ERGO

KHAITAN &CO ADVOCATES SINCE 1911

Enabling Delegated Payments on UPI Rails:

Implications of IoT and Software Integration for UPI Payments under NPCI OC

201-B

20 November 2025

Introduction

On 8th October 2025, the National Payment Corporation of India (NPCI) issued an Operating Circular 201-B (OC), authorising the use of Internet of Things (IoT) devices and software (together, Devices) within the Unified Payments Interface (UPI) Circle framework. This OC builds on NPCI's 2024 circular that introduced delegated payments called UPI Circle - a feature that enables a bank account holder (Primary User) to securely share controlled payment access with trusted individuals or devices (Secondary User).

Under the UPI Circle, a Secondary User may initiate payments from the Primary User's account, strictly in accordance with the rules defined by the Primary User. By enabling this integration, the NPCI has, inter alia, established a foundational framework for "agentic payments" within the UPI ecosystem, i.e., payments executed by AI agents (such as chatbots like ChatGPT) that can initiate, authenticate and complete transactions on a user's behalf, while fully preserving user control, security and consent.

Key Guidelines

The Operational Circular establishes a comprehensive framework of guidelines to ensure a secure, efficient, and compliant integration of Devices for delegated payments within the UPI ecosystem. The key requirements are summarised below:

1. **General Obligations**

(a) *Compliance with RBI Guidelines*: All transactions must strictly adhere to the Reserve Bank of India's (RBI) guidelines on *Harmonisation of Turn Around Time and Customer Compensation for Failed Transactions Using Authorised Payments Systems* dated 20 September 2019. This ensures adherence to mandated turnaround times and the application of prescribed compensation measures for failed transactions.

(b) *Online Dispute Resolution*: A robust and user-friendly online dispute resolution mechanism must be made available, offering a transparent, efficient, and standardised process for users to raise and resolve disputes relating to such transactions.

(c) *Reconciliation and Settlement*: Reconciliation and settlement for such delegated payments shall align with the existing UPI guidelines and processes.

(d) *Device and Software Linking* Controls: Only Devices expressly authorised by NPCI may be linked as secondary Devices within the UPI system. This safeguard is intended to preserve system integrity and reduce security risks. However, NPCI is yet to provide a list of the permitted devices.

(e) *Transaction Scope*: Delegated payments initiated through Devices are limited to domestic Person-to-Merchant (P2M) transactions. Cross-border transactions and peer-to-peer payments remain outside the scope of this framework.

(f) *Proximity Requirement at Linking*: During the process of linking the primary and secondary Devices, both must be in close physical proximity. This requirement enhances security and ensures the legitimacy of the device pairing process.

(g) *Transaction Limits and Cooling Period*: Strict financial limits are imposed to mitigate risk and protect users:

- A maximum monthly limit of INR 15,000 per Device; and
- A per-transaction cap of INR 5,000.

Additionally, after a mandatory 24-hour cooling period applies upon the creation of a new delegation, during which the cumulative transaction limit is capped at INR 5,000.

2. **Obligations for Primary UPI Apps**

(a) *Display and Authorisation of Secondary Devices*: Primary User UPI apps must clearly display all secondary device or software intended for linking. Before any such app is authorised, explicit user consent must be obtained through a secure two-factor authentication (2FA) process to ensure intentional and verified approval.

(b) *Lifecycle Management*: UPI apps must offer comprehensive lifecycle management features, such as tools for managing financial limits, and delinking Devices.

(c) *Device Authorisation Limit*: A Primary User may authorise up to five Devices through the UPI app. This cap helps maintain a balance between user convenience and systematic security**.**

3. **Obligations for Secondary Apps and PSP Banks (Certified on UPI Circle)**

(a) *Onboarding and App Security Evaluation*: Secondary PSP Banks must onboard IoT device applications or software only after conducting thorough due diligence and a comprehensive security evaluation of the respective app or software.

(b) *Registration Process and User Validation*: Secondary PSPs must support the Device registration process by obtaining explicit user consent and implementing robust validation mechanisms, such as verifying the user's mobile number through a one-time password, to ensure authenticity and user intent.

(c) *Device and User Identification*: During registration, Secondary PSPs are required to capture the Device ID and/or user details from the secondary device or software. These identifiers must be validated during each payment request to ensure security and traceable transactions.

(d) *User Profile and Feature Access Control*: Where software applications are utilised, the user profile ID must be recorded as part of the registration process. Initially, access to these features will be restricted to a limited user group to facilitate controlled roll-out and system validation. Following successful validation, NCPI will communicate the expansion of access to the broader user base.

(e) *Consistency in User Profile and Registration*: Secondary apps must ensure that the same mobile number is used both for the user profile and for UPI Circle registration to maintain consistency and security.

(f) *Delegation Acceptance Limitation*: Both Secondary Apps and Secondary PSPs must ensure that a user can accept delegation for any given Device from only one Primary UPI app.

(g) *Security and Data Protection*: Secondary PSP Banks, together with the associated IoT device app or software, must ensure the protection of user and payment data in accordance with NPCI's prescribed processes. This includes maintaining detailed documentation of data flows, complying with data localisation guidelines, and providing regular security reporting as mandated.

(h) *Non-Exclusive Partnerships for Devices without Dedicated Applications*: For IoT devices that do not have a dedicated interface or application, the device must be capable of integrating with multiple supporting Secondary UPI apps. Exclusive partnerships with a single or limited set of UPI apps should be avoided to ensure wider accessibility, interoperability, and user choice.

4. **Obligations on Issuer Banks**

Issuer Banks are required to ensure security, authenticity, and integrity of every transaction initiated through their systems. Prior to debiting a customer's account for payment instructions, Issuer Banks must conduct rigorous validation of both the Device ID and user ID associated with the transaction. These measures are essential in safeguarding user accounts and maintaining trust in the payment ecosystem.

Comments

The OC marks a significant development in India's digital payments landscape, enabling the creation and implementation of automated, intelligent and AI-driven payment solutions. By enabling the integration of IoT devices and software, the OC aims to enhance both the scope and efficiency of digital payment transactions while setting the operational stage for agentic payments.

This framework introduces a secure and interoperable delegation layer that fundamentally transforms the UPI from a system reliant on human-initiated actions to one that is inherently AI-native.

Looking ahead, the integration of such AI-driven delegation frameworks is poised for rapid expansion across India's extensive UPI user base. This development not only underscores India's leadership in real-time, AI-augmented payments but also paves the way for widespread deployment of intelligent, automated payment systems across diverse sectors and consumer use cases.

- *Harsh Walia (Partner); Rupendra Gautam (Senior Associate) and Sanskriti Shrivastava (Associate)*

About Khaitan & Co

Khaitan & Co is a top tier and full-service law firm with over 1300+ legal professionals, including 300+ leaders and presence in India and Singapore. With more than a century of experience in practicing law, we offer end-to-end legal solutions in diverse practice areas to our clients across the world. We have a team of highly motivated and dynamic professionals delivering outstanding client service and expert legal advice across a wide gamut of sectors and industries.

To know more, visit **www.khaitanco.com**