Digital Identity Framework

EU Digital Identity launches 2026. Digital IDs combine verified data with behavioral pattern analysis. Compliance becomes competitive advantage, not cost center.

AGENTS — 2028-30

AI Agents & Non-Human Identity

AI agents projected to handle 15–25% of all US e-commerce by 2030. Verifying non-human buyers in automated transactions is the next identity frontier.

ETHICS — 2026+

Explainable AI & Fairness

Regulators require audit trails for every fraud decision. Biased models may wrongly flag demographics. Transparency, fairness, and explainability become table stakes.

Building Your Resilient Defense Framework

01

Fuse Your Signals

Break the silos between fraud, cybersecurity, and AML teams. A unified data layer connecting KYC, device intelligence, behavioral analytics, and transaction history gives you the 360° view that siloed teams will never achieve.

Action: Establish a cross-functional fraud intelligence team and shared data platform.

02

Shift to Continuous Identity

Replace the 'check once, trust forever' model with dynamic identity assurance across the entire customer lifecycle. Behavioral biometrics, step-up authentication, and adaptive risk scoring protect every touchpoint — not just login.

Action: Audit your current identity checkpoints and identify where continuous assurance gaps exist.

03

Treat AI as Core Infrastructure

AI cannot be a bolt-on layer. Organizations that embed ML natively into decisioning — with explainability and bias controls built in — will outpace adversaries who are already using AI offensively.

Action: Define your AI governance framework and prioritize explainable model deployment.

Myles Simpson

myles.simpson@worldline.com

The organizations that succeed

will be those that act now.

Fuse intelligence.

Continuously verify identity.

Embed AI as infrastructure.

Questions?

WORLDLINE

Sources

- Scamwatchhq slide 2
- Intellicheck slide 2
- DataWalk slide 3
- J.P. Morgan slide 3
- Bankcardinternationalgroup slide 4
- IEEE Computer Society slide 4
- Mastercard Slide 7

Other vocabulary

- formjacking