Comments on Draft Amendment Directions on 'Conduct of Regulated Entities in Recovery of Loans and Engagement of Recovery Agents', dated 20th May 2026

On 20th May 2026, the Reserve Bank of India released the "Draft Amendment Directions on 'Conduct of Regulated Entities in Recovery of Loans and Engagement of Recovery Agents'" (hereafter "Draft Amendments").

The Draft Amendments provide detailed guidance to relevant regulated entities (REs) on the loan recovery process, including mandatory certification for recovery agents, safeguards against harassment, grievance redressal mechanisms, and compensation for wrongful use of technology-based mechanisms. We believe the Draft Amendments are a step in the right direction and appreciate the RBI's efforts to revisit the framework and incorporate stakeholder feedback through this revised draft.

At the same time, we believe that certain aspects of the Draft Amendments would benefit from additional clarification and deferred implementation. In particular, we submit that: (i) the framework should more explicitly address the repossession of assets financed through unsecured credit facilities; and (ii) the provisions permitting technology-based mechanisms for restricting or disabling mobile device functionalities ("digital kill switches") should be operationalised only after the establishment of a more comprehensive governance framework addressing consumer protection, cybersecurity, vendor oversight, and the prudential treatment of such arrangements. We elaborate on these concerns below.

(I) Curbing Repossession of Assets Financed Through Unsecured Credit

In the context of point-of-sale financing/loans disbursed for the purchase of consumer durables, financing arrangements vary between secured consumer durable loans (where the purchased asset is hypothecated in favour of the lender) and unsecured personal credit facilities, where underwriting is based primarily on the borrower's financial profile. While the Draft Amendments include sufficient guidelines regarding the possession of the security underlying a loan, there are often cases in consumer durable financing where the financed asset is repossessed despite the loan being unsecured.

It is common practice for recovery agents to take possession of the financed asset, dispose of it in the secondary market, and utilise the proceeds to repay the RE bearing the credit risk. This scenario stems from misrepresentation by the recovery agents to the borrower (that the loan covenants allow for repossession) and, potentially, also to the RE bearing the credit risk (that the repayment is sourced from the borrower). While the extant guidelines (and the Draft Amendments) continue to place an onus on the REs to ensure there is no misrepresentation, such practices persist. Given that consumer durable finance is a fast-growing category[1], it would be prudent to address such scenarios explicitly. For example, recovery agencies may be mandated to provide an undertaking that neither they

[1] Consumer durable loans had a CAGR of 23.3% between FY 16 to FY 26. See Economic Survey 2025-26 Statistical Appendix https://www.indiabudget.gov.in/economicsurvey/doc/stat/tab3.2.pdf

nor their related parties will enter into any commercial arrangement involving borrowers who are subject to recovery proceedings. Further, post-recovery telephonic confirmation with borrowers in cases involving unsecured consumer durable finance may also be considered to ensure that customers were not misled or coerced into surrendering the financed asset to settle an unsecured loan. Such measures would ensure that recovery actions remain aligned with the actual nature of the underlying credit facility and the customer's understanding of the financing arrangement.

(II) Technology-Based Recovery Mechanisms Require a Comprehensive Regulatory Framework

A significant change between the February draft[2] of the amendments and the current Draft Amendments is the express legitimisation of "deploying any technology-based mechanism for restricting or disabling the functionalities of a mobile device of a borrower" (hereinafter, "digital kill switch"), whereby a lender may remotely restrict certain functionalities of a device purchased using credit upon the occurrence of a default. Before addressing the concerns arising from such mechanisms, it is important to situate the development in context. In 2024, the RBI had restricted lenders from deploying such digital locking mechanisms[3]. Subsequently, in October 2025, Deputy Governor Rajeshwar Rao reportedly observed that: "*The issue of digital locking is under examination. As the Governor had pointed out, there are pros and cons on both sides in terms of balancing the customer rights and requirements, data privacy and also the creditors' requirements. So, we are examining the issue, we will evaluate the pros and cons and then take a view at a later point in time*."[4]

These developments, including the RBI's earlier interventions, suggest that the use of such mechanisms raises significant concerns regarding customer protection and cybersecurity risks. Importantly, such concerns are not limited to situations involving borrower default. Even where borrowers remain regular with their repayment obligations, the existence of a digital kill switch continues to create privacy and cybersecurity concerns. Such technologies necessarily require elevated device-level permissions and centralised administrative controls, potentially enabling access to all device-level data and metadata[5].

The Draft Amendments attempt to address these concerns by providing that an RE "*shall neither access or use nor obtain or retain the data stored in the mobile device of a borrower for the purpose of loan recovery or any other purpose under any circumstances*." However, the present drafting appears limited to data "stored" on the device and does not expressly

---

[2] "Draft Reserve Bank of India (Commercial Banks - Responsible Business Conduct) Second Amendment Directions, 2026." Reserve Bank of India, February 12, 2026. https://www.rbi.org.in/scripts/bs_viewcontent.aspx?Id=4886

[3] Agarwal, Rishika. "Smartphone Loan Defaults Rise after RBI Stops Remote Locking of Devices." *Business Standard*, November 28, 2025. https://www.business-standard.com/finance/personal-finance/smartphone-loan-defaults-rise-rbi-remote-locking-devices-125112800367_1.html

[4] Ibid.

[5] See Yamin, Muhammad Mudassar, and Basel Katt. "Mobile Device Management (MDM) Technologies, Issues and Challenges." *Proceedings of the 3rd International Conference on Cryptography, Security and Privacy*, January 19, 2019, 143–47. https://doi.org/10.1145/3309074.3309103

address data transmitted to or from the device. A creative interpretation of the regulations can, therefore, defeat the intended purpose. For example, when a borrower makes a phone call, the conversation itself is not ordinarily "stored" on the device. Nevertheless, a technology-based mechanism that possesses access to the device's microphone and audio systems could potentially intercept or record such communications. Similarly, while browser history may be stored on the device, information about websites being accessed in real time may not necessarily fall within a narrow interpretation of "stored" data. Essentially, there is a distinction between data in "storage" and data in "transit". As a result, a narrow interpretation of the term "stored data" may substantially dilute the privacy safeguards sought to be introduced through the Draft Amendments. Additionally, the restriction is framed as an obligation upon the RE. However, such technology-based mechanisms are often designed, maintained, and operated by specialised third-party vendors (elaborated in the following paragraph). It is unclear whether equivalent restrictions apply to such vendors. Consequently, a situation may arise where the RE remains technically compliant with the Draft Amendments while the vendor continues to access, process, or retain borrower data in the course of operating the software. While lenders and third-party vendors would remain subject to the Digital Personal Data Protection Act, 2023, the Draft Amendments do not expressly incorporate or operationalise several of the privacy principles, such as data minimisation, purpose limitation, and retention controls, among others, which are particularly relevant in the context of technology-based recovery mechanisms. In such a scenario, the formal requirements of the Draft Amendments may be satisfied while the underlying privacy concerns remain unaddressed.

Further, the Draft Amendments specify that "*the technology-based mechanism deployed for restricting the functionalities of the mobile device shall be uninstalled soon after the loan is repaid in full*." This requirement appears to implicitly contemplate a mechanism deployed by the financier rather than an OEM-integrated framework. At present, such technologies broadly operate through two models: (i) OEM-level device locking mechanisms integrated into the device; and (ii) proprietary software tools deployed by lenders, often through specialised third-party vendors. It is only in the latter scenario that the lender may realistically "uninstall" the mechanism upon repayment of the loan. In the former scenario, while the lender may choose to relinquish access to the control interface, the underlying capability remains embedded within the device.

This distinction raises several additional questions relating to vendor governance, contractual allocation of liability, cybersecurity oversight, audit standards, and the regulatory treatment of third-party technology service providers involved in such arrangements. Without these clarifications, the Draft Amendments do not comprehensively address concerns relating to data protection, privacy rights, and potential customer harms. These are foundational to the broader question of permitting REs to deploy digital kill switches. It is therefore prudent for the RBI to first establish a comprehensive governance framework addressing these mechanisms before formally permitting their use.

Finally, permitting lenders to restrict or disable functionalities of a borrower's mobile device raises a more fundamental question regarding the regulatory characterisation of such financing arrangements, particularly whether the underlying facility should be treated as secured or unsecured credit. The ability of a lender to technologically restrict the use of the financed device resembles a form of collateral-like control over the underlying asset. However, where the loan itself continues to be treated as unsecured credit, such controls appear to extend beyond the ordinary contours of unsecured lending, under which the lender ordinarily bears the credit risk without recourse to the financed asset. The Draft Amendments, therefore, appear to create an intermediate framework that does not fit neatly within conventional classifications of secured or unsecured lending. REs are effectively granted significant functional control over the financed asset without a corresponding clarification of the prudential or regulatory treatment of such facilities. This may create downstream regulatory implications that extend beyond recovery practices, including risk-weight assignment, supervisory reporting, underwriting standards, and broader prudential treatment.

Accordingly, we submit that several upstream and downstream regulatory questions need to be resolved before operationalising such mechanisms. As such, it may be prudent for the RBI to defer the implementation of the provisions relating to digital kill switches pending the formulation of a broader, more comprehensive regulatory framework governing their use.

About Dvara Research

Dvara Research is an independent, non-partisan, not-for-profit policy research institution based in India. Its mission is to ensure that every low-income household and every small enterprise has complete access to suitable financial services and social security through a range of channels that enable them to use these services securely and confidently.

Since 2008, Dvara Research has deeply analysed, and carefully written about, financial inclusion and social protection in India from policy, regulatory, and practitioner perspectives that are anchored to its mission.

Its work has gained the admiration and respect of policymakers and regulators, and since its inception, Dvara Research has been a research-partner of choice for such key policy-making bodies as the Reserve Bank of India, Securities and Exchange Board of India, Pension Fund Regulatory and Development Authority etc.

Website: https://dvararesearch.com