ZIMPERIUM

NPCI's 2025 Mobile Security Mandate

How Zimperium Helps You Comply

What Is This Regulation?

On May 19, 2025, the National Payments Corporation of India (NPCI) issued circular NPCI/2025-26/IS/003 mandating a Comprehensive Mobile Application Security Framework for all UPI applications. The directive applies to every Payment Service Provider (PSP), Application Service Provider (ASP), and Third-Party Application Provider (TPAP) operating on the Unified Payments Interface.

This is not guidance. It is a compliance mandate. All covered entities must submit audit certification from a CERT-IN empanelled auditor by December 31 of each financial year.

Who must comply

All PSPs, ASPs, and TPAPs operating UPI applications in India — including PhonePe, Google Pay, Paytm, and bank-owned UPI apps. Non-compliance risks regulatory action and transaction suspension.

Why Was This Necessary?

India processes over 13 billion UPI transactions per month. That scale makes the payment rail a high-value target. The NPCI circular cites three driving forces:

- Increasing sophistication of mobile-specific attacks including overlay fraud, session hijacking, and runtime manipulation
- Growth of repackaged and fake UPI apps distributed through unofficial channels and the dark web
- Gaps in prior RASP guidance from 2020 that did not account for modern threat vectors like Frida-based instrumentation, screen mirroring abuse, and OTP interception

The framework uses an Identify, Protect, Detect, Respond structure aligned with NIST principles. It covers 23 specific controls across device integrity, application hardening, network security, and runtime threat response.

The business risk is clear

A compromised UPI app exposes millions of users to financial fraud. For PSPs and TPAPs, the consequences include regulatory fines, brand damage, and loss of payment license. Security is now a condition of market participation.

NPCI Requirements Mapped to Zimperium MAPS

Zimperium MAPS (Mobile Application Protection Suite) addresses both the mandatory and recommended controls in the NPCI framework through its on-device AI engine, static analysis, and runtime protection capabilities. The table below maps each major requirement to the corresponding MAPS capability.

NPCI Requirement	Status	MAPS Capability
Root & Jailbreak Detection	**Mandatory**	Detects rooted/jailbroken devices and root cloaking attempts at runtime
App Installation Source Validation	**Mandatory**	Detects sideloaded or repackaged apps from unauthorized sources
Code & Data Integrity at Runtime	**Mandatory**	Memory integrity checks and runtime verification to detect tampering
Anti-Debugging	**Mandatory**	Detects ptrace, gdb, and other debugging tool activity on device
Code Obfuscation & Key Encryption	**Mandatory**	Validates implementation against reverse engineering and key exposure
OWASP Top 10 Coverage	**Mandatory**	Static and dynamic scanning mapped to OWASP Mobile Top 10
Screen Obfuscation & Screenshot Prevention	**Mandatory**	Detects screen capture, screen recording, and overlay attacks
Proxy Network Detection	**Mandatory**	Identifies proxy and VPN usage at runtime, flags suspicious connections
SSL Pinning Enforcement	**Mandatory**	Detects SSL stripping and Man-in-the-Middle attack attempts
Developer Options & USB Debug	**Mandatory**	Blocks app execution when developer mode or USB debugging is active
Screen Mirroring Prevention	**Mandatory**	Detects active screen mirroring to prevent unauthorized monitoring
Reverse Engineering Prevention	**Mandatory**	Behavioral analysis and anti-reverse engineering controls in-app
Auto-Read OTP Security	**Mandatory**	Restricts OTP permissions and detects unauthorized read attempts
Harmful App Detection	**Recommended**	Flags blacklisted and malicious apps installed on the device
Keylogger Prevention	**Recommended**	Detects keylogging tools running alongside the UPI application
Screen Overlay Prevention	**Recommended**	Blocks unauthorized overlays to prevent tapjacking and UI spoofing
Dynamic Instrumentation Prevention	**Recommended**	Detects Frida, Cycript, Ghidra and similar runtime manipulation tools
Alerting & Automated Response	**Mandatory**	Real-time threat alerts with automated response actions to backend

How MAPS Goes Beyond NPCI Compliance

Meeting NPCI's framework is the floor, not the ceiling. MAPS is built to exceed it.

Most teams cobble together four or five point solutions to secure a single app, each with its own dashboard, vendor, and gap. MAPS replaces them all. One platform, one workflow, one place to see everything across your entire app install base.

NPCI requires scanning, hardening, runtime protection, and alerting. MAPS delivers all of that and goes further across four integrated capabilities.

Mobile Application Security Testing scans every build automatically for security, privacy, and compliance issues. CI/CD integration catches vulnerabilities before production. AI generates code-level guidance so developers fix issues directly without waiting on the security team.

App Protection applies code obfuscation, tamper detection, and integrity protection before release. It makes your app resistant to reverse engineering, repackaging, and IP theft on attacker-controlled devices, which is exactly the attack vector NPCI's new controls are designed to close.

Advanced Runtime Protection runs on-device. It detects malware, overlay attacks, emulators, and rogue networks in real time and blocks high-risk transactions on compromised devices before fraud occurs, with no cloud round-trip required.

Cryptographic Key Protection uses white-box cryptography to make encryption keys unrecognizable to attackers even on compromised, rooted, or jailbroken devices. Keys are protected at rest, in transit, and in use with no hardware dependency. NPCI mandates key encryption. MAPS makes those keys effectively invisible.

On top of all that, the Mobile Application Response Agent automatically investigates critical threat alerts, determines whether a threat is a true security incident, and provides step-by-step response guidance. Junior analysts act with senior-level confidence. Mean time to respond drops significantly.

A Fortune 500 global bank deployed MAPS and prevented

$1.35M

in fraud in the first six months.

Learn More about MAPS here: https://zimperium.com/maps

Audit readiness built in

MAPS generates compliance evidence aligned to each NPCI control. Your CERT-IN auditor receives structured output, not a stack of screenshots. That reduces audit time and eliminates last-minute remediation cycles.

About Zimperium

Zimperium is the world leader in **AI-empowered** mobile security. Purpose-built for mobile, Zimperium provides unparalleled protection for mobile applications and devices, leveraging the power of AI to deliver autonomous mobile security that counters evolving threats including mobile phishing (mishing), malware, app vulnerabilities, app tampering, device compromise, and even zero-day attacks. Cybercriminals have adopted a mobile-first attack strategy, targeting **your most vulnerable attack surface** - the mobile apps and devices that your organization and customers depend upon.

Headquartered in Dallas, Texas, Zimperium is backed by Liberty Strategic Capital and SoftBank. Learn more at www.zimperium.com and connect on LinkedIn and X (@Zimperium).

ZIMPERIUM®

Learn more at: zimperium.com
Contact us at: 844.601.6760 | info@zimperium.com
Zimperium, Inc
4055 Valley View, Dallas, TX 75244