SECURITIES AND EXCHANGE COMMISSION OF PAKISTAN
Specialized Companies Division
Policy, Regulation and Development Department

No. SC/NBFC-1-196/Circular/2022/ 49 December 27, 2022

Circular No. 15 of 2022

Subject: **Requirements for NBFCs engaged in Digital Lending**

The Securities and Exchange Commission of Pakistan (the "Commission") in order to ensure fair treatment, full disclosure and protection of personal information of the borrowers, and in exercise of powers conferred under sub-section (3) of section 282B of the Companies Ordinance, 1984 (XLVII of 1984), hereby imposes the following requirements on Non-Banking Finance Companies (NBFCs) undertaking lending activities through mobile applications (Apps), encompassing the following aspects:

1. Applicability:
2. Disclosure to Borrowers;
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; and
9. Glossary of Terms.

1. Applicability

These requirements shall be applicable to the Lending NBFCs with respect to their mobile App being administered, managed or owned by them for digital lending.

2. Disclosure to Borrowers

(1) 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. This information should be presented in the form of audio/video or a pop-out prompt;

(2) **Before entering into any agreement for loan,** 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:

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

b. **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:

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

d. **Early Settlement charges**- calculation of charges/penalties, if the loan facility is settled before maturity of the loan;

e. **fees and charges**- applicable fees and charges by whichever name called, and their nature, including implied charges/penalties; and

f. **contact details**- details of Grievance Redressal System.

(3) 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 as provided in **Annexure – A**:

(4) 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;

(5) Digital Lender shall also provide comprehensive disclosures to the borrowers on collection of data, its safe storage, sharing and its usage and in this regard shall also obtain express 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 including information stored on the device such as videos, photos, SMS or other digital content etc;

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

(7) 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:

(8) 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;

(9) Digital Lender shall ensure that digitally signed documents (on the letter head of the Digital Lender) viz., summary of loan product, sanction letter, terms and conditions, account statements, privacy policies of the Digital Lender with respect to borrower's data, etc. shall automatically flow to the borrowers on their registered and verified email/ SMS upon execution of the loan contract/ transactions;

(10) 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 without prior consent of the borrower;

(11) 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;

(12) 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

(13) 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).

3. Pricing Policy, Credit Risk and Advertisements /Publications

(1) 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;

(2) 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:

a. requiring additional information /undertaking from borrowers regarding their current borrowing from all lenders;

b. obtaining membership of CIBs and use CIB data as part of the loan decision process; and

c. ensuring regular/continuous reporting to all the credit bureaus operating in Pakistan on real time basis.

(3) A Digital Lender shall make available on its website, 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:

a. be fair and reasonable and not contain misleading information;

b. not use official logo of the Commission or any other government agency;

c. contain full disclosure regarding loans on offer and applicable APR; and

d. contain the Digital Lender's full corporate name and licensing status (including license no.) on its App, documentation, advertisements materials, and

e. 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:

a. No. of complaints outstanding from previous month;

b. Total no. of complaints during current month;

c. Nature of repetitive complaints;

d. No. of complaints resolved;

e. No. of complaints outstanding;

f. Satisfaction ratio;

g. Average time taken for disposal of a complaint; and

h. Monthly trend analysis of complaints received and disposed.

5. **Loan Collection**

(1) 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:

(2) 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;

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

a. contacting at unreasonable or inconvenient times i.e. before 7 a.m. or after 10:00 p.m.:

b. notwithstanding the borrower's consent. accessing the borrower's 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;

c. 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;

d. use of or threat to use violence or other illegal means to harm the person. or his reputation or property;

e. use of obscene or profane language for the borrower or the borrower's references or contacts;

f. improper or immoral debt collection tactics. methods or an act that is illegal; and

g. any other conduct whose consequence is to harass. oppress. or abuse any person in connection with the collection of a debt.

(4) 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

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

6. **Requirements for Digital Lending Apps**

(1) Prior to launch of an App or any other digital channel for lending, the Digital Lender shall seek approval of the Commission and submit a certificate from the Pakistan Telecommunication Authority's (PTA) approved Cyber Security Audit Firm (CSAF) regarding compliance with the requirements of this Circular, as applicable:

(2) A Digital Lender at the time of launching the App shall provide license status along with approval granted by the Commission for 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:

(3) A digital lender shall operate only one App at a particular time:

(4) The Digital Lenders having more than one existing App(s). shall submit the name of their one operational App that will continue operations and a list of such additional Apps that they plan to shut down;

(5) For the one existing App that will continue operations, the Digital Lender shall submit the requisite certificate from PTA approved CSAF and ensure that all other Apps shall cease to exist:

(6) The Commission shall maintain and publish the list of the Digital Lending Apps on its official website:

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

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 the 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. Mobile Application Security

(1) 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:

a. Secure Access Management;
b. Perimeter and Network Security;
c. Endpoint, Server and cloud security;
d. Application level Security;
e. Data Security;
f. Incident surveillance and monitoring;
g. Patch management;
h. Logging and backups; and
i. Secure Codes.

(2) 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;

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

a. Put in place necessary App documentation including manuals on development, testing, training, production, operational administration, user guides and Service Level Agreements (SLAs);
b. 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;
c. Carry out system and User Acceptance Testing (UAT) in an environment separate from the production environment; and
d. 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.

(4) Data shall not be stored on any cloud infrastructure outside the jurisdiction of Pakistan. Moreover, data currently stored on cloud infrastructure/hosting/data centers outside the jurisdiction of Pakistan shall be shifted/transferred inside the jurisdiction of Pakistan;

(5) A Digital Lender shall share the particulars of its Security/IT team and any change thereof with the Commission;

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

(7) Digital lenders shall arrange at least on a bi-annual basis (every two years), IT audit of 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 three months of the end of the respective financial year;

(8) 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

(9) 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

(1) **"Digital Lending"** means providing finance through digital, technology-based or internet-based channels, Apps or tools, with limited or no human interaction for loan application, approval, disbursement and repayment;

(2) **"Digital Lender"** means Commission's licensed Lending NBFCs that operate, facilitate, or provide mobile application or platform for Digital Lending to the borrowers;

(3) **"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;

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

(5) **"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 has the right to withdraw from the loan agreement and repay the principal amount to the digital lender without any markup/interest.

Following the issuance of this circular, all Digital Lenders must ensure compliance with requirements under clauses 2, 3, 4, 5 and 7 within seven days and clauses 6 and 8 within ninety days. However, clauses 6(1) and 6(4) will take effect immediately, while digital lenders must ensure compliance with clause 8(4) within one year of the publication of this Circular, and submit quarterly progress reports to the Commission in this respect.

Any non-compliance shall attract the penal provisions of section 282J of the Companies Ordinance, 1984.

(Akif Saeed)
Chairman/Commissioner (SCD)

Distribution:

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

Annexure – A
(Clause 2(3) of the Circular)

Summary of Minimum Information to be provided to the borrower: -

Sr. No.	Parameter	Details
a.	Loan Amount approved (Rs.);	
b.	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):	
c.	Annual Percentage Rate;	
d.	Processing fee charges (Rs.);	
e.	Any other charges (Rs.);	
f.	Amount being disbursed and the amount to be repaid in lump sum or in installments (Rs.);	
g.	Tenor of loan and repayment frequency & date(s);	
h.	Late Payment/Additional Per day charges in case of late payments; and	
i.	Name, designation, address and phone number of officer designated to deal with digital lending complaints/issues.	

Annexure – B
(Clause 8(5) 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 Apps;

(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;

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

f) Define maximum duration for termination of inactive mobile service sessions:

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 or connections from unsecured networks like unsecured Wi-Fi 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;

(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.