VERTICAL EDITION 07 · UPI, WALLET & NEOBANK APPS

The SIM can be swapped. The key cannot.

A neobank's entire relationship lives on one handset: onboarding, the balance, the limit change and the payout all happen there — and so does the attack. NonaShield answers a deterministic question before the request leaves the handset — was this exact request 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 consumer, merchant and onboarding journeys.

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

IN THIS DOCUMENT

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 fintech. 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 UPI OR WALLET APP	LAYER
Takeover from a second handset	Credentials plus a swapped SIM reproduce the account on a device that was never enrolled — the classic post-SIM-swap takeover.	**1, 3, 7**
UPI collect & mandate abuse	Collect requests and autopay mandates pushed from scripted clients and approved inside a socially engineered session.	**2, 4, 6**
Emulator & device-farm onboarding	Bulk KYC completed on emulators and re-flashed handsets to harvest activation incentives and open mule accounts.	**1, 3, 5**
Deepfake & liveness defeat at video KYC	Injected video streams and replayed selfies presented to the onboarding camera pipeline as a live applicant.	**1, 4, 6**
Mule networks & rapid layering	Funds moved through clusters of freshly opened accounts sharing device, IP and beneficiary markers within minutes.	**5, 7**
Repackaged & cloned fintech apps	Modified builds distributed by link and third-party store, harvesting PINs and UPI credentials under your brand.	**1–3**
API abuse & headless clients	Mobile APIs called outside the app — scripted balance checks, limit probing and payout enumeration at machine speed.	**2, 3**
Chargeback, refund & cashback abuse	Coordinated reversal claims and promotion farming across accounts controlled from the same device estate.	**3, 5, 7**

WHERE CRYPTOGRAPHY IS SILENT — STATED PLAINLY

When a genuine customer, on their own enrolled device, is talked into approving a collect request, every cryptographic check passes correctly — because every check is correct. That case belongs to behavioural baselining and intent analysis (Layers 4–6), which apply friction the instant a session deviates from its own baseline, never to the possession proof. Stating the boundary is part of the architecture.

APPS COVERED ON ONE INTEGRATION

Consumer UPI and wallet apps, neobank and prepaid journeys, merchant and payout apps, onboarding and video-KYC flows — Android and iOS from one Kotlin Multiplatform SDK. Layers engaged for this vertical: **1–9**, with Layer 5 carrying the mule and multi-account entity model.

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

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, mule and coordinated-network detection

6 Behavioural Intelligence — continuous interaction and 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

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 the journey that earns — a blocked genuine UPI payment is an uninstall, not a support ticket — 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 traffic, measured against your 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

NPCI UPI Mobile App Security Framework (MASF) and OC-215A

RBI Directions on Cyber Resilience and Digital Payment Security Controls for non-bank PSOs, 2024

RBI Master Direction on Digital Payment Security Controls, 2021

DPDP Act and Rules 2025 — data minimisation on device-side signal capture

Dual-ECDSA-signed transaction evidence for dispute resolution

Five-year WORM retention under compliance lock; regulator-mapped export

WHY DIMEAI

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

Patent published in India, grant awaited — 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 · FINTECH & NEOBANKING

Stop the fraudster. Before the fraud.

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