Discussion Paper

Exploring safeguards in digital payments to curb frauds

Department of Payment and Settlement Systems

Reserve Bank of India

I. Background

Over the past decade, digital payments in India have expanded at an unprecedented pace, reflecting a structural shift in the manner in which individuals and businesses conduct financial transactions. Digital transaction volumes have increased 38-fold, while transaction values have more than tripled. The compound annual growth rate (CAGR) of digital payments over this period stands at approximately 53% and 13% in volume and value terms respectively.

ii. The above growth has been supported by a diverse and interoperable payments ecosystem comprising credit and debit cards, Unified Payments Interface (UPI), Immediate Payment Service (IMPS), National Electronic Funds Transfer (NEFT), Real Time Gross Settlement (RTGS), mobile wallets, and net banking. Strong security architecture, including mandatory Additional Factor of Authentication (AFA), beneficiary name look-up facilities, transaction controls, apart from fast settlement cycles, have enhanced user confidence and promoted seamless digital usage.

iii. However, the potential of digital payments is impeded by complaints related to frauds. 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. Victims, acting under deception, themselves initiate and authenticate transactions, leading to 'Authorised' Push-Payment (APP) frauds. Given the instantaneous nature of payments through systems such as NEFT, RTGS, UPI and IMPS, the scope for timely intervention and recovery of funds becomes limited.

II. Regulatory measures to secure digital payments

iv. Over the years, the Reserve Bank has introduced several measures to strengthen the safety and resilience of digital payments. Two-factor authentication was mandated in digital payment transactions. Storage of actual card data by any entity in the payment chain, other than the card issuer, was sought to be restricted through device tokenisation (2019) and and card-on-file tokenisation (2021). Customer induced controls in cards were mandated in 2020 thereby empowering cardholders to switch on / off and set / modify transaction limits (within the overall card limit, if any, set by the issuer) for all types of transactions – domestic and international, at PoS/ online transactions/contactless transactions, etc.

v. Instructions regarding digital payment system controls for banks (2021) and non-bank PSOs (2024) were issued covering aspects such governance mechanisms for identification, assessment, monitoring and management of information systems and cyber security risks, along with baseline security measures for ensuring system resilience as well as for safe and

secure digital payment transactions. In 2025, the Bank issued a principle-based framework for authentication of digital payment transactions to encourage introduction of new factors of authentication by leveraging upon technological advancements and to enable issuers to adopt additional risk-based checks beyond the minimum two-factor authentication based on fraud risk perception of the underlying transaction.

vi. The customer's liability is limited in case of unauthorised electronic banking transactions as mentioned in instructions issued in 2016.

vii. RBI has also issued directions to various system participants to utilise the Mobile Number Revocation List (MNRL) available on the Digital Intelligence Platform (DIP) developed by Department of Telecommunications (DoT), to monitor and clean their customer database. Telecom Regulatory Authority of India (TRAI) has issued directions to use phone numbers that begin with the '1600xx' series for calling customers regarding transactions or service-related provisions. Further, any marketing or promotional calls should be made from numbers in '1400xx' series. These measures aim to help consumers distinguish between legitimate calls and potential scam attempts made by fraudsters.

viii. Indian Cybercrime Coordination Centre (I4C) has issued a Standard Operating Procedure to deal with complaints lodged with National Cybercrime Reporting Portal (NCRP).

ix. In 2024, Reserve Bank's wholly owned subsidiary - Reserve Bank Innovation Hub (RBIH) has built Mulehunter.AI to enable quick and effective detection of mule bank accounts by the banks. The Reserve Bank is also presently working with RBIH to set-up prototype of a Digital Payment Intelligence Platform (DPIP) by harnessing advanced technologies (AI/ML) to mitigate payment fraud risks. To a remitting bank, the platform is envisaged to provide information about the beneficiary's profile through a risk score generated on a real-time, transaction-by-transaction basis, even before the transaction is executed.

III. Scope for further action

x. Due to robust measures put in by place by banks under RBI's guidance, frauds attributed to account take-over are now negligible and most frauds are Authorised Push Payments or APP frauds, which thrive in environments characterised by easy, and frictionless, payments wherein funds can be transferred instantaneously by customers (victims) with minimal effort before realising that they are being duped. Post-transaction remedies to recover such funds being limited, a defrauded user is often left with a few remedies and uncertain outcomes, which are time-consuming and show low recovery rates.

xi. Figures from the National Cyber Crime Reporting Portal (NCRP) indicate that frauds related to digital payments are on the rise. As can be seen from the data below:

Year	Number of frauds reported	Value of frauds (in ₹ Crore)
2021	2.6 lakh	551
2022	6.9 lakh	2,290
2023	13.1 lakh	7,465
2024	24 lakh	22,848
2025	28 lakh	22,931

Fraudsters are deploying various tactics, such as bogus call centres, deepfake-driven impersonation scams and mule account networks. Almost all sections of society especially the vulnerable groups such as senior citizens have fallen prey to such APP frauds. Therefore, there is an urgent need to put in place systems and processes to address these issues. This discussion paper seeks stakeholder views on the need for introducing extra layers of safeguards.

xii. The discussion paper sets out the following four options, namely,

1) Lagged credit for authorised push payments other than low value;
2) Additional authentication by trusted person for high-value digital transactions by vulnerable sections of society;
3) Only accounts with satisfactory additional review to receive large credits; and
4) Customer-induced controls

These options are aimed at the broad objectives, viz., inducing a lag in select category of digital payments (by way of process-level changes or in terms of additional due diligence requirements) thereby buying time for both customers and PSOs to limit fraudulent transactions from being executed or proceeds thereof from being moved quickly, and, empowering the customer through provision of customised controls.

Each option is detailed in the sections that follow, along with specific questions on which stakeholder feedback is being sought. Stakeholders are requested to provide their views on the desirability and feasibility of each option, both on a standalone basis and in combination with the other possible mechanisms, while keeping in mind the measures already in place or in the works.

Option 1: Lagged credit for authorised push payments

Electronic payments to merchants are ordinarily enabled by banks and Payment Aggregators (PAs) after undertaking the requisite due diligence of the merchants. In such cases, payment networks typically provide chargeback mechanisms as part of the dispute resolution framework. No comparable safeguard exists in the case of account-to-account transfers. Accordingly, introducing a time lag for certain APP transfers to the bank account of an individual, or to the account of a sole proprietorship or partnership firm, at both the payer's and the payee's ends, may serve as an effective fraud-mitigation measure.

1.1 International experience:

1) **United Kingdom (UK):** The UK introduced a formal mechanism (via the Payment Services (Amendment) Regulations 2024) to delay outbound account-to-account payments in suspected fraud cases. Under this framework, payment service providers (PSPs) can hold an outbound payment for up to 72 hours (roughly three business days) if there are reasonable grounds to suspect the payment instruction was induced by fraud or dishonesty. During this delay window, the funds remain frozen in the payer's account, and the PSP must notify the payer and explain the reason. The PSP may also use this time to contact the beneficiary's bank or law enforcement.

2) **Singapore:** Singapore has implemented a preventive approach centered on cooling-off periods and dynamic transaction safeguards. Under the Enhanced Anti-Scam Framework (EASF) and Shared Responsibility Framework (SRF) introduced by the Monetary Authority of Singapore (MAS) and the Association of Banks in Singapore, banks must impose a minimum 12-hour cooling-off period when a customer performs certain high-risk actions – for example, activating digital banking on a new device, resetting critical account credentials, or initiating a first-time transfer to a new payee. During this period, outgoing transactions from that account may be suspended or limited, creating a window to detect and block unauthorised access or scam attempts.

3) **Sweden:** In May 2024, the Swedish Bankers' Association announced a coordinated package to combat frauds. This included adding cooling-off periods, additional confirmation steps for new payees and limits on unusually large or atypical transactions. The design of the specific measure was left to the individual bank based on bank-specific conditions.

1.2 Possible approach:

Introducing a lag at the payer's end is important, as this is the stage at which the decision to transfer funds is made and where social-engineering tactics are deployed. A short delay before execution of the debit can act as a preventive control by disrupting the fraudster's psychological influence over the victim and by giving the payer an opportunity to reconsider the transaction.

To ensure that low-value transactions continue to remain frictionless, such lag mechanisms are proposed to be applied only to APP transactions above a specified threshold. A threshold of ₹10,000 per transaction may be considered appropriate. As per information available with the National Cyber Crime Reporting Portal (NCRP), transactions above ₹10,000 account for approximately 45 per cent of reported fraud cases by volume, but about 98.5 per cent by value.

Under this approach, once a customer (individuals including sole proprietors plus partnership firms) initiates an APP transaction exceeding ₹10,000, a lag period of one hour could be applied. The lag can be applied at the payer's end or at the payee's end or both. From an ease of implementation perspective, it is suggested that the lag is introduced at payer's end only. During this period, the payer's bank would provisionally debit the customer's account, and the payer would retain the option to cancel the transaction for any reason. The proposed one-hour window is consistent with the "golden hour" principle in fraud-risk management, under which the initial period following a fraudulent transaction is critical to prevent the dissipation of funds. During this period, if the payer's bank identifies the transaction as unusual or atypical, it may seek reconfirmation from the payer, while sharing appropriate information on the nature of the suspicion and cautioning the payer. If the payer, after reviewing the information provided, still chooses to proceed, the transaction will be executed by payer bank.

Further, recognising that certain transactions may be time-sensitive, an option may be provided to the payer to override the lag for a specific transaction by explicitly authorising it, for instance through a whitelisting mechanism. In such cases, the lag may be bypassed. Instead of allowing whitelisting of transactions or in addition to it, payees can be whitelisted by the payer. All payments to such whitelisted payees will not be subjected to time lag.

1.3 Pros and Cons:

Pros:

(i) Fraudsters typically rely on creating urgency and maintaining continuous psychological pressure on the victim to prevent deliberation. Introducing lag at payer's end breaks the fraudster's psychological control.

(ii) A delay at the beneficiary's end acts as an additional layer of defence even if the payer-side control is bypassed or fails.

(iii) By slowing down the movement of funds, the mechanism increases the window available for detection and intervention.

(iv) Visible and effective safeguards reassure users that the payment ecosystem is secure and responsive to fraud risks. This is particularly important for onboarding new users and retaining confidence and trust among existing users while making digital payments.

Cons:

(i) Implementing lag would require changes across bank systems and payment system infrastructure, including transaction queuing, cancellation mechanisms, etc. These changes would involve cost and effort for the ecosystem.

(ii) Introducing lag for certain transactions may conflict with the core design principle of immediacy of digital payments.

(iii) Users accustomed to instant transactions could find it difficult to understand why certain payments are delayed while others are not. Clear communication and consistent application of rules would be critical to avoid this confusion.

(iv) Given that an option to whitelist transactions would be available, fraudsters may persuade victims to bypass the safeguard, thereby reducing its effectiveness.

1.4 Brief contours:

Scope	• APP transactions done by individuals (including business accounts, e.g., sole proprietor, partnership firms) save for exclusions listed below.
Exclusions and whitelisting	• All merchant transactions (done through any mode, for example – UPI, cards, net banking etc.,). Recurring payments (such as e-mandates, NACH based payments) and payments through cheques are proposed to be exempted.

	• Payer can also whitelist a particular transaction, if the same is time-sensitive and / or a particular payee.
Threshold	₹10,000 and above
Lag period	Mandatory 1 hour at Payer Bank's end except for whitelisted transactions/whitelisted payee. Payer can cancel the transaction during this period.
Action expected of payer's bank	To seek reconfirmation from the payer if the transaction appears suspicious and to provide a facility to its customer to cancel the transaction.

Question 1: *Given the various measures initiated by RBI to ensure safety and security of digital payments and some others proposed in the paper, whether there is a need to introduce the above option from a cost-benefit perspective?*

Question 2: *Is there any category of transaction / account which may be exempted from this approach?*

Question 3*: Is the suggested threshold of ₹10,000 adequately balancing fraud risk mitigation and customer convenience?*

Question 4*: Is the suggested mandatory lag at payer's end required to balance the need to mitigate fraud while supporting efficiency of digital payment transactions or should the same be optional depending upon the perceived risk underlying the transaction as determined by the payer's bank?*

Question 5*: Is the suggested mandatory lag of one-hour at payer's bank reasonable?*

Question 6: *What are the views with respect to whitelisting? Whether it should be transaction specific or payee specific or both?*

Option 2: Additional authentication by trusted person for high-value digital transactions by vulnerable sections of society

Certain sections of the society, such as citizens above a certain age or differently-abled persons (persons with disabilities) may be particularly vulnerable to social engineering–based frauds. Such frauds often involve impersonation of family members or the fabrication of urgent scenarios relating to medical, legal, or other emergencies. These targeted incidents frequently result in disproportionately higher financial losses, underscoring the need to consider enhanced protective measures for this customer segment, alongside sustained awareness initiatives.

2.1 International experience

i. Sweden: As a part of the package unveiled in May 2024 by Swedish Bankers' Association, it is understood that banks may advise customer that a particular transaction has to be approved by a person trusted by the customer.

ii. United States of America: Some banks offer trusted contact facility to their customers to enable the banks to contact these trusted people in case of suspicion of fraud. A trusted contact can access the account of a bank's customer, provided the latter has provided a financial power of attorney.

iii. Ireland: Any customer who is an individual may choose to nominate a Trusted Contact Person. The financial institution will establish contact with the trusted contact person, when the customer is not reachable or where financial abuse, including fraud, is suspected. However, this trusted person has no decision-making authority and acts only as a support layer.

2.2 Possible Approach:

The policy framework outlines specific provisions for enhanced security measures aimed at safeguarding vulnerable customer segments undertaking specified digital payment transaction. These measures may be made mandatory for citizens aged 70 years and above and persons with disabilities, while remaining optional for all other individual customers. This prioritization ensures tailored protection for those at higher risk of fraud or exploitation due to age or disability, while allowing for flexibility for the broader customer base.

The applicability focuses on APP transaction initiated by vulnerable customers. Notably, merchant transactions (including UPI, card-based, and net banking payments), recurring payments (e.g., e-mandates, NACH), and cheque-based transactions can be explicitly exempted from these requirements. This distinction ensures that the safeguards target high-

risk peer-to-peer transfers without disrupting routine commercial or automated payment workflows.

The enhanced safeguard mechanism can be in the form of a “trusted person” designated by a vulnerable customer. This trusted individual acts as another layer of authentication for high-value transactions, say, those above ₹50,000. It is noteworthy that nearly 92% of value of frauds reported in NCRP are above this limit. Thus, the threshold balances operational efficiency for smaller transactions with robust protection for larger-value transfers.

Any change of trusted person may be permitted only after a mandatory 24-hour cooling period, thereby ensuring that such decisions are deliberate and informed.

For opting out, vulnerable customers may withdraw from the safeguard system after a 24-hour waiting period following their request. Banks are required to clearly explain the associated risks to the customer before processing such requests, thereby ensuring informed decision-making. Simultaneously, a seamless digital pathway must be provided for these customers to re-enroll in the safeguard system at any time in future, thus maintaining accessibility and flexibility without compromising security. This approach prioritises customer autonomy while embedding safeguards against potential coercion or hasty decisions.

2.3 Pros and Cons

Pros:

- Provides an additional layer of verification by an independent trusted individual who is unlikely to be subjected to the same coercion, urgency, or social engineering pressure as the account holder.
- Particularly useful for account segments with large balances, where the potential financial loss from fraudulent transactions may be significant.

Cons:

- Existing banking practice recognises only the account holder(s) or authorised signatories as legitimate operators of an account. Under this framework, the additional authenticator would neither have a legal nor beneficial interest in the account; yet would effectively influence the execution of outward transactions by virtue of the authentication requirement.
- May result in delays in transaction execution if the trusted individual is not immediately available to authenticate the transaction.

2.4 Brief contours:

Applicability	Mandatory for: • Citizens aged 70 years and above • Persons with Disabilities Optional for: Any other customer (individual)
Scope	• APP transactions to bank accounts done by vulnerable sections. • Merchant transactions (done through any mode, for example – UPI, cards, net banking etc.,) recurring payments (such as e-mandates, NACH based payments) and payments through cheques are proposed to be exempted.
Threshold	Above ₹50,000
Enhanced safeguard	Additional authenticator through a trusted person identified by the vulnerable customer. Any change in the trusted person to be allowed only after a cooling period of 24 hours.
Opting-out	Vulnerable sections can opt-out of the facility after 24 hours of receipt of such a request. In such cases, the bank should clearly explain the attending risks before allowing the opt-out. A digitally seamless avenue for such a customer to opt-in at any time thereafter should also be provided.

Question 7: *Is the coverage of the solution adequate or should any other segment of population be mandatorily covered? Is the age limit reasonable? Should all PwD be covered or only a certain section thereof and, if so, what should be the basis for selection?*

Question 8: *Are there any legal, contractual, or consumer protection concerns regarding the role envisaged for additional authenticator?*

Question 9: *What level and form of due diligence should be prescribed for verifying an additional authenticator who does not maintain a customer relationship with the bank? Whether banks should be permitted to rely primarily on customer declaration and consent, or whether independent verification of the additional authenticator be required?*

Question 10: *Is the suggested threshold of above ₹ 50,000 reasonable?*

Question 11: *What guardrails should be laid out to protect the interests of vulnerable sections choosing to opt out of the facility?*

Option 3: Accounts to receive credits commensurate with nature of relationship with banks

As part of the KYC process, a bank is required to obtain supporting documents in respect of the nature of business and financial status of the customer. Besides, it is also required to undertake ongoing due diligence of an account to ensure that transactions therein are consistent with bank's knowledge about the customer, customer's business and risk profile, the customer's declared sources of funds/wealth, etc. In order to further strengthen these guidelines, and to control use of bank accounts as "mules" to route money proceeds of Digital Frauds, it is proposed to bring in a regulatory measure of limiting aggregate credits in an account without an additional review of satisfactory business relationship.

3.1 Possible approach:

RBI shall prescribe a ceiling, say ₹ 25 lakh, for annual aggregate credits into a bank account for which additional proof in support of genuine requirement of higher aggregate credit is not taken from the customer (hereinafter called as a low credit turnover account).

A bank may fix a limit, not higher than this prescribed ceiling, for such low credit turnover accounts, based on its own internal risk management.

All bank accounts, existing and new, shall have a flag associated with them. If the account is a low credit turnover account, the flag shall be on, and off otherwise. The default flag for each account shall be on. A bank may turn off the flag of an account as per a policy to be formed by it, on the basis of guidance provided by the RBI through regulations / directions. This may be based on income, revenue, turnover, wealth, assets, etc. of the account holder or his / her parents, etc. for which additional documentation shall be taken by the bank.

Whether a flag is to be turned on or not shall be decided at the time of onboarding the customer. However, the flag can be turned on or off even later, based on additional information received by the bank. For existing customers, the bank shall have to take a view as per its policy on the basis of the guidance provided by regulations in a time bound manner, as may be provided by regulations.

A bank account with flag turned on shall receive annual aggregate credit of up to the limit set by the bank. If credit is received beyond this limit, the bank shall permit only shadow credit into the account. Such funds shall be available for utilization only after the bank has satisfied itself that the transaction is genuine, based on additional information and / or documents submitted by the intended beneficiary. However, should a beneficiary not be able to satisfy the bank within a period of, say, 30 calendar days from the date of such shadow credit, the

same shall be reversed and the amount sent back to the source. The bank may also turn off the flag after satisfying itself about the same.

It is clarified that each bank shall continue to comply with the extant Reserve Bank's instructions on KYC including ongoing due diligence.

The overall objective of this approach is to ensure enhanced responsible conduct of bank accounts without unduly inconveniencing genuine customers.

3.2 Pros and Cons:

Pros:

- Strengthens the identification and prevention of fraudulent activities in bank accounts.
- Allows funds to be credited only after proof of genuine activity.

Cons:

- Difficulty in assessing the low credit turnover account
- Additional requests for documentation may lead to customer inconvenience.

3.3 Brief contours:

Accounts covered and exempted	Bank Accounts of Individuals (including joint accounts), Sole Proprietorship Accounts, Partnership Accounts (including LLP). Large accounts such as Corporates, listed companies and of Govt. (Central / State) are not covered.
Cumulative annual aggregate credit threshold	₹25 lakh or below, as determined by the bank, based on its internal risk assessment. A bank can remove this ceiling, based on additional information supported by suitable documents, as required. For existing customers, banks to take a view based on guidance provided by regulations.
Action expected of banks, in case of breach of threshold	Shadow credit to be permitted' with utilization of funds allowed after the bank has satisfied itself based on additional information and / or document(s) shared by customer, failing which the shadow credit shall be reversed after 30 days and the amount sent back to source.

Question 12: *What are the views on this approach, including from the perspective of proportionality?*

Question 13: *Is the suggested threshold of ₹ 25 lakh considered reasonable?*

Question 14: *Are 30 calendar days enough for the customer to satisfy his / her bank for crossing the aggregate credit threshold?*

Option 4: Customer-induced controls

Currently, card-based payment systems provide customers with a 'switch on/off' facility for domestic and international usage as well as for setting limits for different transaction types. This facility has proven effective in empowering customers in terms of enhancing their control over payment instruments and reducing instances of fraud. However, similar user-controlled mechanisms are not uniformly available across other digital payment channels.

4.1 International scenario:

Singapore:

It has formally introduced a customer-controlled 'kill switch'. Customers can instantly lock their online banking account via mobile app or hotline and, thereby, disable fund transfers, digital banking access, and payment functions. Such action can be reversed only after identity verification by the bank.

Australia:

Some banks have rolled out "digital padlock" or "safe block" option, which would allow customers to disable digital access in case they suspect unauthorised activity in their accounts.

4.2 Possible approach:

4.2.1 Transaction level controls

Customers can be provided with digital payment controls which would consist of a 'switch on/off' facility for any digital payment mode as well as for setting limits for different transaction types at the account level.

This would allow customers to control the debit transactions at the account level across any or all digital payment channels. It may be made accessible to the customer either through bank branch visits or through Internet banking, Mobile banking, Phone banking, Interactive Voice Response or any other authenticated bank interfaces.

4.2.2. Kill-switch

Customers may also be provided with a single facility to disable all digital payment transactions from the account ('kill switch') at one stroke.

Kill-switch activation at the account level shall override other controls / configurations set-up by the account holder. Once the kill-switch is enabled, disabling the kill-switch to re-activate digital payments can be permitted either through digital modes after taking proper authentication / verification measures, or through a physical visit to a bank branch by the account holder. For disabling the kill-switch through digital modes, the bank may put in place relatively stringent authentication / verification measures to ensure the genuineness of the customer.

4.2.3 Other aspects

Certain kind of transactions such as payment mandates, standing instructions, etc may be exempted from the controls and kill-switch.

While the digital payment controls and the kill switch can certainly be extended to existing customers as an optional facility, a key policy question is whether or not digital payment modes should be disabled by default for new customers unless explicitly enabled by them.

On one hand, keeping digital payment modes disabled by default for new customers may strengthen the ‘secure by default’ principle. Newly opened accounts are often vulnerable to misuse in cases of identity theft, mule accounts, or onboarding fraud. However, disabling digital payment facilities by default may also affect customer convenience and ease of adoption of digital payments. Many customers today expect immediate access to payment channels such as UPI, cards, and internet banking at the time of account opening.

4.3 Pros and Cons:

Pros:

- This measure strengthens the principle of customer-controlled security. Customers can customise access to payment modes according to their usage patterns and risk appetite.
- In fraud situations, time is critical. A kill switch enables customers to immediately disable all digital payment access without navigating multiple systems or contacting different banks.
- This measure ensures a more uniform and robust customer protection framework across the payments ecosystem.

Cons:

- Customers may inadvertently activate the kill switch or disable certain payment channels, resulting in disruption to legitimate transactions.
- Implementing a universal kill switch across multiple payment channels such as UPI, cards, net banking, wallets, and other digital instruments may require significant technological development for banks.
- The controls may not serve their purpose in cases wherein fraudsters gain temporary access to a customer's device.

4.4 Brief contours:

Scope	Banks may provide customers with a facility to enable or disable digital payment channels (one or all) through various interfaces.
Exemptions	Certain type of transactions may be exempted such as payment mandates, and standing instructions.
Process to reactivate digital payments	Through digital modes or through a physical visit to a bank branch.

***Question 15**: What other transactions, apart from payment mandates and standing instructions, be exempted from the suggested digital payment controls and kill-switch?*

***Question 16**: Should new accounts be "default off" for all the digital payment channels, or should certain low-risk channels be enabled by default? If so, what should these be?*

***Question 17**: If the kill-switch has been applied, should the re-activation of digital payments be facilitated only through visit to a bank branch or through digital channels as well? If the latter, what guardrails should be put in place to check misuse?*

V. Submission of comments and Way forward

i. Comments / feedback on this Discussion Paper, particularly with reference to the key questions raised in the paper and any other matters germane to the subject may be submitted to RBI through 'Connect 2 Regulate' link on RBI website.

ii. After analysing comments received on the Discussion Paper, RBI will consider issuing draft guidelines on introducing additional measures for countering digital payment fraud on its website.

iii. The last date for submission of comments is **May 08, 2026**.

****