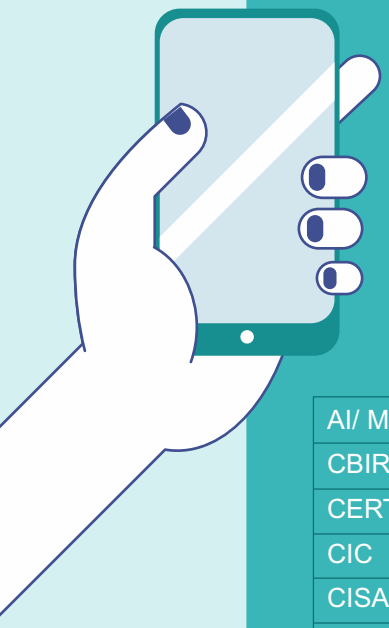
CHASE INDIA

Whitelisting Framework for Digital Lending Apps (DLAs)

Report | April 2023



Abbreviations

AI/ ML	Artificial Intelligence/ Machine Learning
CBIRC	China Banking and Insurance Regulatory Commission
CERT-IN	Computer Emergency Response Team India
CIC	Credit Information Company
CISA	Cybersecurity and Infrastructure Security Agency
Customer/ User/ Borrower/ Consumer	For the purposes of this report, the words are used interchangeably
DEA	Department of Economic Affairs
DLAs	Digital Lending Apps/ Platforms
DLG	Guidelines on Digital Lending
DPDP Bill	Draft Digital Personal Data Protection Bill
ED	Directorate of Enforcement
FBS Lending	FinTech Balance Sheet Lending
GST	Goods and Services Tax
GSTIN	Goods and Services Tax Identification Number
IT	Information Technology
KFS	Key Fact Statement
KYC	Know Your Customer
MCA	Ministry of Corporate Affairs
MeitY	Ministry of Electronics and Information Technology
MOF	Ministry of Finance
MSME	Micro, Small and Medium Enterprise
NBFC	Non-Banking Financial Company
PA	Payment Aggregator
PAN Card	Permanent Account Number Card
PG	Payment Gateway
RBI	Reserve Bank of India
REs	Regulated Entities
SAR	System Audit Report
SRO	Self-Regulatory Organisation
WGDL	Working Group on Digital Lending

Index

Foreword 1

Executive Summary 2

1. Background 3

2. Need for Regulation 4

3. Whitelisting Framework 5

- 3.1. General Establishment Requirements 6
- 3.2. Technology and Data Requirements 6
- 3.3. Customer Protection and Grievance Redressal Requirements 11
- 3.4. Other Requirements 12

4. Global Overview 13

5. Way Forward 14

References 16

Foreword

While India's banking and digital payments penetration improved rapidly in the past decade, the country has also started witnessing a similar scenario with respect to credit and lending. As per a recent study titled 'Empowering Credit Inclusion: A Deeper Perspective on Credit Underserved and Unserved Consumers', about half of India's population stood credit unserved by the end of 2021. This gives a glimpse into the scale and scope for credit offtake in India and the untapped potential of Indian credit markets. The growth and development of India's digital infrastructure has a key role to play in this respect.

The proliferation of smartphones, access to cheap data, rise in financial literacy, and financial inclusion have already created the right environment for FinTech apps to flourish and overcome the long-prevailing challenge of ease of access to credit. There is enough evidence suggesting that these applications have acted as a bridge to unserved or underserved credit markets and for this reason, they are witnessing a steep growth rate. Reports suggest that India's digital lending market, currently valued at $270 billion, is likely to grow to a $1.3 trillion valuation by 2030.

Although FinTech revolutionised India's credit markets, the rapid sectoral growth brought along its own set of perils. Borrowers bore the brunt of unchecked digital lending practices which took the form of lending at exorbitant interest rates, unethical and predatory recovery practices, additional hidden charges in lending transactions, misuse of customers' data, etc. While a favourable policy and regulatory infrastructure for digital lending services is in the pipeline, it is imperative to simultaneously look into and shape a framework for consumer focused applications/ platforms to ensure their protection.

The Union Finance Minister has also raised the same concern and has undertaken an exercise to whitelist loan apps. On this backdrop, this report attempts to supplement such an exercise by attempting to identify the key aspects of what can be termed as a 'Whitelisting Framework for Digital Lending Apps (DLAs)' in order to weed out illegal loan apps.

Dr. Deepali Pant Joshi
Former Executive Director, Reserve Bank of India &
Senior Advisor, Chase India

Executive Summary

India's digital lending sector is likely to emerge as the backbone for higher credit penetration and vision of financial inclusion. However, keeping in view the protection and safety of borrowers, the government has stepped up regulatory action against applications/ entities involved in unethical lending practices. While the RBI unveiled its digital lending guidelines in September 2022, it has simultaneously started conducting a whitelisting exercise to weed out illegal loan apps for borrowers' safety.

India's trajectory of policy and executive actions undertaken by the government for digital lending started circa 2020. Cases concerning unethical digital lending were brought to the government's notice and the RBI issued a cautionary notice to borrowers which was followed by the Working Group on Digital Lending (WGDL) Report. Meanwhile, the Enforcement Directorate (ED) cracked down on entities running/ supporting illegal loan apps. Based on the WGDL Report, the RBI issued the Digital Lending Guidelines (DLG) for all entities involved in the digital lending ecosystem. A week after the RBI notified the DLG, the Union Finance Minister called a meeting on illegal loan apps and it was suggested that the RBI should prepare a whitelist of DLAs.

In a latest development, MeitY issued ban on some of the DLAs and in response to a Rajya Sabha question it was further unveiled that the names of such whitelisted apps was provided by RBI to MeitY as part of a whitelisting exercise. Most recently, Google updated process of registration for the apps facilitating personal loans on its platform in its policy update of April 2023, to be effective from May 31st, 2023 aligning the same with the efforts being taken by RBI and MoF.

In its efforts to support the government to build a legal, procedural & technical framework for compliance on a regular basis, this report delineates 4 key aspects of DLAs' Code of Conduct –

- General Establishment Requirements *(Formation of Legal Entity, GST Registration, Website and Internet Presence)*;
- Technology and Data Requirements *(Data Storage and Collection, Privacy Policy, Security Standards, Data Access and Data Localisation)*;
- Customer Protection and Grievance Redressal Requirements *(KYC Guidelines and Key Fact Statement)*; and
- Other Miscellaneous Requirements *(Reporting Requirements, Compliance with Credit Information Companies Regulation Act, 2005 and Prevention of Misleading Advertisements and Endorsements for Misleading Advertisements, 2022, and Risk Management).*

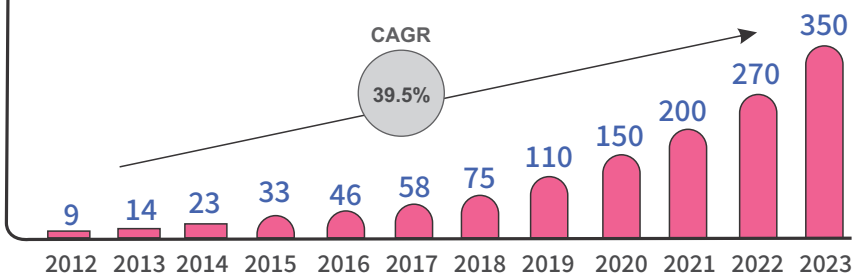
The report also provides a brief overview of the global approaches towards regulation of lending services provided.

Moreover, the report concludes by suggesting that fostering a favorable policy and regulatory ecosystem for digital lending will enable the sector to grow, which will in turn boost not only India's agenda for financial inclusion but also improve credit offtake for MSMEs. The report aims to enable the regulators and the industry to build a compliant framework which delineates essential requirements, practices and standards that should be followed by DLAs to ensure safety of users and foster growth of the sector. Establishment of SROs or dedicating a Nodal Agency within the Regulator's purview may also be explored for quick, easy and effective implementation of the devised Whitelisting Framework. Upon this and other areas identified through research in this report, dialogue can be promoted between government and industry stakeholders with respect to the approach and measures that should be undertaken to whitelist the DLAs for borrower protection.

1. Background

India witnessed twelvefold increase in the digital lending sector as per the WGDL report of the RBI. However, owing to unchecked industry practices, customers bore the brunt of unscrupulous lending practices such as providing loans at excessive interest rates, unethical and predatory recovery practices, additional hidden charges applicable on lending transactions, misuse of customers' data, and much more. The rising cases of suicides and other crimes across India due to gruesome lending practices did not escape the government's attention.

Growth of Digital Lending in India (in USD billion)[1]



Source: A Review of India's Credit Ecosystem – joint report by Experian and Invest India

With many individuals falling prey to the unscrupulous and usurious digital lending practices adopted by unauthorised DLAs, the RBI issued a Press Release on 23rd December 2020, warning consumers to be cautious while taking loans from such entities.

These concerns led RBI to set up the WGDL on 13th January 2021. WGDL was presented with a wide array of representation across public sectors as well as industry players. The WGDL report released on 18th November 2021 wherein it recommended the creation of a "*list of NBFCs and the brand names and apps associated with them, which will serve as a whitelist of all the regulated apps in public domain.*"

Based on WGDL's Report, the RBI issued a Press Release on Digital Lending in August 2022, wherein recommendations made by the RBI's WGDL were identified for implementation; for in-principle approval requiring further examination; and for consideration by legislature stating further detailed guidelines. Pursuant to the Press Release, the RBI issued Guidelines on Digital Lending (DLG) in September 2022. The DLG laid out norms for players in the digital lending ecosystem with respect to their conduct, loan disbursal methods, fee/ charges, mandatory disclosures to customers, and grievance redressal measures, to name a few.

In addition to the action undertaken by the RBI, the ED stepped up its investigation into loan app fraud cases and harassment of borrowers on account of loans. In its probe into loan app fraud cases, the ED froze funds of many entities under the anti-money laundering law, to the tune of INR 9.82 crore.

Also, in a latest development in February 2023, MeitY issued ban on some of the DLAs as part of a whitelisting exercise. A Rajya Sabha response in this regard further unveiled that the names of such whitelisted apps was provided by RBI to MeitY. After this development, recently Google Playstore also tweaked its policy for listing of DLAs in lines with the latest guidelines and progress in the sector.

2. Need for Regulation

CREDIT GAP-RELATIVE TO GDP

Source: FinTech-led Digital Lending: Coming of Age – Joint Report by Experian and DLAI

As per a survey, 83% of small business owners in India are unable to access finance despite the government and the regulator introducing several measures to improve credit offtake among MSMEs. Lack of availability of adequate and timely credit, collateral requirements, high cost of credit, etc., are some reasons that hinder credit offtake among MSMEs. In such a scenario, digital lending can be the MSME sector's panacea as DLAs provide timely access to low-value credit using alternate data, which traditional banking is yet to offer. However, this solution of digital lending for all seems far from the reality till the time the domain is well overlooked and supervised, at least, if not heavily regulated.

The lack of regular cash flow and cash flow constraints experienced by MSMEs led them to approach loan apps which offer "Instant Loans" based on algorithmic lending. While algorithmic lending leads to swift onboarding of customers there were many catches like non-disclosure of actual interest rates, hidden charges etc. which led MSMEs as well as individuals into debt traps. Hence the need to pay heed to the rising concerns out of unchecked and unscrupulous digital lending practices was felt to enhance consumer protection, foster economic growth, and curtail adverse socio-economic effects.

Microlending gathered pace in the Indian market when pandemic pushed people under severe financial stress due to which scores of illegal and fraudulent apps became popular among unsuspecting customers. These apps successfully attracted many borrowers, leading to numerous cyber and financial frauds being reported for mis-selling, data privacy breaches, unfair business conduct, charging of exorbitant interest rates, and unethical recovery practices.

Such illegal apps use unsecure technological tools, weak and exposed cyberspace, and unsafe software that leave borrowers vulnerable to financial fraud and expose India's critical financial data outside the national borders. The prevalence of such apps could spell danger for India's economy as it can disturb the entire credit market, dampen the government's financial inclusion initiatives, and instill fear in consumers' minds through data privacy violations. To attract many customers, these platforms skip the due diligence needed to ensure borrowers' credibility, which may lead to unpredictable inflation because of an unstable repayment system.

While regulations were released to monitor the digital lending ecosystem in India, it was also important to ensure that DLAs which indulge in unauthorised and usurious practices are not accessible to customers, to ensure their protection. Therefore, the need for whitelisting of loan applications was felt. Through a whitelisting exercise, only legally recognised DLAs will be available to consumers on Playstores/ App stores i.e., such a whitelisting exercise will allow market access only for identified DLAs.

In this regard, on 9th September 2022, a week after the RBI notified the DLG, Union Finance Minister Nirmala Sitharaman chaired a meeting on 'Illegal Loan Apps' and the issues arising out of them. The meeting was attended by senior representatives from the Department of Economic Affairs (DEA),

Ministry of Finance (MoF), Ministry of Electronics and Information Technology (MeitY), the Reserve Bank of India (RBI), and other relevant government bodies.

It was suggested in the meeting that the RBI would prepare a whitelist of illegal loan apps, and MeitY will ensure that only identified apps are listed on app stores. In addition, it was also decided in the meeting that the RBI would monitor 'mule/ rented' accounts used for money laundering, the RBI would review/ cancel dormant NBFCs to avoid misuse and also ensure registration of payment aggregators (PAs) within a timeframe and no un-registered payment aggregator be allowed to function after that. It was also decided that the Ministry of Corporate Affairs (MCA) would identify shell companies, and all other Ministries/ Agencies would strive to prevent operations of illegal loan apps and would take steps to increase cyber awareness.

The government's decision to whitelist loan apps fulfills the need of the hour, since challenges posed by illegal loan apps *(such as suicides resulting from loan frauds and unethical harassment of borrowers, among other unscrupulous lending practices)* have given rise to a new socio-economic evil. Thus, this step is critical for both – consumer welfare as well as economic security. Whitelisting of illegal loan apps will not only benefit the consumers by helping them avoid falling prey to gruesome lending practices, but will also protect the image of legitimate DLAs from being tarnished by the extreme instances and mishaps reported in the past few years. Hence, the market players will also benefit from such an exercise as it will add more credibility and stability to this evolving sector.

3. Whitelisting Framework

A whitelisting framework for DLAs will serve as the blueprint laying down criteria for legitimate DLAs. This framework will be based on relevant rules and regulations which have been previously identified, practised or proposed for the digital lending sector as well as other relevant sectors, for instance data protection, IT, etc.

The WGDL also made observations and suggestions on the whitelisting of DLAs. Some of these are:

- Establishment of Self-Regulatory Organisation for the digital lending ecosystem,
- DLAs to be verified by an independent nodal agency,
- Identification of baseline technology standards,
- Prior and explicit consent received from borrowers for collection of data with verifiable audit trails,
- User data to be stored in servers located in India,
- Designing a Code of Conduct to govern use of unsolicited commercial communications,
- Maintaining a 'negative list' of Lending Service Providers,
- AI/ ML used in digital lending must be ethical and transparent, etc.

On the basis of aspects identified and discussed in the RBI's WGDL Report, the RBI's Guidelines on Digital Lending, global regulatory approaches for digital lending, India's extant laws/ regulations for various other sectors etc. the following key features and requirements for whitelisting of DLAs have been identified in this report:

3.1. General Establishment Requirements

3.2. Technology and Data Requirements

3.3. Customer Protection and Grievance Redressal Requirements

3.4. Other Requirements

3.1. General Establishment Requirements

(For regulators and the government to monitor & supervise the digital lending ecosystem in India, it is crucial that the entities are duly registered under Indian laws and regulations. In this regard, government may also explore additional establishment and structure requirements owing to the sensitive nature of services offered.)

3.1.1. Legal Entity

- Any organisation providing digital lending application/ platform services in India must be a legal entity in the form of a company registered under the Companies Act of India which should have a proper board composition with board members having required residential status, business integrity and acumen. The company must follow all the rules regarding all the required internal and external committees of the board and other laws laid down in the Act and pertaining rules therein.
- The ownership of the company must be well diversified as per the relevant laws.
- Neither the company nor any of the promoters/ directors of the company should have been convicted of any economic offence or offence, including moral turpitude, in the past. The directors/ promoters should be in line with the 'fit and proper' criteria envisaged by the RBI.
- The company should have a minimum net worth of INR15 crore, which should gradually be increased to INR 25 crore in the period of the next 3 years and shall be maintained at all times. However, such figures may be decided by the lawmakers post analysis and consultation with the stakeholders in the domain.

3.1.2. GST Registration

- The company must have valid registration certificates required for the purpose of taxation i.e., PAN Card, GST Registration Certificate, GSTIN etc.
- The company shall file all the returns and reports in a timely manner.

3.1.3. Internet Presence

- The company must have a registered domain name and a fully developed website which shall be duly maintained, updated and functional with the latest information at all times.

3.1.4. Website Link[1]

- The company should have links to the website/ application where further/ detailed information about the loan products, the rate of interests, the risk factors *(if it's a peer-to-peer lending platform)* of the lender, other partners, particulars of customer care, link to sachet portal, features, fees, minimum and maximum period for repayment, risks, benefits of loan products, maximum annual percentage rate, the representative example of the total cost of the loan, along with the privacy policy that comprehensively discloses the access, collection, use, and sharing of personal and sensitive user data etc. which can be accessed by the borrowers/ customers.
- It shall be ensured that all such details are available at a prominent single place on the website as well as on the app and the application for ease of accessibility.

3.2. Technology and Data Requirements

(A robust technological infrastructure is the backbone of a transparent and credible digital lending ecosystem as it prevents scams/ mishaps which may cause collective damage to the economy as well as society. Also, a lot of data is shared by the consumers with DLAs to avail the services and in the wake of recognition of the Right to Privacy as a Fundamental Right, it's important to identify baseline standards for data accessibility to uphold the Right of Privacy of every individual availing such services.)

1 Digital Lending Guidelines (DLG), 2022.
2 Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules (SPDI Rules), 2011.
3 Draft Digital Personal Data Protection (DPDP) Bill, 2022.
4 Digital Lending Guidelines (DLG), 2022.

3.2.1. Consent for Data Collection & Storage[2,3,4]

- The DLAs, while dealing with any information which includes personal information (as described herein), shall obtain prior consent from the data principal for collection of data. Such personal information consists of information relating to — (i) password; (ii) financial information such as bank account or credit card or debit card or other payment instrument details; (iii) physical, physiological and mental health condition; (iv) sexual orientation; (v) medical records and history; (vi) biometric information; (vii) any detail relating to the above clauses as provided to body corporate for providing service; and (viii) any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise; or (ix) any other information recognised as personal information as per the DPDP Bill (after its enactment).
- DLA or any person on its behalf shall not collect personal data or information unless — (a) the information is collected for a lawful purpose connected with a function or activity of the entity or any person on its behalf; and (b) the collection of the sensitive personal data or information is considered necessary for that purpose. The DLAs should also disclose the purpose of obtaining borrowers' consent at different stages as is decided by the concerned authority/ regulator. Such stages may, for instance, be at the time of installation of app, approval and sanctioning of loan, disbursement of loan etc.
- DLAs to use collected information only for the purpose for which it has been collected.
- DLAs should not store personal information of borrowers except some basic minimal data (viz., name, address, contact details of the customer, etc.) that may be required to carry out their operations. Also, DLAs should be prohibited from collecting/ storing biometric data, unless such storage/ collection is required under extant statutory guidelines.
- While collecting information or asking access to services on the users' device like contacts, camera etc. directly from the person concerned, the DLA or any person on its behalf shall take explicit consent to ensure that the person concerned is having the knowledge of — (a) the fact that the information is being collected; (b) the purpose for which the information is being collected; (c) the intended recipients of the information; and (d) the name and address of — (i) the agency that is collecting the information; (ii) the agency that will retain the information and

  (iii) the agency that will process the information further; (e) restrictions on the use of data; (f) data destruction protocol; (g) standards for handling security breach.
- Every request for consent shall be presented to the customer in a clear and plain language. The DLA shall give to the customer the option to access such request for consent in English or any language specified in the Eighth Schedule to the Constitution of India.
- The request for consent shall also include contact details of the grievance officer or any other person authorised by the DLA to respond to any communication from the customer for the purpose of exercise of their rights.
- DLA or any person on its behalf holding personal data or information shall not retain that information for longer than is required for the purposes for which the information may lawfully be used or is otherwise required under any other law for the time being in force.
- DLA or any person on its behalf to permit the providers of information, as and when requested by them, to review the information they had provided and ensure that any personal data or information found to be inaccurate or deficient shall be corrected or amended as feasible, "provided that the DLA shall not be responsible for the authenticity of the personal data or information supplied by the provider of information to such DLA or any other person acting on behalf of such DLA."
- DLA or any person on its behalf shall, prior to the collection of information including personal data, provide an option to the provider of the information to not to provide the data or information sought to be collected. The provider of information shall, at any time while availing the services or otherwise, also have an option to withdraw consent given earlier to the DLA. The ease of such withdrawal shall be comparable to the ease with which consent may be given. In the case of provider of information not providing or later withdrawing their consent, the

entity shall have the option not to provide goods or services for which the said information was sought.

- If provider of information withdraws consent, the DLA shall, within such timeframe as may be decided by the lawmakers post analysis and consultation with the stakeholders in the domain, cease and cause its agencies to cease processing of personal data of such provider of information unless such processing without the provider's consent is required or authorised under the provisions of any law for the time being in force.
- After the enactment of DPDP Bill, the provisions of it and provisions of the DLG to be analysed comprehensively for the purposes of framing for consent for data collection and storage wherein preference should be given to the provisions of DLG.

3.2.2. Privacy Policy for Handling of Personal Information[5]

- The DLA or any person who on behalf of DLA collects, receives, possesses, stores, deals, or handles information of provider of information, shall provide a privacy policy for handling of or dealing in personal information including sensitive personal data or information and ensure that the same are available for view by such providers of information who has provided such information under lawful contract.
- Such policy shall be published on the website and the relevant application of the DLA or any person on its behalf and shall provide for— (i) clear and easily accessible statements of its practices and policies; (ii) type of personal or sensitive personal data or information collected

  (iii) purpose of collection and usage of such information; (iv) disclosure of information including sensitive personal data or information (v) reasonable security practices and procedures.

3.2.3. Access to Data[6]

- Details of third parties engaged by DLAs shall be disclosed in the privacy policy (wherever applicable) and be updated from time-to-time in the policy itself in case of any change, where such third parties are allowed to collect personal information of the user through the DLA. The DLAs should have in place a code of conduct/ guiding principles to appoint such third parties as well.
- All the laws applicable on the DLAs related to data should also be followed by the third parties engaged by them with respect to privacy, customer data maintenance, etc.
- Where various allied services are offered together via the same platform/ application, the platforms/ applications have access to data, that otherwise they would not have, which is critical for smooth offering of their services and better customer experience. For these super apps, relaxed norms/ rules on data accessibility should be placed and exceptions should be carved out for data accessibility. In such cases, the applications/ platforms should have separate privacy policies/ terms service wise – for example, it should be exhaustive in nature for lending and stringent or lenient for others depending on the nature of criticality from one service to another – which can be easily accessed by users on their website.
- Proper standards for cyber security, privacy, and fraud must be laid out and adhered to by the company. Any privacy lapses which have been observed across DLAs must be addressed diligently. An exhaustive list of such lapses however may be decided and put in the rules by the lawmakers post analysis and consultation with the industry stakeholders and experts in the domain.
- Adequate transparency about what information is collected, why it is collected, and how it will be used to be duly provided to the consumers.
- Except as required under applicable law, an option should be given to users for updating, managing, exporting, and deleting their own data after their loan has been paid. The option for such deletion should be displayed on the application/ website at a prominent position.
- Proper disclosure of partner banks or NBFCs to the consumers must be made.
- DLAs/ recovery agents should be prohibited from using borrowers' phone contacts, photos, or

5 Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules (SPDI Rules), 2011.
6 Digital Lending Guidelines (DLG), 2022.

any other sensitive data to harass borrowers and their friends or family. Stringent penal measures must be identified in case of abuse by recovery agents. However, for ease of loan recovery by the recovery agents of the DLAs in case of any expected or potential default by the customer, the customers' reference contacts *(number of reference contacts may be decided in the industry consultations)* must be given by the borrower/ customer to DLAs and their agents at the time of issuance of loan, which shall not be misused in any case. Only the customers and their nominated references are to be approached by the DLA/ their recovery agents, if required.

- The details of recovery agents should be disclosed to the borrower beforehand, at the stage of issuance of loan, and also at the stage of passing the recovery responsibilities to such recovery agents. Additionally, this shall be updated to the customers from time to time in case of a change of such agents to avoid any unauthorised collection. The frequency and occasions at which this information needs to be shared may be decided by the lawmakers post analysis and consultation with the stakeholders in the domain.
- The DLAs shall not store personal banking data (such as Bank Account Number, IFSC Code, etc.) and if such data was stored previously, it shall be purged. However, DLAs can store limited data – last four digits of actual bank account number and bank's name, etc. – for transaction tracking and / or reconciliation purposes. Wherever such data is stored it is to be endured by the DLA that such data is tokenised for the security purposes.

3.2.4. Reasonable Security Standards[7,8,9,10,11]

- The DLA or a person on its behalf shall be considered to have complied with reasonable security practices and procedures, if they have implemented such security practices and standards and have a comprehensive documented information security programme and information security policies that contain managerial, technical, operational, and physical security control measures that are commensurate with the information assets being protected by the nature of business.
- In the event of an information security breach, the DLA or a person on its behalf shall be required to demonstrate, as and when called upon to do so by the agency mandated under the law, that they have implemented security control measures as per their documented information security programme and information security policies. The international standard IS/ISO/IEC 27001 on "Information Technology - Security Techniques - Information Security Management System - Requirements" is one such standard.
- The DLAs who have implemented either IS/ISO/IEC 27001 standard or the codes of best practices for data protection as approved and notified shall be deemed to have complied with reasonable security practices and procedures provided that such standard or the codes of best practices have been certified or audited on a regular basis by entities through independent auditors, duly approved by the Central Government.
- The audit of reasonable security practices and procedures shall be carried out by an auditor at least once a year or as and when the DLAs undertake significant upgradation of its processes and computer resources.
- The DLA should have a certification from a CISA certified auditor that it has a robust and secure IT system in place for preserving and protecting the data relating to the credit information.
- CERT-In Directions should be extended to DLAs as they mandate service providers, intermediaries, data centres and body corporates (Applicable Entities) to mandatorily report cyber incidents (as defined under the Information Technology *(The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 (CERT-In Rules)* within: (a) six hours of noticing such incidents; or (b) such incident being brought to the notice of such Applicable Entities. In addition to the Applicable Entities being mandated to report cyber incidents, within the prescribed time and in the prescribed manner,

7 Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules (SPDI Rules), 2011.
8 Eligibility for Specified User under Clause 3(j) of Credit Information Companies Regulations (Amendment) Regulations, 2021.
9 CERT-In Directions, 2022.
10 Frequently Asked Questions (FAQs) issued by CERT-In, 2022.
11 RBI's Guidelines on Regulation of Payment Aggregators and Payment Gateways, 2020.

they are also required to report cyber security incidents (*prescribed under CERT-In Directions), on meeting the following threshold (as laid out in the FAQs):* (i) cyber incidents and cyber security incidents of severe nature *(such as denial of service, distributed denial of service, intrusion, spread of computer contaminant including ransomware)* on any part of the public information infrastructure, including backbone network infrastructure; (ii) data breaches or data leaks; (iii) large-scale or most frequent incidents such as intrusion into computer resources, websites etc.; and (iv) cyber incidents impacting the safety of human beings.

- Guidelines should be introduced by the regulator/ relevant authority which set baseline-technology standards for DLAs to adopt. Such guidelines may include the following but is not limited to the same:

  Information security governance, data security standards, security incident reporting, merchant onboarding, cyber security audit and reports, information security, IT governance, enterprise data dictionary, risk assessment access to application, competency of staff, vendor risk management, maturity and roadmap, cryptographic requirement, forensic- readiness, data sovereignty, data security in outsourcing, and payment application security, and any other aspect as is deemed necessary by the relevant regulatory authority.

3.2.5. Data Localisation[12,13,14]

- DLAs must ensure that all data is stored only in servers located within India, unless an exemption is carved out under extant statutory guidelines.
- DLAs must ensure that the entire data relating to digital lending systems operated by them are stored in a system only in India. This data should include the full end-to-end transaction details and information pertaining to lending or settlement transaction that is gathered / transmitted / processed as part of a message / instruction. This may, interalia, include - Customer data (Name, Mobile Number, email, Aadhaar Number, PAN number, etc. as applicable); lending sensitive data (customer and beneficiary account details); payment credentials, if any involved (OTP, PIN, passwords, etc.); and, transaction data (originating & destination system information, transaction reference, timestamp, amount, etc.) and other data points of the borrower as may deemed appropriate by the regulatory authority.
- System providers must submit the System Audit Report (SAR) on completion of the requirement above. The audit should be conducted by CERT-In empaneled auditors certifying completion of activity. The SAR duly approved by the Board of the DLAs should be submitted to the RBI before such date as may be decided by the lawmakers post analysis and consultation with the stakeholders in the domain.

12 Digital Lending Guidelines (DLG), 2022.
13 RBI's Regulation on Storage of Payment System Data, 2018.
14 Draft Digital Personal Data Protection (DPDP) Bill, 2022.

3.3. Customer Protection and Grievance Redressal Requirements

(Considering that actions required for availing digital lending services take place on tech-enabled platforms over which consumers have little control, it is important to acknowledge and imbibe into practice measures which prioritise customer protection. Not just that, a transparent grievance redressal mechanism is also needed to resolve complaints of consumers.)

3.3.1. Grievance Redressal[15]

- The DLAs should appoint a Grievance Redressal Officer and their contact details should be prominently displayed on the websites of the DLAs and in the Key Fact Statement (KFS) provided to the borrower.
- The Grievance Redressal Officer shall deal with complaints against their respective DLAs.
- The facility of lodging complaints shall also be made available on the DLA's website and applications.
- With industry consultation, a timeframe should be decided within which the complaint has to be resolved by the Grievance Redressal Officer expeditiously. Suggested timeframe is 1 month from the date of receipt of grievance.
- The Grievance Redressal Officer shall report details of the complaints filed and complaints resolved to the executive body/ regulator concerned, as decided by the government.
- A mechanism shall be developed for consumers to appeal to ombudsman and then further escalation in case of non-resolution in a given time frame by each authority.

3.3.2. Key Fact Statement[16]

- DLAs shall provide a KFS to the borrower before the execution of the contract in a standardised format for all digital lending products. The format of KFS is provided in Annex-II of DLG.
- The KFS shall, apart from other necessary information, contain the details of Annual Percentage Rate, the recovery mechanism, details of Grievance Redressal Officer designated specifically to deal with digital lending/ FinTech related matter and the cooling-off/ look-up period.

3.3.3. KYC Guidelines[17]

- There shall be an internal Know Your Customer (KYC) policy. The KYC policy shall include the following four key elements: Customer Acceptance Policy; Risk Management; Customer Identification Procedures; and Monitoring of Transactions. The DLA should report to the partner regulated entity of any suspicious/ fraudulent transaction etc. for the RE to take necessary actions/ steps in this regard.
- DLAs to facilitate and provide full support to REs in their risk assessment exercise periodically to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk for clients, countries or geographic areas, products, services, transactions, or delivery channels etc.
- DLAs to help, to the extent possible, REs in documentation of the risk assessment reports to confirm its proportionality to the nature, size, geographical presence, complexity of activities/ structure, etc.
- DLAs to facilitate Lenders/ REs as and when required in the best possible manner in the Digital KYC Process as laid down under Annex I of the Master Direction – KYC Direction, 2016.

15 Digital Lending Guidelines (DLG), 2022.
16 Digital Lending Guidelines (DLG), 2022.
17 Master Direction - Know Your Customer (KYC) Direction, 2016.

3.4. Other Requirements

(Some additional caveats need to be established by the regulators and the government to ensure overall safety of markets, economy as well as consumers.)

3.4.1. Reporting Requirements

- The DLAs should file all the required monthly, quarterly, bi-annually or annual returns and information as, when, how and to whom directed by the RBI. The body in the form of SRO or nodal agency in the digital lending space as created by the RBI may seek such information in the format and timelines as deemed appropriate by it, including but not limited to necessary information about company registration, link of website, tax registration, kind of products/ services offered, associated NBFCs and banks, privacy policy, certifications for cyber security standards, audit reports, financials, details of Grievance Redressal Officer, investor related information *(eg. Country/ origin from which the investors have invested funds into the DLA)* to enable effective regulation and supervision of DLAs. Further, in the event of any material change in the information provided, the DLA must intimate such body/ RBI as and how directed.
- Any investor/ investment of DLAs from the sanction list of DLA or the associated REs, or the investor/ investment from China or other such countries which are notified from time to time by the government, or from such other entities which are identified by the regulator, must be immediately disclosed to the regulator in the manner prescribed by the regulator.

3.4.2. Compliance with Credit Information Companies Regulations[18,19]

- Any lending done should be reported to Credit Information Companies (CICs) irrespective of its nature/ tenor.
- As per Section 17 of the CIC Act, only Specified Users were authorised to access the credit information of the customer, and any sharing of credit information with entities other than Specified Users was considered unauthorised sharing. The RBI has brought FinTech companies within the ambit of Specified Users, who are involved in the processing of information, for the support or benefit of credit institutions, provided these companies comply with the eligibility criteria (issued vide press release dated 05.01.2022). Thus, DLAs should obtain membership of CICs as a Specified User.

3.4.3. Refrain From Misleading Advertisements[20]

- The DLAs must adopt due diligence measures provided in Guidelines for Prevention of Misleading Advertisements and Endorsements for Misleading Advertisements, 2022 to reflect that the advertisement is genuine and not deceptive. Among other things specified therein, the DLAs must not be involved in publishing or advertising content which is misleading and have false pretense, publishing or advertising bait and hook advertising, and publishing or advertising free claims which are not in compliance with the Guidelines.

3.4.4. Risk Management[21]

- The DLAs shall adopt a board-approved Disaster Management and Business Continuity Plan to enhance preparedness in case of adverse/ extreme events affecting business.
- DLAs shall put in place adequate information and data security infrastructure and systems for prevention and detection of frauds.
- The requirement of obtaining Legal Entity Identifier (LEI) may be extended to the digital lending apps as well as the entities obtaining loan of more than a certain ticket size as decided by the regulator. The framework may help keep track, and bring ease and convenience in the transactions.

18 Digital Lending Guidelines (DLG), 2022.
19 Eligibility for Specified User under Clause 3(j) of Credit Information Companies Regulations (Amendment) Regulations, 2021.
20 Guidelines for Prevention of Misleading Advertisements and Endorsements for Misleading Advertisements, 2022.
21 RBI's Guidelines on Regulation of Payment Aggregators and Payment Gateways, 2020.

4. Global Overview

Policymakers can also refer to global best practices to develop a positive regulatory model. In the UK, no single regulatory framework governs FinTech, but their regulated activities fall within the respective regulator's ambit. In the US, FinTech offerings are subject to product-level regulation by the federal government and individual states. They regulate the digital lending sector by responding to various product innovations to maintain competitiveness.

The table below presents an overview of global regulatory approaches undertaken for digital lending in the case of FinTech Platform Financing i.e., financing done through electronic platforms which are not operated by commercial banks:

	Japan	USA	Germany	Brazil	China	Indonesia
License/ Approval/ Registration	Any non-bank lender must register itself as a money lending business operator	Unless they partner with a chartered bank, they are often required to obtain a license in every state in which they lend. Nationwide lenders to obtain numerous state licenses	Need banking license	Any entity engaged in FBS lending to be licensed as a Direct Credit Company by the Central Bank of Brazil	As per Draft Rules, licenses for eligible lenders to be renewed every 3 years	Licensing and registration to be obtained from the Financial Services Authority
Framework/ Regulation	No regulations/ framework introduced	Non-bank lenders are required to comply with applicable state laws regulating money lending. Nationwide lenders are subject to 50 state regulatory frameworks	No regulations/ framework introduced	Regulations have been prescribed for direct credit companies called Sociedades de Crédito Direto	Draft Rules on Online MicroLoans issued by People's Bank of China (PBOC) and CBIRC in 2020 Also, Online Lending Rules of 2016 issued by CBIRC to target activities of peer-to-peer lending	Regulations on IT-Based Borrowing-Lending Services of 2016

Until now, India had followed a 'light-touch' approach to FinTech regulation, however now it is increasingly moving towards a full-regulation model. While this holds true for other verticals, such as payments, the recent developments in digital lending also indicate that the country will follow the same trajectory. Another approach which India undertakes is that of creating new regulatory frameworks for specific digital or FinTech activities which suit the Indian ecosystem.

5. Way Forward

India's digital lending sector is on the cusp of a revolution. With that, the need to regulate the ecosystem is imperative to ensure social as well as economic security. The WGDL in its report suggested whitelisting of DLAs and thus, such whitelisting exercise is critical as it will weed out DLAs with illegal practices from the market. Understanding the urgency of the situation, this report has attempted to list key features and requirements in DLAs which can serve as the Whitelisting Framework. This report seeks to supplement the efforts of the concerned government bodies – like RBI, MeitY, MCA and others – as they are already engaged in a similar exercise, in monitoring and supervision of the digital lending ecosystem.

This Whitelisting Framework may additionally serve as a Standardised Code of Conduct for DLAs that will lay out model industry practices for the sector and add legitimacy to the businesses.

Under the whitelisting framework, the government may also consider formation of SRO which has been suggested by the WGDL and the WG on FinTech and Digital Banking. An SRO will be identified by the RBI and be responsible for promoting good industry practices viz. genuine and authentic technological tools, cyber-safe software, and mechanisms. In addition to this and as also suggested in the WGDL report as well, the government may also explore dedicating an independent nodal agency, within the purview of the RBI in consultation with relevant stakeholders. A nodal agency may hinder innovation whereas an SRO may comprise mostly practitioners and encourage innovation with guard rails reducing regulatory burden off the shoulders of the government. Similarly, an SRO may not have the ability to enforce its suggestions unless granted the specific powers by law while nodal agency may be backed by such authorities. Alternatively, the government may implement both and after holding discussions with relevant stakeholders, assign the various responsibilities between the SRO and the nodal agency within the purview of the RBI.

To further strengthen the credit lending systems in India, the idea propounded by the former Deputy Governor of RBI, Viral Acharya with respect to the Public Credit Registry (PCR) may also be adopted. PCR is a proposed centralised database of credit information which would collect, store, and disseminate credit data of all the borrowers in the country. The database would include information such as credit history, outstanding loans, collateral, and other relevant data of borrowers. The benefits of a PCR include improving the credit culture in the country, facilitating better credit decision-making, reducing credit risk, and promoting financial stability. It would also reduce the cost of credit for borrowers by providing lenders with accurate and reliable information on borrowers' creditworthiness. In 2018, the RBI constituted a high-level task force on the development of a PCR for India. The task force submitted its report in 2019, which recommended the establishment of a PCR in India.

Over and above these recommendations, since the DLAs may be heavily regulated by the concerned authorities and adequate reporting requirements are to be put in place, the RBI may consider expanding the role of DLAs from being merely facilitators to being lenders, given they have the capacity to lend, and provided they follow basic principles/ regulatory requirements as applicable on the lending entities.

We believe, the collective efforts will help in the protection of digital borrowers from unchecked loan-sharking practices prevailing in the market. This will result in a synchronised digital lending ecosystem and boost confidence in this sector which has the potential to reach every nook and corner of the country, people from all walks of life and from diverse social strata.

As the government revs up the MSME growth engine to take India to its $7 trillion target, digital lending can provide the necessary oil, albeit within an ecosystem that supports businesses operating with good faith to maintain the country's financial stability. This report is an effort to supplement the government's vision of making India a leader in digital finance and revolutionise social welfare on the back of the digital economy.

With this report, we hereby request the government to consider our suggestions and recommendations to build the framework for mapping of legal players and for eliminating non-compliant players which may then be respectively enforced by the RBI, MeitY, MCA and other government bodies in their respective areas of engagement. With the uptake of the suggestions/ recommendations made in this report, both – customer protection as well as credible legitimacy can be enhanced.

References

1. *Report by RBI's Working Group on Digital Lending (WGDL), 2021.*
2. *Digital Lending Guidelines (DLG), 2022.*
3. *Draft Digital Personal Data Protection (DPDP) Bill, 2022.*
4. *Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules (SPDI Rules), 2011.*
5. *Eligibility for Specified User under Clause 3(j) of Credit Information Companies Regulations (Amendment) Regulations, 2021.*
6. *RBI's Regulation on Storage of Payment System Data, 2018.*
7. *Indian Computer Emergency Response Team (CERT-In) Directions (2022).*
8. *FAQs on Cyber Security Directions CERT-In of 28th April 2022.*
9. *Master Direction - Know Your Customer (KYC) Direction, 2016.*
10. *Guidelines for Prevention of Misleading Advertisements and Endorsements for Misleading Advertisements, 2022.*
11. *RBI's Guidelines on Fair Practices Code for Lenders, 2003.*
12. *RBI's Guidelines on Regulation of Payment Aggregators and Payment Gateways, 2020.*
13. *RBI's Notification on Legal Entity Identifier (LEI) for Borrowers, 2022.*
14. *FAQs on RBI's Regulation on Storage of Payment System Data, 2018.*
15. *FinTech Regulation in Asia Pacific (APAC), University of Cambridge, 2022.*

CHASE
INDIA

First Floor, 74, Link Road, Lajpat Nagar III,
New Delhi – 110024, India.

Founded in 2011, Chase India is a leading public policy research and advisory firm with growing practices in Technology & FinTech, Transport & Infrastructure, Healthcare & Life Sciences, Development and Sustainability. Chase provides consultancy services to organizations for mitigating business risks through insight-based policy advocacy. Over the years, Chase India has collaboratively worked with multiple stakeholders such as government, parliamentarians, civil society organizations, academia, and corporates on several policy issues of critical importance. Chase India is committed to using its knowledge, high ethical standards, and result-oriented approach to drive positive action for its partners. Chase India has pan India presence with offices in New Delhi, Mumbai, Pune, Hyderabad, Chennai, and Bengaluru and is a part of the WE Communications Group worldwide.

For more information, please visit www.chase-india.com

AUTHORS:

Aishwarya Sharma
Associate
Chase India
aishwaryas@chase-india.com

Srishti Vajpayee
Senior Manager
Chase India
srishtiv@chase-india.com

Kaushal Mahan
Vice President
Chase India
kaushal@chase-india.com