VERTICAL EDITION 01 · RETAIL, CORPORATE & PSO APPS

Stop the transfer the customer never meant to make.

Retail banking fraud no longer begins with a stolen credential — it ends with one. A remote-access session, a SIM swapped hours before the OTP, a customer talked through an approval on their own handset — each arrives as a correctly authenticated request. NonaShield answers a deterministic question before the instruction 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 retail, corporate and PSO apps.

400+	40+	9	1
Distinct threat vectors monitored across device, network and server	Behavioural vectors profiled per banking 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 payments. 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 BANKING APP	LAYER
RAT & screen-share takeover	Remote-access and screen-sharing tools driven onto the customer's own handset, authorising transfers from inside a live, genuine session.	**1–3, 6**
SIM swap before OTP release	The number ports to a new SIM hours before a high-value transfer; the OTP lands on a handset the customer never held.	**1, 3, 5, 7**
Authorised push payment fraud	A genuine customer, on a genuine device, talked through an approval by an impersonated caller. Every cryptographic check passes correctly.	**4–7**
Overlay & accessibility abuse	Malicious overlays and accessibility services harvesting PINs and silently confirming beneficiary additions and limit changes.	**1–2**
Credential stuffing & mule onboarding	Breached credential lists replayed at scale; accounts opened in bulk to receive and layer proceeds across the network.	**1, 3, 5**
Cloned & repackaged banking apps	Fake builds distributed outside official stores, harvesting credentials, card data and OTPs from your customers under your brand.	**1–3**
Replay & tampered payment instructions	Beneficiary or amount altered between handset and switch, or a valid instruction re-submitted after settlement.	**2, 3, 8**
Corporate & maker-checker abuse	Bulk-payment files and approvals submitted from compromised, shared or unenrolled corporate handsets.	**1, 3, 7, 8**

WHERE CRYPTOGRAPHY IS SILENT — STATED PLAINLY

When a genuine customer authorises a transfer on their own enrolled device — the talked-through approval — every cryptographic check passes correctly, because every check is correct. That case belongs to behavioural baselining, graph and intent analysis (Layers 4–6), which apply friction the instant a session deviates from its own baseline. Any vendor claiming cryptography alone closes it is describing marketing, not architecture.

APPS COVERED ON ONE INTEGRATION

Retail banking apps, corporate and cash-management apps, UPI and wallet journeys, agent and business-correspondent apps — Android and iOS from one Kotlin Multiplatform SDK. Layers engaged for this vertical: **1–9**, the full pipeline, with Layers 8–9 producing supervisory and dispute evidence by construction.

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 transfer is a contact-centre call and an ombudsman complaint — 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

RBI Master Direction on Digital Payment Security Controls, 2021

RBI Directions on Authentication Mechanisms for Digital Payment Transactions, 2025

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

PCI DSS v4.0.1 for cardholder data and client-side controls

Dual-ECDSA-signed transaction evidence for dispute and supervisory review

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 · BANKING & PAYMENT SYSTEM OPERATORS

Stop the fraudster. Before the fraud.

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