VERTICAL EDITION 05 · SHOPPER, SELLER & RIDER APPS

Stop the order that was never a customer.

Commerce fraud is a margin problem before it is a security problem: promo abuse, refund rings, bots and chargebacks are paid out of contribution margin, and every extra check costs conversion. NonaShield answers a deterministic question before the request leaves the handset — was this exact order produced by the physical device holding the non-exportable key, and has it been altered since? Attestation, RASP, fingerprinting, behavioural intelligence, network defence, risk decisioning and forensic evidence run as one signed pipeline across your shopper, seller and delivery-partner apps.

400+	40+	9	1
Distinct threat vectors monitored across device, network and server	Behavioural vectors profiled per shopping session, continuously	Architectural layers delivered as one cryptographically signed pipeline	Vendor, contract, integration and console — not four or five

IN THIS DOCUMENT

EX 1 The fraud that actually costs a marketplace — eight vectors, and the layer that stops each

EX 2 One platform, nine layers — and only three permitted to make a binary decision

EX 3 Commercial & deployment model — one vendor instead of five, chargeback-ready evidence

HARDWARE ATTESTATION · RASP · FINGERPRINTING · BEHAVIOURAL BIOMETRICS · GRAPH INTELLIGENCE · NETWORK DEFENCE · API GATEWAY · RISK DECISION ENGINE · EVIDENCE & COMPLIANCE

EXHIBIT 1 — EIGHT VECTORS, ONE ARCHITECTURE

The vocabulary is commerce. The question underneath is possession.

Every vector below reduces to the same test: was this request produced by the physical device it claims to come from, by the person entitled to hold it, in an environment that has not been tampered with? The architecture does not change per sector — what changes is the policy set in Layer 7 and the entity model in Layer 5.

VECTOR	HOW IT ARRIVES ON A COMMERCE APP	LAYER
Account takeover & credential stuffing	Breached credential lists replayed at scale against login, saved cards and wallet balances from unattested clients.	**1–3, 7**
Promotion, coupon & referral abuse	Device farms and emulator estates creating accounts in bulk to harvest first-order discounts and referral credit.	**1, 3, 5**
Return, refund & RTO fraud	Serial refund claims and non-delivery disputes staged by clusters sharing device, address and payment markers.	**5, 7**
Card testing & payment fraud	Scripted checkout attempts probing stolen card ranges; loss lands as chargebacks and gateway penalties.	**2, 3, 6**
Cloned & repackaged shopping apps	Fake builds outside official stores harvesting logins, addresses and card data from customers.	**1–3**
Scraping & inventory bots	Headless clients scraping price and stock, hoarding limited drops and denying genuine buyers at launch.	**2, 3, 6**
Seller-account takeover & payout diversion	Seller bank details changed ahead of settlement; marketplace listings hijacked from compromised handsets.	**2, 3, 7**
Delivery-partner & COD collusion	GPS spoofing and app tampering on rider apps, false delivery marking, cash-collection and incentive fraud.	**1, 2, 5**

WHERE CRYPTOGRAPHY IS SILENT — STATED PLAINLY

When a genuine customer on their own device abuses a policy — serial refunds, staged non-delivery — every cryptographic check passes correctly. That case belongs to graph, behavioural and intent analysis (Layers 4–6), which surface repeat-abuse clusters and apply friction only to the affected journey, never to the checkout as a whole.

APPS COVERED ON ONE INTEGRATION

Shopper app, seller and vendor apps, delivery-partner and store-ops apps, wallet and checkout journeys — Android and iOS from one Kotlin Multiplatform SDK. Layers engaged for this vertical: **1–3 and 5–7**, with Layers 8–9 engaged where chargeback and dispute evidence is required.

EXHIBIT 2 — ONE PLATFORM, NINE LAYERS

Six procurements, one signed pipeline — and only three layers may say no.

Device trust, app logic, network gateways, identity, backend controls and forensic chain-of-custody are conventionally six disjointed purchases correlated after the fact. NonaShield delivers them as a single pipeline in which every signal is bound to the same cryptographic assertion at the moment of capture.

BAND A · LAYERS 1–3 **Deterministic device & payload truth**	**1 Mobile SDK** — runtime signal capture, RASP, on-device enforcement **2 API Gateway & Network** — edge enforcement, signed-payload validation on checkout, coupon and seller-payout endpoints **3 Trust Verification** — server-side hardware key attestation	WHAT IT ESTABLISHES Binary authority. These layers may allow or block outright because their error rate justifies it.
BAND B · LAYERS 4–6 **Probabilistic risk enrichment**	**4 Fraud Intelligence** — risk modelling and scoring across entities **5 Graph Intelligence** — entity linkage, abuse-cluster and coordinated-network detection across accounts, addresses and devices **6 Behavioural Intelligence** — continuous interaction and purchase-intent analysis	WHAT IT ESTABLISHES Graded risk only. These layers modulate friction; they never make a binary access decision alone.
BAND C · LAYERS 7–9 **Verdict & accountability**	**7 Decision Engine** — real-time rule and model enforcement: allow / step-up / block **8 Evidence Engine** — hash-chained, tamper-evident immutable record per order, refund and payout **9 Compliance** — regulatory controls, WORM retention, regulator-mapped export	WHAT IT ESTABLISHES One graded, signed verdict — and non-repudiable accountability as a by-product of the transaction path.

DETECT ———▶ ENFORCE ———▶ DECIDE ———▶ HARDENED RULES PUSHED BACK TO THE SDK

THE SEPARATION MATTERS MORE THAN THE COUNT

Most platforms fail not because they lack signals but because they let weak signals make strong decisions. Segregating binary authority (Bands A and C) from probabilistic enrichment (Band B) keeps false positives out of checkout — a blocked genuine order is lost revenue and a lost customer — while still allowing behavioural evidence to add friction the instant a session deviates from its own baseline.

EXHIBIT 3 — POINT SOLUTIONS VERSUS ONE UNIFIED PLATFORM

The stack you would otherwise assemble has four seams.

	FOUR TO FIVE POINT SOLUTIONS	NONASHIELD (UNIFIED)
Vendors to contract & manage	4–5 separate vendors	**1**
Integrations to build & maintain	One per vendor, each with its own SDK and API	**Single SDK + gateway + backend**
Signal correlation across layers	Manual or none — each tool sees only its own slice	**Fused into one explainable risk score**
Threat vectors covered	Varies per tool; gaps at the seams	**400+, continuously correlated**
Compliance & audit evidence	Assembled after the fact from disparate logs	**Native hash-chained evidence, regulator-mapped**
Time to deploy	Sequential vendor onboarding	**A single integration cycle**

DEPLOYMENT

01 Threat-surface review — map your current stack, seams and highest-loss journeys. Two weeks.

02 Pilot — one app, one journey, production checkout flow, measured against existing controls.

03 Production rollout — full journey coverage, policy tuning, evidence chain live for audit.

04 Continuous hardening — detect, enforce, decide, with hardened rules pushed back to the SDK.

COMPLIANCE & ASSURANCE

Aligned to PCI DSS for cardholder data and card-network dispute evidence requirements

ISO 27001, DPDP and RBI payment-security guideline alignment

Five-year WORM retention under compliance lock

Chargeback-defensible, dual-ECDSA-signed transaction evidence

Fail-closed queuing; zero backend exposure on blocked traffic

Post-quantum-ready cryptographic design

WHY DIMEAI

25 years of banking-technology and e-governance security experience behind the architecture

Patent-backed, tamper-evident evidence chain

Explainable ML risk scoring — decisions you can defend to a regulator

Android & iOS from one Kotlin Multiplatform SDK

Cloud, on-premises or hybrid — matched to your infrastructure posture

One commercial relationship, one console, one support line

NONASHIELD · E-COMMERCE & MARKETPLACES

Stop the fraudster. Before the fraud.

contactus@diimeai.com
+91 85917 55427
DIIMEAI.COM