Digital Microloans in Sri Lanka: Closing Regulatory Gaps and Protecting Borrowers

Digital microloans are proliferating in Sri Lanka, promising fast, flexible credit, particularly for people excluded from mainstream financial institutions and serving urgent needs. Borrowers use these services to meet expenses relating to rent, medical costs, personal emergencies, business costs and children's expenses, often because banks are too slow, too laborious or require collateral they do not have. Apps promote instant approval, minimal documentation and low or zero interest. However, borrowers report opaque terms and conditions, hidden and unpredictable fees, repeated rounds of borrowing to repay existing debts, and aggressive debt collection practices. Reviews of loan services also reveal major risks around transparency and personal data protection. The interconnected and coordinated nature of Sri Lanka's digital microlending ecosystem adds to the complexity of the problem.

Regulatory gaps and the absence of clear oversight leave borrowers exposed to harmful practices. In addition to regulation as a financial service, there are wider risks to be addressed relating to data protection, cyber harassment, consumer protection, and the economic insecurity driving reliance on digital loans.

This Policy Note highlights some of these key gaps and recommends a coordinated response.

Key findings from the study:

- Borrowers often turned to these services to meet urgent needs such as rent, medical expenses, business costs and children's expenses. Most borrowers did not use formal financial institutions as they took too long, had onerous requirements, or asked for collateral they could not provide.
- Loan services marketed instant approvals and low or zero interest, yet borrowers frequently reported service fees and late fees that add to borrowing costs. Many borrowers fell into cycles of repeat borrowing to repay existing debts.
- Borrowing terms and privacy policies were vague and often unavailable in local languages and restricted borrowers' ability to provide informed consent for the terms of the loans they obtain.
- Loan apps collected pervasive personal, financial and device data, including accessing photographs, location and contacts from borrowers' devices. Companies reserved broad powers to share it with third parties, retain it for unspecified periods, and transfer it internationally.
- Borrowers who defaulted faced multi-faceted distress - repeated phone calls, threats, intimidation and reputational harm, which damages relationships, employment prospects, and mental wellbeing.
- Many loan service apps seem to share developers, marketing strategies and ownership structures, and are linked to international financial technology networks. This suggests a network of companies that makes it challenging for any single regulator to trace and regulate.

1. Regulatory Gap in Digital Lending

Digital microloan services in Sri Lanka operate in a regulatory black hole. The Central Bank of Sri Lanka (CBSL) regulates only deposit-taking institutions and can take action on illegal deposit taking activities. As these digital microloan services do not accept public deposits, they do not fall under the CBSL's regulatory ambit. The Microfinance and Credit Regulatory Authority Act No. 9 of 2026 provides a potential route to address this gap, but it is yet to be implemented. The Act provides for the regulation of money-lending and microfinance businesses, including those carried out through digital or electronic means. However, as at the time of writing, it is unclear as to when the Authority will be established, as it appears that the Act is being revised even before coming into operation. Delays in operationalising the Act and the Authority continue to leave borrowers exposed to practices that existing oversight cannot adequately address.

Policy Recommendations

- **Fastrack the operationalisation of the Microfinance and Credit Regulatory Authority (MCRA)**: The MCRA's regulatory ambit must explicitly cover money-lending and credit activities conducted through digital platforms and mobile applications. The Authority must be given the authority to establish a licensing and oversight framework for digital money-lending businesses. It must also have the technical and enforcement capacities to regulate interest fees, rates and loan recovery practices, enforce the disclosure of all terms and conditions, and implement effective systems for receiving and resolving borrower complaints.
- **Issue interim warnings and public notices about digital microloan services**: While the MCRA is being established, CBSL should continue to communicate relevant warnings about online lending risks and financial fraud within its existing mandate. This effort should be complemented by coordination with the Computer Crimes Division of the Sri Lanka Police (CCID) and the Sri Lanka Financial Sector Computer Security Incident Response Team (FinCSIRT).
- **Establish a coordinated framework for regulatory oversight and enforcement**: Clear coordination mechanisms between the MCRA, the CBSL, the Consumer Affairs Authority (CAA), FinCSIRT and CCID are necessary to address complaints involving overlapping mandates. This should include referral procedures, defined institutional responsibilities and information-sharing arrangements to ensure that complaints are directed to the appropriate authority and that harmful practices do not fall through gaps in oversight.

2. Data Protection, Digital Governance and Digital Literacy

Digital microloan services collect extensive amounts of borrowers' personal information. While some of this collection might be warranted to assess the creditworthiness of a borrower, it raises concerns about whether this data is collected, used and shared with adequate consent and safeguards. The misuse and dissemination of borrowers' personal information has exposed them to harassment, coercion and reputational harm. Existing legal and institutional mechanisms have different mandates: the Personal Data Protection Act No. 9 of 2022 provides a framework for data protection, the Computer Crimes Investigation Division (CCID) of Sri Lanka Police investigates cybercrime, and the Sri Lanka Computer

Emergency Readiness Team (SLCERT) provides technical and incident-response support. However, gaps in implementation, enforcement and institutional responsibilities can leave borrowers without effective redress.

Policy Recommendations

- **Prepare for the implementation of the Personal Data Protection Act No. 9 of 2022 (PDPA)**: The Data Protection Authority (DPA) should prioritise preparatory measures to ensure that digital lending services are required to comply with applicable data protection requirements ahead of the enforcement of the Act in January 2027. This should include issuing sector-specific regulations regarding informed consent, the collection and use of personal information, and the sharing of borrowers' data with third parties. Borrowers should be able to understand what information is collected, why it is needed, for how long it is retained and how it may be used or shared.
- **Establish clear channels for reporting cyber incidents and harassment**: SLCERT, FinCSERT and the CCID should clarify how borrowers can report incidents involving unauthorised disclosure of personal information, threats, digital harassment and other suspected cybercrime. SLCERT should provide technical guidance and incident-response support within its remit, while suspected criminal conduct should be referred to FinCSERT and the CCID for investigation. Public-facing guidance should explain these distinct roles and how complaints can be escalated.
- **Strengthen public awareness of digital safety and borrowers' rights**: Lack of borrower awareness of the importance of protecting personal data, recognising suspicious loan offers and understanding application permissions is a threat to the implementation and sustainability of any regulatory oversight. A coordinated campaign from all relevant agencies to strengthen borrower awareness of digital safety and borrower rights is necessary.
- **Ensure digital transformation includes safeguards for vulnerable users**: The Ministry of Digital Economy should consider the risks that digital lending presents for personal data protection, cybersecurity and consumer rights within its digital transformation agenda. In coordination with the relevant regulatory authorities, it should support the integration of safeguards and accessible complaint information into digital public awareness initiatives. Its role should complement, rather than substitute for, the statutory responsibilities of the MCRA, DPA, CAA and cybersecurity authorities.

3. Social Protection and Household Vulnerability

Digital microloans must be understood in the context of the economic insecurity that drives people to seek fast, accessible credit. Borrowers turn to these services to meet urgent expenses, including utility bills, health emergencies, household needs and livelihood costs, often when formal credit is inaccessible and when social protection schemes have gaps. Predatory lending cannot be addressed through financial regulation alone; any regulatory response must remain attentive to the economic circumstances that have created - and are likely to continue to create - demand for these services. Primarily, the lack of adequate and meaningful social welfare schemes for the most vulnerable communities, and safety nets during times of economic downturn or adverse climate events (like flooding during Cyclone Ditwah) needs emphasis.

Policy Recommendations

- **Invest in a constellation of social protection measures**: Rather than relying primarily on cash transfers, insurance and pension schemes, social protection must address the underlying causes of household vulnerability. It should focus on increasing financial resourcing for health and education, creating sustainable livelihood opportunities, better worker protections for the informal sector (for example, paid leave and sick leave), and other mechanisms that support families across the spectrum and make them less dependent on predatory lending.
- **Support accessible, community-based financial alternatives**: The Department of Development Finance and other relevant public institutions should examine opportunities to support cooperative and community-based credit mechanisms that provide accessible financing for households and small-scale livelihoods. Any support should include appropriate safeguards, transparent terms and accountability, so that alternatives do not reproduce the harmful practices associated with predatory lending.

A coordinated response

Digital microloans sit at the intersection of financial regulation, consumer protection, data governance, cybersecurity, law enforcement and social protection. The interconnected operations and cross-border links of digital microlending services providers make it difficult for any single institution to address the full range of risks.

Sri Lanka has an opportunity to close these gaps through a coordinated response. Establishing the Microfinance and Credit Regulatory Authority is an important step, but it must be accompanied by transparent lending standards, effective complaint mechanisms, stronger data protection and cyber response, and measures that address household vulnerability.

The objective should not be to leave people without access to credit. Digital financial services can provide an important source of funding for people excluded from traditional banking. The priority is to ensure that access to credit does not expose borrowers to opaque costs, abusive recovery practices or the exploitation of their personal data.

A comprehensive response must protect borrowers while creating pathways to appropriate credit and stronger economic security.

Scan the QR code to access the report, *"In the Shadows of Fast Credit: Examining Digital Micro Lending in Sri Lanka."*

Centre for a Smart Future is an Asia-centric public policy think tank based in Colombo, Sri Lanka with interdisplinary researchers, advisors, practitioners and partners around the world.

Our partners include London School of Economics, Cambridge University, Max Planck Foundation, ADB, Open Society Foundations, UNICEF, Blue Resources Trust, The Asia Foundation, Gamani Corea Foundation, Biodiversity Sri Lanka, Parliament of Sri Lanka, Institute of Development Studies (UK), SEVANATHA Urban Resource Center, and others.

This is a publication under CSF's thematic pillar on:
Inclusive Technology and Innovation

Under this pillar, we conduct research and policy engagement on platform-based gig work, governance of digital policies and national digital transformation, and digital inclusion and equity in areas such as social protection and education.

This Policy Note was authored by Piyumi Wattuhewa (Junior Researcher) under the guidance of Anushka Wijesinha (Director).

@CSFasia
@csfasia
@centreforasmartfuture
@centreforasmartfuture

www.csf-asia.org