SECURITIES AND EXCHANGE COMMISSION OF PAKISTAN
Specialized Companies Division
Lending & Private Fund Department

No. SC/NBFC-1-196/Circular/2024/ 76 **May 15, 2024**

Circular No. 12 of 2024

Subject: Requirements for NBFCs engaged in Digital Lending

The Securities and Exchange Commission of Pakistan (the "Commission") in exercise of powers conferred under sub-section (3) of section 282B of the Companies Ordinance, 1984 (XLVII of 1984) read with regulation 28(da) of the NBFC Regulations, 2008, in supersession of its earlier Circular 15 of 2022 dated December 27, 2022, Circular 10 of 2023 dated August 7, 2023 and Circular 15 of 2023 dated September 25, 2023, is hereby pleased to issue this circular imposing the following requirements on Non-Banking Finance Companies (NBFCs) engaged in digital lending to ensure fair treatment, full disclosure and protection of personal information of the borrowers. The Circular encompasses the following aspects:

1. Disclosures through App interface, limits, conditions & mandatory requirements
2. Limits, conditions and disclosures applicable to each category
3. Pricing Policy, Credit Risk and Advertisements/Publications
4. Grievance Redressal Mechanism
5. Loan Collection
6. Requirements for Digital Lending Apps
7. Confidentiality
8. Mobile Application Security
9. Glossary of Terms

1. Disclosures through App interface, limits, conditions & mandatory requirements: -

(a) Any digital App user should be given the general information about the App, including any access to user data or information that the App may gather after installation during App registration process;

(b) Before entering into any agreement for financing, the Digital Lender shall give full disclosure to the prospective borrower on all the terms of the agreement, including but not limited to the following:

(i) **privacy policy** – the privacy policy shall be duly vetted by a law firm specialized in the field of Banking and Finance;

(ii) **mark-up rate-** rate of mark-up that will be charged on the loan whether it is on fixed, variable or combination of fixed and variable rates;

(iii) **financing details-** amount and term of loan along with number of installments and the amount to be paid for each installment;

(iv) **Early Settlement** - Early Settlement may be allowed;

(v) **fees and charges-** applicable fees and charges by whichever name called, and their nature, including implied charges/penalties; and

(vi) **contact details-** details of grievance redressal system;

(c) Before proceeding for loan disbursement, a Digital Lender shall display a summary of key fact statement to the borrower through a video/audio, screen shot and email/SMS in English and Urdu languages. The key fact statement shall be presented in a simple, clear and easily accessible format and shall include the minimum information specific to each category as applicable as provided in **Annexure – A**;

(d) Any fees, charges, etc., which are not mentioned in the key fact statement (Annexure - A) cannot be charged to the borrower at any stage during the term of the loan;

(e) A Digital Lender shall also provide comprehensive disclosures to the borrowers on collection of data, its safe storage, sharing and usage and in this regard shall also obtain explicit consent of the borrower. Furthermore, a digital lender shall not acquire any information that is personal in nature and is not directly related to the credit score calculations;

(f) Any fee, charges etc. payable with respect to the credit intermediation process shall be paid directly by Digital Lender and not by the borrower;

(g) No upfront deductions (first instalment, charges, fee etc.) shall be made from the loan disbursement amount and the loan amount disbursed shall be equal to the loan amount approved;

(h) In case of Buy Now Pay Later (BNPL) or product financing arrangements, financing amount may be recovered as a down payment or first installment, through Cash on Delivery (COD), debit and credit card transactions, or designated bank account transfers. Furthermore, if a loan application is rejected

ML.

or if the product delivery fails, the amount received shall be refunded to the borrower within a period not exceeding two working days;

(i) The loan disbursement shall be subject to acceptance of all the underlying terms and conditions by the borrowers. The Digital Lender shall provide a choice to the borrower to accept or decline the offer through conspicuously provided click on the button options;

(j) Digital Lender shall ensure that digitally signed documents i.e. summary of loan product, sanction letter, terms and conditions and account statements with respect to financing details, etc. shall automatically flow to the borrowers on their registered and verified email/ SMS upon execution of the loan contract/ transactions;

(k) The terms and conditions along with Annual Percentage Rate (APR) as agreed between Digital Lender and borrower at time of grant of loan shall not be subsequently changed;

(l) A Digital Lender shall allow the Cooling Off period on every loan and clearly communicate and explain it to the borrowers. The Digital Lenders shall however, be eligible to collect National Database and Registration Authority Verisys cost, fund transfer cost (if incurred) and CIB costs from such borrowers who avail the cooling off facility:

Provided that incase of BNPL/Product financing the cooling off period will be applicable until the product is shipped to the borrower and cooling off period will not be required in case of other licensed categories, as applicable;

(m) A Digital Lender shall give borrower a digital receipt for every repayment made on account of any loan at the time of such repayment; and

(n) All transactions including disbursement and recovery shall be carried out only through the bank accounts/branchless banking accounts of the digital lender and disbursement shall be ensured to be made in the bank account/branchless banking account of the borrower (IBAN/E-Wallet Mobile Account Number after title verification through 1-link title fetch service or IBAN/E-Wallet mobile account number and CNIC Pairing).

2. Limits, conditions and specific disclosures applicable to each category:

(a) Digital Nano Lending: -

(i) A NBFC can extend a maximum amount of Rs 50,000/- as nano lending to a borrower, with a tenor of up to 90 days;

(ii) Compounding of markup shall not be allowed (no markup shall accrue either on original markup or on late payment charges);

(iii) Aggregate amount of nano-lending extended to a borrower by all NBFCs shall not exceed Rs. 100,000 at any point in time;

(iv) An NBFC can rollover/restructure a loan in such a way that period of the loan including the original and rollover tenor shall not exceed 90 Days;

(v) An NBFC shall consider rollover/restructuring as extension of existing loan and shall not treat it as new loan;

(vi) An NBFC shall apply the same APR and terms to loan rollover/restructuring as applied to the existing loan;

(vii) Digital Lender shall not charge Profit Rate (PR) exceeding 0.75% per day, with an APR not to exceed 274%;

(viii) An NBFC shall not recover from a borrower, on account of all costs of the loan including the nominal interest/markup/profit rate and all other applicable fees (i.e processing fees, services fees, notarial fees, handling fees and verification fees, among others) as well as penalties for late payment and non-payment, an aggregate amount exceeding the principal of the loan;

(ix) A Digital Lender, for accurate computation of PR and APR shall ensure that, -

(I) Entire principal amount of the loan shall be disbursed by the lender on the issue date of the loan and shall be payable by the borrower either in lump sum on maturity date of the loan, or in equal intervals during the loan period, or on the extended maturity date in case of rollover of a loan; and

(II) Entire profit amount shall be payable by the borrower either in lump sum on maturity date of the loan, or in equal intervals during the loan period;

ML

(x) A prompt/alert in English and Urdu shall appear with the following minimum contents should appear, whenever a user opens the nano-lending App and/or website,

قرض لیتے وقت ہمیشہ ذمہ داری کا مظاہرہ کریں اور صرف اتنا ہی قرض
حاصل کریں جو آپ ، کسی مالی مشکل کا شکار ہوئے بغیر، آسانی کے ساتھ
مقررہ مدت کے اندر اندر ادا کر سکتے ہیں۔ قرض لینے سے پہلے ہمیشہ دئے گئے
شرائط و ضوابط کو غور سے پڑھیں اور سمجھیں۔

"Digital Nano loans are short-term loans with high-interest rates and additional charges. It is essential to that you understand potential risk of over-indebtedness. Borrow responsibly and only take loans that you can comfortably repay within the agreed timeframe to avoid financial difficulties. Always read the terms and conditions carefully before availing any loan. Your financial well-being is our priority.".

(xi) A calculator shall be provided on the App/website homepage where a user can evaluate impact of costs including processing fee, platform fee, PR, late payment charges and all other applicable charges for different borrowing options; and

(xii) Any change/ updates in the whitelisted App shall be made only with prior intimation to the Commission. Intimation will be considered acknowledged if no observation/query has been shared by the Commission within 5 working days.

(b) **Earned Wage Access: -**

Digital Lender acting as Employer-Integrated Earned Wage Access Provider shall not;

(i) Share fees received from a person with the person's employer;

(ii) Use a person's credit report or credit score to determine the person's eligibility for the EWA services;

(iii) Charge any late fee or other penalty for a person's failure to pay;

(iv) Report a person's failure to pay to a credit bureau; and

(v) Compel the person to pay through civil action, a debt collector, or selling or assigning outstanding amounts to a debt collector or debt buyer.

(c) **Embedded Lending: -**

(i) NBFCs are permitted to extend their lending services by integrating Application Programming Interface (API) with digital lending apps/platforms/tools that have been duly whitelisted by the Commission; and

(ii) NBFCs can extend their lending services through API integration with other digital platforms as per requirements specified by the Commission.

3. Pricing Policy, Credit Risk and Advertisements /Publications: -

(a) A Digital Lender shall develop and implement appropriate pricing policies approved by its board of directors that ensure access to affordable financial services along with operational and financial sustainability of the NBFC;

(b) In order to prevent borrower's over-indebtedness and manage credit risk, the Digital Lenders shall develop an internal mechanism to monitor the overall exposure of its borrowers by,-

(i) requiring additional information /undertaking from borrowers regarding their current borrowing from all lenders;

(ii) obtaining membership of Credit Information Bureaus licensed by State Bank of Pakistan (CIBs) and obtain a credit report and use CIB data as part of the loan decision process for every loan application including renewal & rollovers except in the case of Earned Wage Access; and

(iii) ensure regular/continuous reporting to all the credit bureaus operating in Pakistan on real time basis.

(c) A Digital Lender shall make available on its website and App, updated information regarding its lending products including complete terms and conditions. Any advertisement and publication, whether in textual, digital, audio or visual form, in relation to the digital lending business of a Digital Lender, directly or through any other person, shall, -

(i) be fair and reasonable and not contain misleading information;
(ii) not use official logo of the Commission or any other government agency;
(iii) contain full disclosure regarding loans on offer and applicable APR; and
(iv) contain the Digital Lender's full corporate name and licensing status (including license no.) on its App, documentation, advertisements materials, and
(v) ensure to include its App name, web address, telephone hotline for handling complaints and a risk warning statement, prominently and easily legible in the written or visual part of the advertisement.

4. **Grievance Redressal Mechanism.-** All the requirements of Commission's Circular No. 24 of 2018 dated December 27, 2018 relating to Guidelines on Grievance Redressal System in Non-Bank Microfinance Companies shall be applicable to Digital Lenders. In addition, digital lenders shall report to the commission on a monthly basis, the following information:

(i) No. of complaints outstanding from previous month;
(ii) Total no. of complaints during current month;
(iii) Nature of repetitive complaints;
(iv) No. of complaints resolved;
(v) No. of complaints outstanding;
(vi) Satisfaction ratio;
(vii) Average time taken for disposal of a complaint; and
(viii) Monthly trend analysis of complaints received and disposed.

5. **Loan Collection, -**

(a) In case, the digital lender outsources its loan collection function to third-party service providers (agents), it shall also maintain complete record of employees/personnel engaged in recovery of loans;

(b) A Digital Lender, its employees or agents while refraining from unscrupulous and untoward acts; shall only resort to reasonable and legally permissible means for collection of amounts due from the borrowers under the loan agreements;

(c) Without limiting the general application of the foregoing requirement, a Digital Lender, shall not, engage in any of the following unfair collection practices. -

(i) contacting at unreasonable or inconvenient times i.e. before 7 a.m. or after 10:00 p.m.;
(ii) notwithstanding the borrower's consent, accessing the borrower's SMS or call log or phone book or contacts list or photo gallery and contacting the persons in the borrower's contact list, other than those who have been specifically authorized by the borrower as guarantors and who have also provided their consent to the digital lender at the time of loan approval:
Provided that Digital Lender engaged in licensing activity other than nano-lending may access phone gallery to the extent of obtaining requisite document relevant to its business model as applicable;
(iii) post, share or publicize a borrower's personal or sensitive information online or on any other forum or medium, or threatening to do so, except to the extent of reporting to credit bureaus or other legal forums, as per authorization from the borrowers;
(iv) use of or threat to use violence or other illegal means to harm the person, or his reputation or property;
(v) use of obscene or profane language for the borrower or the borrower's references or contacts;
(vi) improper or immoral debt collection tactics, methods or an act that is illegal; and
(vii) any other conduct whose consequence is to harass, oppress, or abuse any person in connection with the collection of a debt, -

(d) All calls and messages for loan collection should be made via company's designated phone numbers (to be made public through website & App) and all calls should be recorded. The call recordings and log of messages should be maintained for a period of at least one year; and

(e) Digital lenders shall handle defaulters as per the law of Pakistan.

6. **Requirements for Digital Lending Apps:-**

(a) Prior to launch of an App or any other digital channel for lending, the Digital Lender shall submit an application to the Commission for listing on SECP App Whitelist along with self-assessment declaration of compliance with regulatory framework;

(b) A Digital Lender at the time of launching the App shall provide license status along with acknowledgement of whitelisting from the Commission of the App to Google Play Store and/or App Store. Proof for the same shall subsequently be provided to the Commission and maintained by Digital Lender as record. Only whitelisted App shall be listed on Google Play Store/App Store (Apple Inc.) and URL of that App shall be displayed on the App Whitelist to be maintained and published by the Commission on its Official website.

(c) A digital lender shall operate only one App at a particular time;

(d) In order to address the prospective risk of identity theft; the App shall require provision of a live selfie for photo verification or In-App biometric verification as part of their Know Your Customer (KYC) process;

(e) The Commission may delist a digital lending App from App Whitelist if digital lender fails to comply with applicable regulatory requirements. Furthermore, digital lender shall not onboard new clients or disburse loans as a result of-delisting of the App with immediate effect. However, a digital lender shall be allowed to recover its outstanding loan through its app; and

(f) Digital Lenders shall submit monthly report to the Commission gender disaggregated loan portfolio data as specified in the Annexure-B of the Circular by the 10th of every month.

7. **Confidentiality. -** Data collected by Digital Lenders through mobile Apps or any other means is subject to privacy of the borrower and shall be used only for loan processing or transactions related to the loan. A Digital Lender shall keep the data of the borrower strictly confidential, except in the following circumstances, -

(a) Disclosure of information with the specific written or recorded consent of the borrower;

(b) Release, submission or exchange of borrower information with other financial institutions, credit information bureaus and duly licensed lenders;

(c) Disclosure of information upon orders of a court of competent jurisdiction or any government office or agency authorized by law;

(d) Disclosure to collection agencies, counsels and other agents of the Digital Lenders to enforce the latter's rights against the borrower;

(e) Disclosure to third party service providers solely for the purpose of assisting or rendering services to the Digital Lenders in the administration of its lending business; and

(f) Disclosure to third parties such as insurance companies, solely for the purpose of insuring the Digital Lenders from borrower default or other credit loss, and the borrower from fraud or unauthorized charges.

8. **Requirements for Mobile Application Security of Digital Lending App: -**

(a) Digital lender shall ensure that adequate cybersecurity measures and controls are in place to ensure confidentiality, integrity and availability of the data and information. The controls shall include but not limited to:

(i) **Secure Access Management: -**

(I) Approved policies and procedures for secure access management should exist;

(II) User account of employees who leave the organization should be disabled;

(III) Ensure no privileged (admin) user IDs are in use without formal approval;

(IV) Maintain inventory of privileged accounts and review frequency should be defined.

(V) Ensure that access rights review document for application is in place.;

(VI) Appropriate user creation, modification of rights, revocation of rights should be performed and approvals from line manager should be in place; and

(VII) Validate that strong password policy is implemented which covers password complexity, minimum length, history and minimum age;

ML.

(ii) Perimeter and Network Security: -

(I) Maintain high level network diagram of mobile application environment indicating the location of network devices, app and database servers and other components attached;

(II) Implement security measures to protect against unauthorized access or attacks;

(III) Validate that inbound security policies are enabled for in scope application environment;

(IV) Verify from firewall that only trusted users are allowed to access the applications;

(V) Logging and monitoring process on firewall put in place; and

(VI) Validate the details of Encryption mechanism, TLS version, digital certificate on application portal;

(iii) Endpoint, Server and Cloud Security: -

(I) Verify that versions and patches of all endpoints are updated and secured;

(II) Ensure that software installation and upgradation rights on servers/instance is only limited to the Authorized person; and

(III) Ensure that software installation on endpoints should be restricted and approved on a need-to-use basis;

(iv) Application Level Security: -

(I) Make sure all the components required for the application such as web server and other components are updated and running on latest versions;

(II) Implementation of Web Application Firewall (WAF) on customer facing interfaces should be ensured;

(III) Maintain details of the latest VAPT conducted on mobile application portal/mobile app, system, and database;

(IV) Conduct VAPT on the in-scope system, including the mobile application portal/mobile app, system, and database; and

(V) Ensure that API are not using outdated SSL/TLS protocols.

(v) Data Security: -

(I) Approved data security policy and procedure should be in place;

(II) Ensure that the relevant documentation is maintained and reviewed;

(III) Encrypt data at rest (including backups) and in transit using strong and non-obsolete cryptographic algorithms;

(IV) Ensure appropriate measure have been taken to avoid accidental deletion or overwrite of data/information; and

(V) Ensure that the separate channels are being used for storage and transmission of critical data.

(vi) Incident surveillance and monitoring: -

(I) Ensure the policies and procedures are in place for Incident Management and Reporting;

(II) Ensure that the anomalies are detected and resolved in a timely manner;

(III) Ensure that incident management procedure is implemented and appropriate reporting matrix is maintained for such incidents;

(IV) Incident response functions shall be implemented in application system, responses to any incident should be documented for record; and

(V) Ensure that the potential risks and vulnerabilities are identified in a timely manner, which could impact business continuity. Moreover, ensure reviewal and updating of the risk assessment.

(vii) Patch management: -

(I) Validate that log of patches deployed are documented;

(II) Validate that formal process of approval is in place for patch testing, User acceptance testing and migration to production;

(III) Approved patch management policies and procedures should be in place;

(IV) Procedure for approval of tested patches should be defined. UATs of the patches should be in segregated environment; and

(V) Validate that patches are applied on test system first before provisioning to live.

ML

(viii) Logging and backups: -

(I) Validate that policies and procedures are approved and implemented for Backup and recovery of in-scope application;

(II) Validate that logging is enabled at application, platform, database and operating system levels;

(III) Validate that log file can't be modified, even system administrator not have access to modify own logs and logs must be secured at directory levels; and

(IV) Frequency of backups should be defined in the system for both production and development and the same shall be documented in relevant policy.

(b) Digital Lenders shall develop a policy governing mobile Apps' business objectives, standards, compliance, guidelines, controls, responsibilities and liabilities. As a principle, the policy shall achieve a balance between the security of Apps, convenience and performance. The policy shall at least be revisited annually and/or when a significant change is made in the environment;

(c) Digital Lenders may develop mobile Apps in-house, through outsourcing or by a combined approach. To manage mobile App development projects, Digital Lenders shall:-

(i) Put in place necessary App documentation including manuals on development, testing, training, production, operational administration, user guides and Service Level Agreements (SLAs);

(ii) Carry out vulnerability assessment, penetration testing and performance assessment of mobile Apps to ensure effective and smooth operation, before deploying the same in production environment;

(iii) Carry out system and User Acceptance Testing (UAT) in an environment separate from the production environment; and

(iv) Put in place an escrow arrangement in cases where third party vendors develop mobile Apps but the source codes are not released to the Digital Lender;

(d) Data shall not be stored on any cloud infrastructure outside the jurisdiction of Pakistan;

(e) Digital Lenders shall ensure compliance with the requirements relating to the mobile App, as provided in **Annexure-C** to this Circular;

(f) Digital Lender from the date of whitelisting of the app shall carry out the following and submit the reports to Commission within one month;

(i) self-assessment on semi-annual basis in the format specified by the Commission;

(ii) third party vulnerability assessment, penetration testing and performance assessment of mobile Apps on annual basis from the date of whitelisting.

(g) Digital lenders shall arrange at least once every three years from the date of whitelisting, IT audits of its IT infrastructure including the App by an independent audit service provider having qualified CISA / Certified ISO27001:2013 Lead Auditor certification to check compliance with regulatory requirements and shall submit the report to the Commission within the three months.

(h)The Digital Lender shall ensure compliance of all applicable laws in force in Pakistan related to cyber security, personal data protection, cloud usage and data privacy; and

(i) The Digital Lender shall solely be responsible for any digital fraud as a result of security lapse, operational issues, architecture of the App or any other malfunction of the App.

9. Glossary of Terms: -

(a) **"Digital Lender"** means lending NBFCs engaged in digital lending through digital, technology-based or internet-based channels, Apps or tools, being administered, managed or owned by them;

(b) **"Annual Percentage Rate" or "APR"** means effective annualized rate (%) (computed on net disbursed amount using IRR approach and reducing balance method) comprising all costs of the loan including the nominal interest/markup/profit rate and all other applicable fees (i.e. processing fees, service fees, notarial fees, handling fees and verification fees, among others), that represent a cost to the borrower by whichever name called. The APR does not include penalties for late payment and non-payment;

(c) **"CIB"** means Credit Information Bureaus; and

(d) **"Cooling off Period"** means a minimum period of 24 hours or such higher period as determined by Board of Directors, from the disbursement of loan during which the borrower

ML.

has the right to withdraw from the loan agreement and repay the principal amount to the digital lender without any markup/interest;

(e) **"B2C Financing"** means Business to Consumer Financing/Leasing for example digital nano lending, BNPL, EWA, education financing, product financing/leasing and advance against salary;

(f) **"B2B Financing"** means Business to Business Financing, referring to the provision of financial services or products directly to businesses for example working capital finance, stock/inventory financing, invoice factoring, COD financing and product financing/leasing;

(g) **"Digital Nano Lending"** means providing unsecured short-term cash loan up to Rs 50,000/- for a maximum tenor of 90 days through digital lending:

Provided that Digital Nano Lending does not include unsecured consumer, finance provided by Lending NBFCs for explicit purchase of any products/ goods or Earned Wage Access;

(h) **"BNPL"** means a buy now pay later arrangement, or a series of arrangements, through online or hybrid mode, -

(A) under which a person (the merchant) supplies goods or services to another person (the retail client);

(B) under which a third person (the BNPL provider) directly or indirectly pays the merchant an amount that is for the supply mentioned in paragraph (a); and

(C) that includes a contract between the BNPL provider and the retail client under which the BNPL provider provides credit to the retail client in connection with the supply mentioned in paragraph (a);

(i) **"Earned wage access"** means the payment of earned but unpaid salary/wage;

(j) **"Employer-integrated earned wage access provider"** means a Digital Lender who provides earned wage access services to a person in collaboration with the person's employer;

(k) **"Loan Period/Tenor"** The time period (in days) from issue date till maturity date of the loan;

(l) **"Principal"** The amount disbursed by the lender to the borrower at the beginning of the loan period;

(m) **"Profit for the Loan Period"** The amount including all costs, by whatever name called (markup, interest, profit, processing fee, service fee, handling fee etc.), payable by the borrower during the Loan Period;

(n) **"Loan rollover"** the renewal or extension of an existing loan, where the borrower is provided with new terms and conditions for repayment without fully repaying the original loan, and 'restructured loan' refers to a modification of the terms and conditions of an existing loan that results in a change to the repayment schedule, fees or other terms.

(o) **"Profit Rate for the Loan Period - %":** Expressed as percentage per annum and computed by simple annualization of the PR without considering the reinvestment or compounding of Profit over the next twelve (12) months;

$$\boldsymbol{APR(\%\,p.a.) = Profit\ Rate \times \frac{365}{Loan\ Period}}$$

Illustration

Principal	10,000	10,000
Issue Date	1 Oct 2023	1 Oct 2023
Maturity Date	15 Oct 2023	15 Oct 2023
Loan Period	14 days	14 days
Markup	500	900
Fees	300	600
Profit	500 + 300 = 800	900 + 600 = 1,500

ML.

Profit Rate - % per day	0.57%*	1.07%*
APR - % p.a.	0.57% x 365 = 208.6%	1.07% x 365= 390.5%
Ceiling for APR - % p.a.	274%	274%
Whether APR is within the APR Ceiling	Yes	No

This Circular shall come into force immediately and any non-compliance shall attract the penal provisions of section 282J of the Companies Ordinance, 1984 (XLVII of 1984).

(Mujtaba Ahmad Lodhi)
Commissioner (SCD)

<u>Distribution:</u>

1. Chief Executive Officers of All Non-Bank Finance Companies
2. Chief Executive Officer, Pakistan Microfinance Network
3. Chief Executive Officer, Pakistan Fintech Network
4. Chairman, NBFI & Modarabas Association of Pakistan

Annexure – A
(Clause 1(c) of the Circular)
(Minimum Information to be provided to the borrower)

Sr. No.	Parameter	Details
a.	Loan Amount Approved Rs.	
b.	Tenor of Loan	
c.	Maturity Date	
d.	No. of Instalments with due date	
e.	Annual Percentage Rate %	
f.	Processing Charges Rs.	
g.	Other Charges Rs.	
h.	Total Markup Rs.	
i.	Total Payable Amount	
j.	Cooling off period Cooling off period to withdraw from the loan agreement and repay the principal amount without any markup/interest except applicable Verisys (Rs.), CIB (Rs) costs and Fund Transfer Cost (if Applicable) (Transaction/IBFT Cost);	

Annexure -B

(Clause 6(g) of the Circular)

(Format of Gender Disaggregated Loan Portfolio Monthly Report submitted to the Commission)

Name of NBFC:
License Type:
Name of App:
Category:
Reporting Month

During the Month

No.of users registered/onboarded		**No. of Loan Disbursed**		**Total Amount Disbursed**		**Amount Recovered**		**Non-Performing Loans**	
Male	Female	Male	Female	Male	Female	Male	Female	Male	Female

Total as of till date;

No.of users registered/onboarded		**No. of Loan Disbursed**		**Total Amount Disbursed**		**Amount Recovered**		**Non-Performing Loans**	
Male	Female	Male	Female	Male	Female	Male	Female	Male	Female

Description	As end of Month,
Outstanding Loan Portfolio	
Active Borrowers	
Avg Outstanding Loan	
Avg Loan Disbursed	
% of Application rejection during the month	

No.of downloads	Registered Users	No.of users obtained loans	% of user retention

Annexure – C
(Clause 8(e) of the Circular)
(Mobile App Requirements)

A. Architecture of Apps

(i). Digital Lenders shall be responsible for development of a standard architecture based on set of security principles, rules, techniques, processes, and patterns to design a secure App;

(ii). The entire development of Apps shall revolve around the architecture principles, which can be updated based on the learnings during the course of development of application layers (or equivalent) and operational usage and consumer feedback;

(iii). Digital Lenders shall ensure that the Apps architecture is robust and scalable, commensurate with the application volumes and borrower growth. For this purpose, a robust capacity management plan shall be put in place to meet evolving demand.

B. Device Registration/Binding

(i). Digital Lenders shall implement a flexible device registration/binding functionality using only registered devices to access backend servers.

(ii). The device registration/binding shall preferably be implemented using a combination of hardware, software and service information. In case, multiple devices are registered by a user:

a) the user must be notified of every new device registration on the registered mobile number, email or phone call; and

b) Digital Lenders shall maintain record of all registered devices, providing the user a facility to disable a registered device.

C. Authorization and Authentication of the User

(i). Digital Lenders shall ensure that explicit customer consent in a convenient manner is obtained before allowing registration of Apps;

(ii). A login authentication shall be in place.

(iii). Digital Lenders shall ensure that the access to personal data is protected by strong customer authentication mechanism including:

a) Implementation of multi-factor authentication (MFA) for registration of Apps user-account;

b) Strong and configurable PIN/password/pattern or a biometric credential such as face recognition or fingerprint recognition;

c) Time-based one-time passwords (TOTP) for authentication;

d) OTP auto-fetching functionality; The validity of OTP shall not exceed more than 120 seconds.

e) Configure maximum number of failed attempts of authentication after which access to the App is blocked;

f) Maximum duration for termination of inactive mobile service sessions shall not exceed thirty minutes;

g) Ensuring that user authentication shall be processed only at the App owner's server-end; and

h) Ensure that authentication attempts are logged and monitored to detect login anomalies and possible breaches.

D. Protection of Sensitive Personal Data

(i). Digital Lenders shall ensure that sensitive information is not stored in a shared store segment with other Apps on mobile devices. It is recommended to utilize only the device internal storage, which is virtually sandboxed per App or preferably in a container App without meddling with other applications or security settings of the mobile devices;

(ii). Digital Lenders shall ensure that confidential data is deleted from caches and memory after it is used and/or uninstalled. Further, Digital Lenders shall ensure that Apps erase/expire all application-specific sensitive data stored in all temporary and permanent memories of the device during logoff or on unexpected termination of App instance.

(iii). Customer credentials and transactional data shall be encrypted while in-transit and at rest using strong, internationally accepted and published standards for key length, algorithms, cipher suites, digital certificates and applicable protocols that are not deprecated/ demonstrated to be insecure/ vulnerable;

(iv). Encryption keys shall only be stored with appropriate robust security controls and shall remain in a non-exportable form in a highly secure and standard key store. It may be bound to the secure hardware (e.g. Trusted Execution Environment, Secure Element for Android or its equivalent on any other platform). Further, Key Use Authorization shall be implemented, which should not be changed after generation of keys.

E. Network and Interfacing Security

(i). Digital Lenders shall ensure to enforce secure communication during the session establishment, exchange of data among Apps and backend services (including microservices);

(ii). Transport layer encryption shall be implemented for all communications between the Apps and App servers.

(iii). Digital Lenders shall setup their own Trust Manager to avoid accepting every unknown certificate. Apps shall use valid certificates issued by a trusted certificate authority;

(iv). Apps shall have inbuilt controls to mitigate bypassing of certificate pinning;

(v). Apps shall cease operations until certification errors are properly addressed;

(vi). Digital Lenders shall ensure that Apps must be able to identify new network connections and appropriate controls shall be implemented under such circumstances;

F. Session Management

(i). Digital Lenders shall ensure that Apps have automatic user-logoff functionality after a configurable idle time-period not exceeding thirty minutes;

(ii). Digital Lenders shall ensure that Apps have an easy to use and clearly visible logoff method;

(iii). Digital Lenders shall ensure that Apps erase/expire all application specific sensitive data stored in all temporary and permanent memories of the device during logoff or on termination of App instance;

(iv). Digital Lenders shall ensure that a procedure is in place to detect multiple simultaneous login attempts and immediately communicate it to the concerned user through alternate channels such as callback, SMS, email etc.

G. Tampering Detection

(i). Digital Lenders shall implement necessary checks on the server-side to verify Apps integrity and to detect any manipulation.

(ii). Digital Lenders shall ensure that installation of Apps is not allowed on rooted/jail broken devices;

(iii). Digital Lenders shall ensure that Apps are not allowed to run inside a debugger/emulator. For this purpose, Apps shall have debugger/emulator detections in place. Further, Digital Lenders shall not allow any third party to debug the application during runtime.

H. App Permissions

(i). Digital Lenders shall ensure to restrict data shared with other applications on the device through fine-grained permissions;

(ii). Digital Lenders shall ensure to minimize the number of permissions requested by the App and ensure that the permissions correlate to functionality required for the App to work. Apps shall defer or relinquish permissions when the same are no longer needed;

(iii). Unless for a specific business requirement in accordance with the security architecture principles, Digital Lenders shall not allow users to navigate to other Apps, sites or view objects that are not trusted and outside of App environment.

I. Secure Coding

(i). Digital Lenders shall ensure that their Apps developers adhere to industry accepted secure coding practices and standards;

(ii). Digital Lenders shall ensure that security libraries offered by mobile operating systems are correctly designed and implemented and that the cipher suites they support are sufficiently strong. Accordingly, Digital Lenders shall only use necessary and secure services, protocols, components, and dependent software and hardware, including those provided by third parties.

(iii). Digital Lenders shall document all required protocols, services, components, and dependent software and hardware that are necessary for any functionality of the application.

(iv). Digital Lenders shall have knowledge of all off-the-shelf libraries/modules/components utilized in the development of Apps;

(v). Digital Lenders shall ensure that code signing is used for the Apps to confirm the software author and guarantee that the code has not been altered or corrupted since it was signed;

(vi). Digital Lenders shall ensure that private key used for code signing is generated, securely stored and appropriately backed-up;

(vii). Digital Lenders shall ensure that minification and source code obfuscation techniques are used in the Apps;

(viii). Digital Lenders shall ensure to review application code prior to release to customers after any significant change, to identify any potential coding vulnerabilities;

(ix). Digital Lenders shall verify that apps are not vulnerable to common coding vulnerabilities by performing manual or automated penetration testing.

J. Input and Output Handling

(i). Digital Lenders shall ensure that any input coming from the client that is to be stored in databases is properly validated;

(ii). Digital Lenders shall ensure that input and output data is properly sanitized and validated at the server and at the client-end;

(iii). Auto-complete feature shall be disabled for sensitive information such as login IDs and passwords;

(iv). Clipboard/ copy-paste function shall be disabled for sensitive data. Digital Lenders may also use in-App keypad/ keyboard to capture the input from users.

K. Error and Exception Handling

(i). Apps shall have a proper error-handling mechanism and all errors shall be logged in the server.

(ii). Sensitive information and/or hints shall not be disclosed in error/warning messages and notifications;

L. Monitoring, Logs and Data Leakage

(i). Digital Lenders shall ensure that the App usage behavior is maintained and monitored through automated mechanism and deploy tools to identify any anomaly in the usage and behavior. The mechanism shall integrate with complete process of customer support for verification to clear the anomaly for consumer protection;

(ii). Digital Lenders shall ensure that Apps logs do not contain any sensitive data and where essentially required should be masked such that it no longer remains directly constructible in its complete form by collating components;

(iii). The logs shall be stored separately from the application/database servers and protected with appropriate access controls;

(iv). Digital Lenders shall implement appropriate security safeguards to protect the logs from unauthorized modification or destruction;

(v). Digital Lenders shall ensure that all the ecosystem logs are available for audits;

(vi). Digital Lenders shall implement appropriate control to protect transactional data/information against any loss or damage;

(vii). Server access controls and audit logs shall be maintained at the server level as per data retention policy.

M. App Vulnerability Assessment, Patching and Updating

(i). Digital Lenders shall ensure that the Apps have passed through extensive and recursive vulnerability assessment, scan and intrusion tests to identify weaknesses in App through both internal and independent assessors;

(ii). Digital Lenders shall ensure that the vulnerabilities identified during assessment scans, usage of the App or through independent identifier sources are fixed and updated to respective platform stores;

(iii). Digital Lenders shall ensure notifying users about update and enforce it within a grace period depending upon the criticality of fixes. The information about fixes shall be published in App release notes.

N. Application Programming Interface (APIs)

In order to establish adequate safeguards to manage the development and provision of APIs for secure delivery of third party provided services through Apps, Digital Lenders shall implement following measures:

(i). Establish security standards for designing and developing secure APIs including measures to protect the API keys or access tokens, which are used to authorize access to APIs to exchange confidential data. Digital Lenders shall define and enforce a reasonable timeframe for access token expiry to reduce the risk of unauthorized access;

(ii). A well-defined vetting process shall be put in place for assessing the appropriateness of third parties in connecting to the Apps via APIs, as well as governing third-party API access. The vetting criteria shall consider third party's nature of business, security policy, industry reputation and track record amongst others;

(iii). Perform risk assessment before allowing third parties to connect to their systems via APIs, and ensure the security implementation for each API is commensurate with the sensitivity and business criticality of the data being exchanged;

(iv). Strong authentication and access control mechanism to authorize and control access to designated API services in order to safeguard customer information;

(v). Strong encryption standards and key management controls to secure transmission of sensitive data through APIs;

(vi). The Digital Lenders shall have the ability to log the access sessions by the third party(ies), such as the identity of the third party making the API connections, and the data being accessed by them. Digital Lenders shall ensure to perform a robust security screening and testing of the API between the Digital Lenders and third party before going live;

(vii). Deploy real-time monitoring and alerting capabilities to ensure visibility of the usage and performance of APIs and detect suspicious activities. In the event of a breach, measures shall be in place to promptly revoke API keys or access tokens;

(viii). Take steps to handle high volumes of API call requests by legitimate applications, and implement measures to mitigate denial-of-service attacks while ensuring that these measures are commensurate with the criticality and availability requirements of the App.

O. Customer Awareness

(i). The App shall have a visible section/tab/module containing necessary legal, regulatory and compliance related information with required disclaimers and acknowledgment of facts (such as relating to the extent of collection, storage, and disposal of data), rights, responsibilities and liabilities of both the borrowers and Digital Lenders;

(ii). Digital Lenders shall ensure to educate and inform borrowers/users clearly about how to access, download, securely use and cease to use the Apps within the App interface as well as through official application release channels in order to mitigate the risk of running malware-infected Apps;

(iii). Digital Lenders shall ensure that a robust remedial process of customer support and complaint resolution is defined and implemented to address any security incidence albeit targeted, sectoral or global related to Apps user(s) or their back-end infrastructure;

(iv). Digital Lenders shall ensure that Apps are hosted only at the relevant App platform and shall not be hosted for downloading at App owner's website or the vendor website or any other third-party website;

(v). Digital Lenders shall undertake active awareness campaigns to educate customer and internal staff about malicious messages, phishing attacks, and spoofing;

(vi). All of the above information should be in a structured, clear and understandable form at least both in English and Urdu languages.