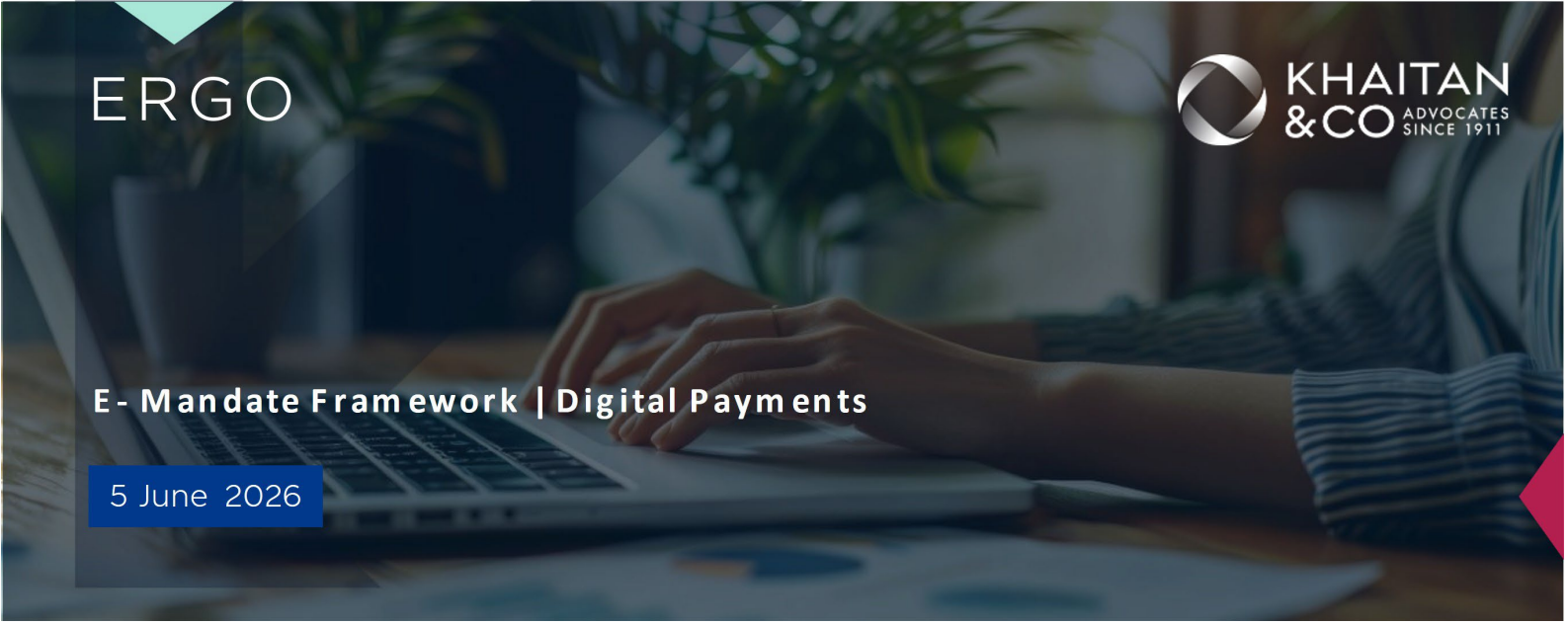

ERGO

KHAITAN &CO ADVOCATES SINCE 1911

E- Mandate Framework | Digital Payments

5 June 2026

Introduction

India's digital payments landscape / ecosystem has grown exponentially and at a pace that regulators struggled to match. The rules governing automatic recurring charges remained scattered across multiple directives issued at different times. Between 2019 and 2024, 8 separate circulars attempted to regulate e-mandates; each adding layers, refining thresholds, or extending rules to new payment instruments.

Regulatory Chronology (2019–2026)

- 2019: Initial enablement of card-based recurring e-mandates introduced the basic auto-debit construct and issuer responsibilities, with an emphasis on Additional Factor of Authentication (AFA) at registration and consumer control. In 2020, the scope expanded to Unified Payments Interface (UPI) and Prepaid Payment Instruments (PPI) as recurring use-cases matured.

- 2020–2021: Through late-2020 circulars and a 31 March 2021 framework, Reserve Bank of India (RBI) refined pre-debit notifications, clarified handling of first versus subsequent transactions, and tightened issuer obligations. A clarification issued in October 2021 addressed operational frictions observed during industry rollout (notably notification timing, content, and opt-out pathways).

- 2022–2024: Successive circulars adjusted thresholds and expanded coverage, responding to scaling volumes and fraud-risk learnings. By August 2024, a coherent set of operational expectations had emerged but remained distributed across multiple circulars, creating interpretive and operational fragmentation for industry participants.

- 21 April 2026: The 2026 Framework (*as defined hereinafter*) consolidates and supersedes the prior instruments, aligns definitions to the RBI's 2025 authentication directions[1], codifies tiered AFA thresholds, standardises pre and post-debit notifications, sets out dispute-resolution expectations, and expressly repeal the earlier circulars. This completes the migration from fragmented guidance to a single, technology-neutral code for recurring payments.

Consequence

Consequence, a stark picture and significant numbers: Approximately 28 lakh fraud cases totalling INR 22,931 crore were reported in 2025, compared to just 260,000 cases worth INR 551 crore in 2021. That is a tenfold increase in case volume and a more than fortyfold increase in value over four years. Banks reported 13,516 card and internet fraud cases worth INR 520 crore in FY 2024-25, down from 29,080 cases and INR 1,457 crore the year before.[2]

---

[1] Reserve Bank of India (Authentication mechanisms for digital payment transactions) Directions, 2025 dated September 25, 2025 and Master Direction on Regulation of Payment Aggregator (PA) dated September 15, 2025.

[2] Data from the National Cyber Crime Reporting Portal (NCRP), cited by the RBI in its April 2026 discussion paper titled 'Exploring safeguards in digital payments to curb frauds' ("Discussion Paper"), paints See Page 138 of the Annual Report for FY 2024-25 published by the RBI on 29 May 2025

In the context of recurring payments, this meant that loosely regulated auto-debit arrangements, moved too slowly. These revealed systemic weaknesses in digital payments architecture, no single point of accountability and obvious vulnerability, endemic gaps, inadequate KYC procedures, insufficient oversight of intermediaries, and regulatory frameworks.

Tightening the e-mandate framework with standardised authentication, mandatory pre-debit alerts, and clear opt-out mechanisms was a direct response to this risk.

Discussion Paper

On 6 February 2026, the Governor in his statement announced action on three fronts: mis-selling of financial products, harsh loan recovery practices, and fraud compensation. The RBI committed to a discussion paper on digital payment safety, looking at 'calibrated safeguards such as lagged credits and additional authentication for vulnerable users, including senior citizens.'

The single most compelling driver is the sheer scale of digital payment fraud in India. The RBI acknowledged in its Discussion Paper that '*the potential of digital payments is impeded by complaints related to frauds*' and that '*a typical fraud through digital payments may not involve technical compromise of systems, but mostly through manipulation of users through social engineering, coercion, or impersonation.*'

In April 2026, a discussion paper was released with concrete proposals: a one-hour wait for payments to new beneficiaries, a 'trusted person' approval step for customers aged 70 (seventy) and above, and a 'kill switch' to let users block all outgoing digital transactions instantly.

The e-mandate consolidation, arriving just days later, can be read as part of the RBI's broader effort to tighten governance across the payments' ecosystem.

E-mandate Framework, 2026 - Circular

On 21 April 2026, the fragmented regulation approach ended with the RBI issuing the Digital Payments – E-mandate Framework, 2026 (Circular No. RBI/DPSS/2026-27/396) (2026 Framework).

This circular consolidates all prior directives on e-mandates into a single unified framework that applies immediately to all payment system providers and participants.[3] What makes this consolidation significant is the administrative convenience it brings, and the regulatory priorities and RBI's wider push to protect customers, security, transparency, and consumer control.

The Consumer Protection Pivot | Four Pillars of Control

The 2026 Framework rests on four core pillars: registration and authentication, transaction limits with tiered thresholds, mandatory notification requirements, and consumer protection measures.

To appreciate the consolidation's significance, comparing the old and new regimes is relevant:

Aspect	Old Regime (2019–2024)	2026 Framework
Regulatory Structure	Eight separate circulars issued over five years	Single consolidated direction; all predecessors repealed
Instrument Coverage	Started with cards; UPI and PPIs added incrementally	Cards, UPI, and PPIs covered uniformly in one rulebook
Transaction Limits	Thresholds adjusted across multiple circulars; no single reference	Tiered limits codified clearly: INR 15,000 (general), INR 1,00,000 (insurance, MFs, credit cards)

[3] Reserve Bank of India, Digital Payments – E-mandate Framework, 2026, Circular No. RBI/DPSS/2026-27/396 (21 April 2026), available at www.rbi.org.in

Aspect	Old Regime (2019–2024)	2026 Framework
Pre-Debit Alerts	Introduced and refined piecemeal	Standardised 24-hour window with mandatory content
Cross-Border Transactions	Addressed later; not part of original scope	Covered from day one alongside domestic transactions
Compliance Burden	Multiple documents to cross-reference	One document, one set of rules

Authentication:

Every recurring payment begins with registration. A customer wishing to set up an e-mandate is required to undergo a one-time registration process, with the mandate registered after successful validation through an AFA in addition to normal issuer procedures.[4] This might be an OTP, biometric verification, or similar second factor. Any change to a mandate requires the same AFA validation.

Issuers must provide customers with a facility to choose or change their preferred notification channel (SMS, email, etc.) at registration.[5] This puts customer in control. Subsequent debits follow a tiered approach rather than blanket authentication requirements, a pragmatic balance between security and user action.

Transaction Limits | Tiered Approach

The idea that all recurring transactions are created equal is taken away by the 2026 Framework. All recurring transactions may be authorised without AFA up to INR 15,000 per transaction.[6] This is applicable for small payments such as utility bills, subscriptions, and routine payments.

For transactions above INR 15,000 i.e., payment of categories with elevated thresholds, such as insurance premiums, mutual fund subscriptions, and credit card bill payments may be processed without AFA up to INR 1,00,000 per transaction.[7] These categories, whilst higher in value, are typically predictable and low-risk compared to arbitrary transfers.

Pre-Debit Alerts and Post Debit Communication:

Once an e-mandate is registered, issuers are required to send a pre-transaction notification to the customer at least 24 hours prior to the actual charge or debit, informing the customer of the merchant's name, transaction amount, date and time of debit, the e-mandate reference number, and the reason for the debit.[8] This provides customers with time to cancel the specific transaction or withdraw the mandate entirely before money leaves their account. The issuers are required to provide customers with a facility to opt out of any particular transaction or the e-mandate itself, with any such opt-out validated by the issuer using AFA and confirmed via intimation to the customer.[9]

There is one exception to pre-transaction notification: for e-mandates registered to auto-replenish balances such as FASTag and the National Common Mobility Card (NCMC).[10]

After the money has been debited, issuers are required to send a post-transaction notification informing the customer of the merchant's name, transaction amount, date and time of debit, reference numbers of both the transaction and e-mandate, the reason for debit, and crucially, details on grievance redressal.[11] This last element is crucial where customers need to know exactly where and how to raise concerns.

An appropriate dispute redressal system must be established by the issuer to facilitate customer grievances.

The RBI's existing instructions on limiting customer liability for unauthorised transactions now expressly apply to recurring transactions under e-mandates as well.[12] This extension of liability protections is

[4] Ibid., Para 4(a).
[5] Ibid., Para 4(d).
[6] Ibid., Para 8(a).
[7] Ibid., Para 8(b).
[8] Ibid., Para 6(a)–(b).
[9] Ibid., Para 6(c).
[10] Ibid., Para 6(d).
[11] Ibid., Para 7.
[12] Ibid., Para 9(a)–(b).

significant where customers disputing fraudulent recurring charges enjoy the same safeguards as those disputing one-off fraudulent transactions.

Consumer-Friendly Provisions

Several measures designed to lower adoption barriers and to strengthen consumer trust have been introduced in the 2026 Framework:

Zero charges: No charges shall be levied on customers for availing the e-mandate facility for recurring transactions.[13] This removes any financial disincentive for using the system.

Card reissuance continuity: Existing e-mandates can be mapped to reissued cards, i.e., if a card expires or is replaced, the customer does not need to re-register.[14]

Extended liability protections: The 2026 Framework's express application of unauthorised-transaction liability limits to e-mandates. The customers are now protected regardless of whether fraud occurs through a one-off transaction or an unauthorised recurring charge. The RBI has proposed compensating customers up to INR 25,000 for small-value digital fraud losses, with costs split between the customer, the issuing bank, the receiving bank, and an industry fund.

Implications for Stakeholders

For Payment Service Providers and Banks

The 2026 Framework places explicit compliance obligations on service providers. Acquirers are required to ensure compliance with these directions by merchants on-boarded by them.[15] This creates a chain of accountability where issuers cannot ignore merchant misbehaviour by claiming that they merely process transactions. The burden of ensuring merchant compliance is explicit.

This means for issuing cards or operating UPI networks, the immediate priority is operational: reviewing existing e-mandate implementations and ensuring alignment with the 24-hour notification window, tiered AFA requirements, and dispute resolution procedures.

For Fintech Companies and Payment Aggregators

The consolidation reduces interpretive risk. For compliance teams, rather than piecing together guidance from 8 circulars, they have a single, immediate-effect direction to work with. The definitions are aligned with the RBI's 2025 authentication directions, minimising gaps or ambiguities.

However, the 2026 Framework's emphasis on AFA for modifications and opt-outs means that fintech platforms must build or ensure their upstream partners build robust authentication workflows. A customer experience that makes opting out cumbersome or confusing exposes the fintech companies to regulatory action.

For Customers

The 24-hour pre-debit alert coupled with easy opt-out mechanisms provides customers the required control. Unlike systems where recurring charges surprise the customer, the 2026 Framework ensures required disclosures by agencies and desired awareness by customers. Combined with the extension of unauthorised-transaction liability protections, customers face reduced financial risk.

The Bigger Picture: Consumer Protection as Policy

The e-mandate consolidation signals a decisive pivot towards customer protection, proposing measures to curb mis-selling, tighten loan recovery practices, and introduce compensation frameworks for digital fraud losses. The 2026 Framework shifts the burden of protection onto the system rather than expecting individual customers to be perpetually vigilant.

---

[13] Ibid., Para 10(a).
[14] Ibid., Para 10(b).
[15] Ibid., Para 10(c).

The practical impact for all stake holders is substantial. A compliance officer at a mid-sized fintech company no longer needs to reconcile 8 circulars issued at different times. A merchant onboarded by an acquirer now operates under rules that apply uniformly across all payment instruments. A customer receives consistent protections whether paying via card, UPI, or prepaid instrument.

As a foundation for the next phase of digital payments growth, this consolidation represents regulatory housekeeping. Strategically, governance and model-risk teams should now monitor loss-trend data and user-friction metrics and anticipate fine-tuning of thresholds or notification carve-outs. The 2026 Framework's consolidation should simplify audits, regulatory reporting, and transaction-monitoring.

- *Nikhilesh Panchal (Partner); and Amiya Kumar Pati (Principal Associate)*

About Khaitan & Co

Khaitan & Co is a top tier and full-service law firm with over 1300+ legal professionals, including 340+ 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**