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

No. SC/NBFC-1-196/Circular/2024/ 77

May 22**, 2024**

Circular No. 14 **of 2024**

Subject: Requirements for Self-Assessment Declaration to be submitted by NBFCs engaged in Digital Lending along with application for whitelisting of digital Lending App

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, and in furtherance to its earlier Circular No. 12 of 2024 dated May 15, 2024, is hereby pleased to specify the contents and format of the self-assessment declaration, to be signed by the Chief Executive Officer of the Digital Lender, as required in terms of clause 6(a) of the above referred circular dated May 15, 2024.

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).

Commissioner (SCD)

Enclosed: As above

Distribution:

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

SECURITIES & EXCHANGE
COMMISSION OF PAKISTAN

SELF-ASSESSMENT DECLARATION FOR DIGITAL LENDING APP WHITELISTING

SELF-ASSESSMENT DECLARATION OF REGULATORY COMPLIANCES

For Whitelisting of Digital Lending App under Clause 6(a) of Circular 12 of 2024

Reference to Clause 6(a) of Circular 12 of 2024 issued on May 15th 2024 (the Circular), whereby a digital lender is required to submit self-assessment declaration of regulatory compliance for listing its Digital Lending App (App) on SECP App Whitelist. The self-assessment declaration shall cover all requirements of regulatory compliance specified in the Circular on format specified in Annexure-A. The self-assessment will also be supported by the documents mentioned in Annexure-B.

(i) All lending NBFCs are hereby advised to consider following points while designing the UI/UX of their proposed App:
1. All access related permissions shall be sought from the user at the time of sign-up and all required documents other than loan agreement shall be disclosed to user before sign-up.
2. In-case of nano lending the option of calculator shall be displayed at sign-up screen.
3. Not use official logo of the Commission or any other government agency.

(ii) All Digital Lenders are required to ensure that 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.

(iii) All Digital Lenders engaged in digital nano lending are required to ensure that:
1. Compounding of markup shall not be allowed (no markup shall accrue either on original markup or on late payment charges).
2. Aggregate amount of nano-lending extended to a borrower by all NBFCs shall not exceed Rs. 100,000 at any point in time.
3. 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.
4. An NBFC shall consider rollover/restructuring as extension of existing loan and shall not treat it as new loan.
5. An NBFC shall apply the same APR and terms to loan rollover/restructuring as applied to the existing loan.
6. 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.

Name of NBFC ________________________________

License Type ________________________________

Category (i.e Nano, BNPL, B2B, EWA etc) ________________________________

Name of the App ________________________________

Date of submission ________________________________

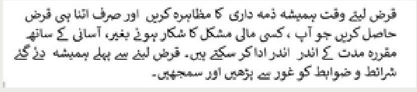
I hereby declare that the self-assessment conducted on our App adheres to all stipulated requirements. Our diligent evaluation ensures compliance with data protection, cybersecurity, borrowers protection including all disclosure requirements specified in the Circular.

________________________________ ________________________________

Chief Executive Officer **Signature & Stamp**

Annexure - A

Checklist of Compliance Related to App UI/UX

S#	Section / Stage	Clause	Description	Compliance Status (P)		Evidence / Screenshot *(Mention Attachment Reference)*
				Yes	***No***	
1	Main Screen	3(c)(iv)	Contain the Digital Lender's full corporate name and licensing status (including license no.) on its App, documentation and advertisement materials.			
2		1(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 the App registration process.			
3	Awareness Message Pop-up	2(a)(x)	A prompt/alert in English and Urdu 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 دیۓ 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."*			
4	Sign-up/User Registration	C(i) of Annex-C	Digital Lenders shall ensure that explicit customer consent in a convenient manner is obtained before allowing registration of Apps.			
5		C(ii) of Annex-C	A login authentication shall be in place.			
6		C(iii) of Annex-C	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.			

S#	Section / Stage	Clause	Description	Compliance Status (P)		Evidence / Screenshot *(Mention Attachment Reference)*
				Yes	*No*	
7	Sign-up/User Registration	5(c)(ii)	Digital Lender shall not access the borrower's SMS or call log or phone book or contacts list or photo gallery and contact 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.			
8		1(b)(i)	Privacy policy duly vetted by a law firm specialized in the field of Banking and Finance.			
9		1(b)(vi)	Details of grievance redressal system.			
10		1(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.			
11	Post-sign up	2(a)(i)	Display of Maximum Loan Size & Tenor. In case of nano; 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.			
12		2(a)(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 option.			
13	KYC /Borrowers Information		Mandatory information related to KYC requirement shall be sought from the borrower.			
14	Existing credit exposure	3(b)(i)	Requiring additional information /undertaking from borrowers regarding their current borrowing from all lenders. *In-app check on credit exposure of the App*			
15	Reference Contacts	5(c)(ii)	Reference contacts who have provided their consent to digital lender at time of the loan approval.			
16	CNIC Upload		As part KYC requirement digital lenders are required to upload CNIC picture (front & back) and OCR function shall be enabled.			
17	Live Selfie/In-app biometric verification	6(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 KYC process.			

S#	Section / Stage	Clause	Description	Compliance Status (P)		Evidence / Screenshot *(Mention Attachment Reference)*
				Yes	*No*	
18	Title Fetching	1(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).			
19	Key Fact Statement	1(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. *Explanation: Text to Speech option shall be clearly understandable and preferably in Urdu language.*			
20		1(d)	Disclose that any fees, charges, etc., which are not mentioned in the key fact statement cannot be charged to the borrower at any stage during the term of the loan.			
21		1(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.			
22		1(b)(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.			
23		1(b)(iii)	**Financing details -** amount and term of loan along with number of instalments and the amount to be paid for each instalment.			
24		1(b)(iv)	**Fees and charges -** applicable fees and charges by whichever name called, and their nature, including implied charges/penalties.			
25		1(b)(v)	Details of early Settlement if allowed.			
26		1(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.			
27		2(a)(vii)	In case of nano lending; Digital Lender shall not charge Profit Rate (PR) exceeding 0.75% per day, with an APR not to exceed 274%			

S#	Section / Stage	Clause	Description	Compliance Status (P)		Evidence / Screenshot *(Mention Attachment Reference)*
				Yes	*No*	
28	Key Fact Statement	1(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 or if the product delivery fails, the amount received shall be refunded to the borrower within a period not exceeding two working days.			
29		1(i)	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 in case 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.			
30	Submission of Application/ Dissemination of Documents /SMS	1(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. *Note: Digital Lender shall disseminate message at time of application submission, loan approval and disbursement of funds.*			
31	Intimation of the loan approval		Digital Lender shall intimate the borrower regarding the approval of loan through SMS/In-app notification and after the acceptance loan shall be disbursed.			
32	Loan disbursal	1(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.			
33	Repayment option through App		Specify the mode of recovery collection.			
34		1(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.			

S#	Section / Stage	Clause	Description	Compliance Status (P)		Evidence / Screenshot *(Mention Attachment Reference)*
				Yes	*No*	
35	Pricing Policy, Credit Risk and Advertisements /Publications	3(c)(iii)	Any advertisement and publication shall contain full disclosure regarding loans on offer and applicable APR.			
36		3(c)(v)	An NBFC shall 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.			
37	Loan Collection	5(c)(ii)	Digital Lender shall not access the borrower's SMS or call log or phone book or contacts list or photo gallery and contact 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.			
38	Confidentiality	7(a)	Disclosure of information with the specific written or recorded consent of the borrower.			

Requirements for Mobile Application Security

S#	Section / Stage	Clause	Description	Compliance Status (P)		Evidence / Screenshot *(Mention Attachment Reference)*
				Yes	*No*	
1	Secure Access Management	8(A)(i)(I)	Approved policies and procedures for secure access management should exist.			
2		8(A)(i)(II)	User account of employees who leave the organization should be disabled.			
3		8(A)(i)(III)	Ensure no privileged (admin) user IDs are in use without formal approval.			
4		8(A)(i)(IV)	Maintain inventory of privileged accounts and review frequency should be defined.			
5		8(A)(i)(V)	Ensure that access rights review document for application is in place.			
6		8(A)(i)(VI)	Appropriate user creation, modification of rights, revocation of rights should be performed and approvals from line manager should be in place.			
7		8(A)(i)(VII)	Validate that strong password policy is implemented which covers password complexity, minimum length, history and minimum age.			
8	Perimeter and Network Security	8(A)(ii)(I)	Maintain high level network diagram of mobile application environment indicating the location of network devices, app and database servers and other components attached.			
9		8(A)(ii)(II)	Implement security measures to protect against unauthorized access or attacks.			
10		8(A)(ii)(III)	Validate that inbound security policies are enabled for in scope application environment.			
11		8(A)(ii)(IV)	Verify from firewall that only trusted users are allowed to access the applications.			
12		8(A)(ii)(V)	Logging and monitoring process on firewall put in place.			
13		8(A)(ii)(VI)	Validate the details of Encryption mechanism, TLS version, digital certificate on application portal.			

S#	Section / Stage	Clause	Description	Compliance Status (P)		Evidence / Screenshot *(Mention Attachment Reference)*
				Yes	***No***	
14	Endpoint, Server and Cloud Security	8(A)(iii)(I)	Verify that versions and patches of all endpoints are updated and secured.			
15		8(A)(iii)(II)	Ensure that software installation and upgradation rights on servers/instance is only limited to the Authorized person.			
16		8(A)(iii)(III)	Ensure that software installation on endpoints should be restricted and approved on a need-to-use basis.			
17	Application Level Security	8(A)(iv)(I)	Make sure all the components required for the application such as web server and other components are updated and running on latest versions.			
18		8(A)(iv)(II)	Implementation of Web Application Firewall (WAF) on customer facing interfaces should be ensured.			
19		8(A)(iv)(III)	Maintain details of the latest VAPT conducted on mobile application portal/mobile app, system, and database.			
20		8(A)(iv)(IV)	Conduct VAPT on the in-scope system, including the mobile application portal/mobile app, system, and database.			
21		8(A)(iv)(V)	Ensure that API are not using outdated SSL/TLS protocols.			
22	Data Security	8(A)(v)(I)	Approved data security policy and procedure should be in place.			
23		8(A)(v)(II)	Ensure that the relevant documentation is maintained and reviewed.			
24		8(A)(v)(III)	Encrypt data at rest (including backups) and in transit using strong and non-obsolete cryptographic algorithms.			
25		8(A)(v)(IV)	Encrypt data at rest (including backups) and in transit using strong and non-obsolete cryptographic algorithms.			
26		8(A)(v)(V)	Ensure that the separate channels are being used for storage and transmission of critical data.			
27	Incident Surveillance and Monitoring	8(A)(vi)(I)	Ensure the policies and procedures are in place for Incident Management and Reporting.			
28		8(A)(vi)(II)	Ensure that the anomalies are detected and resolved in a timely manner			

S#	Section / Stage	Clause	Description	Compliance Status (P)		Evidence / Screenshot *(Mention Attachment Reference)*
				Yes	*No*	
29	Incident Surveillance and Monitoring	8(A)(vi)(III)	Ensure that incident management procedure is implemented and appropriate reporting matrix is maintained for such incidents.			
30		8(A)(vi)(IV)	Incident response functions shall be implemented in application system, responses to any incident should be documented for record.			
31		8(A)(vi)(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.			
32	Patch Management	8(A)(vii)(I)	Validate that log of patches deployed are documented.			
33		8(A)(vii)(II)	Validate that formal process of approval is in place for patch testing, User acceptance testing and migration to production.			
34		8(A)(vii)(III)	Approved patch management policies and procedures should be in place.			
35		8(A)(vii)(IV)	Procedure for approval of tested patches should be defined. UATs of the patches should be in segregated environment.			
36		8(A)(vii)(V)	Validate that patches are applied on test system first before provisioning to live.			
37	Logging and Backups	8(A)(viii)(I)	Validate that policies and procedures are approved and implemented for Backup and recovery of in-scope application.			
38		8(A)(viii)(II)	Validate that logging is enabled at application, platform, database and operating system levels.			
39		8(A)(viii)(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.			
40		8(A)(viii)(IV)	Frequency of backups should be defined in the system for both production and development and the same shall be documented in relevant policy.			
41	Policy	8(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.			

S#	Section / Stage	Clause	Description	Compliance Status (P)		Evidence / Screenshot *(Mention Attachment Reference)*
				Yes	***No***	
42	Third Party Vendor Assessment	8(c)(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.			
43	Data Residency Requirement	8(d)	Data shall not be stored on any cloud infrastructure outside the jurisdiction of Pakistan.			

Annexure - B

Requisite Documents to Accompany Application for Whitelisting

S#	Document
1	Privacy Policy vetted by Law Firm
2	Undertaking confirming that all requisite agreements with relevant parties (including all private credit bureaus, NADRA, payment gateways, local cloud service provider etc.) are in place
3	Terms & Conditions of the App
4	Grievance Redressal Policy
5	Copy of standard loan agreement
6	Board authorization for the Chief Executive Officer to submit this self-assessment declaration