**PART II**

**Statutory Notifications (S. R. O.)**

**GOVERNMENT OF PAKISTAN**

**Securities and Exchange Commission of Pakistan**

**NOTIFICATION**

***Islamabad, November 11, 2025***

**S.R.O.2120(I)/2025.-** In exercise of the powers conferred by sub-section (2) of section 282B of the Companies Ordinance, 1984 (XLVII of 1984), the Securities and Exchange Commission of Pakistan is pleased to make the following amendments in the Non-Banking Finance Companies and Notified Entities Regulations, 2008, and the same having been previously published in official Gazette vide S.R.O 1103(I)/2025, dated June 5th 2025, namely:-

**AMENDMENTS**

In the aforesaid Regulations, -

(1) in regulation 2, in sub-regulation (1), -

(i) after clause (i), the following new clause shall be inserted, namely: -

"(ia) "Buy Now Pay Later (BNPL)" means a buy now pay later arrangement, or a series of arrangements

(a) under which a person (the merchant) supplies good or services to another person (the consumer);

(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 consumer under which the BNPL provider provides finance to the consumer in connection with the supply mentioned in sub-clause (a);"

(ii) for clause (iii), the following shall be substituted, namely: -

"(iii) Borrower" means a person who has obtained Finance from a lending

NBFC;

(iii) after clause (xi), the following new clause shall be inserted, namely: -

"(xia) "Credit Guarantee Institution" means an NBFC licensed as Investment Finance Services, to undertake the activities provided under the Rule 2(1)(xx)(ii).";

(iv) after clause (xia), inserted as aforesaid, the following new clause shall be inserted, namely: -

"(xiab) "Customer" means person to whom finance has been extended by a lending NBFC";

(v) for clause (xiaa), for the word "User's", the word "participant's" shall be substituted;

(vi) for clause (xxviib), the following shall be substituted, namely: -

"(xxviib) "Microenterprises" means projects or businesses in trading or manufacturing or services or agriculture that lead to livelihood improvement and income generation. These projects or businesses are undertaken by micro entrepreneurs who are either self-employed or employ few individuals not exceeding 25 (excluding seasonal labour) Microenterprises may include carpentry, electrical works, food stalls, farms (crops & non-crops), lathe machine workshops etc. which have traditionally lacked access to formal financial services.;";

(vii) after clause (xxviib), substituted as aforesaid, the following new clause shall be inserted, namely: -

"(xxviiba) "Nano Loans" are unsecured, short-term cash financing facilities, subject to maximum limits as determined by the Commission from time to time.";

(viii) for clause (xxxive), the words "or otherwise" shall be omitted;

(ix) after the clause (xxxivf), the following new clause shall be inserted, namely: -

"(xxxivg) i. "Qualified Financial Institution" means a local or an international multilateral financial institution rated AAA by a credit rating agency registered with the Commission.

ii. For the purpose of this regulation expressions are defined as:

(a) "Capital Event" means the depletion of the equity (after the Callable Capital has been completely drawn down by the lending NBFC) of the lending NBFC.

(b) "Callable Capital" means share capital that, in terms of a written agreement entered into between the NBFC and a sponsor, shareholder and/or investors, as the cause may be, is agreed to be subscribed on the following terms and conditions: -

iii. The shares shall be fully subscribed over a period of twenty-four (24) months from the date of the written agreement;

(a) During the subscription period specified in sub-clause (a), the obligation to subscribe to shares shall be irrevocable and on demand, at the sole discretion of the NBFC; and

(b) the subscription obligation shall be secured by a bank guarantee or standby letter of credit from a commercial bank rated AAA or higher by a credit rating agency registered with the commission;"; and

(c) "Contingent Capital'' means long term commitment for finance that, in terms of a written agreement entered into between the NBFC and a Qualified Financial Institution(s), is provided as a second loss facility on the following terms and conditions: -

(i) at any time, the Contingent Capital, in aggregate, shall not exceed one and a half (1.5) times of the sum of paid up share capital and Callable Capital of the NBFC;

(ii) the commitment shall, in accordance with the terms thereof, be irrevocable, confirmed and fully committed;

(iii) the long-term commitment and the finance thereunder shall be available on a revolving basis;

(iv) the finance under the commitment shall be callable on demand upon a Capital Event and at the sole discretion of the NBFC or on a direction by the Commission (after giving the NBFC a reasonable opportunity of a hearing), which shall be binding on the NBFC; and

(v) the commitment shall be replaced by the NBFC if the financing entity ceases to be a Qualified Financial Institution;";

(x) after clause (xl), the following new clause shall be inserted, namely: -

"(xla) "Shariah Advisor" shall have the same meaning as assigned to it in the Shariah Governance Regulations, 2023";

(xi) in clause (xli), -

(a) in sub-clause (a), the words "and employees (including contractual) up to 50; and" shall be omitted; and

(b) in sub-clause (b), the words "and number of employee (including contractual) between 51 to 100 for trading entity and between 51 to 250 for manufacturing or service entity." shall be omitted;

(xii) for clause (xliii), for the words "fixed assets", the words "property plant and equipment;"; shall be substituted; and

(xiii) clause (xlix) shall be omitted;

(2) in regulation 4, -

(i) after the words "Schedule I.", the following proviso shall be inserted, namely: -

"Provided that an NBFC licensed for investment finance services shall be valid to undertake leasing, housing finance services, and discounting services without requiring separate licenses for each form of business. It shall, maintain the minimum equity requirement prescribed in Schedule I for investment finance services.";

(3) in regulation 12, after the words "shall apply to", the words "Lending NBFCs including" shall be inserted;

(4) in regulation 15B,-

(i) for sub-regulation (2), for the first and second proviso, the following shall be substituted, namely: -

"Provided that contingent liability of credit guarantee institution shall not exceed the 10 times of the equity and qualified capital specified under these regulations and its terms and conditions";

(5) in regulation 17,-

(i) for sub-regulation (1), the following shall be substituted, namely: -

"(1) The total outstanding Exposure (fund based and non-fund based) by an NBFC to a person shall not at any time exceed twenty per cent (20) of the equity of an NBFC (as disclosed in the latest financial statements:

Provided that the maximum outstanding fund based Exposure does not exceed fifteen per cent (15) of the equity of an NBFC:

Provided further that the total outstanding Exposure non-fund based by a credit guarantee institution to a person shall not at any time exceed forty per cent (40%) of the equity, subject to that its contingent liability shall not exceed five time of its equity (as disclosed in the latest financial statements) and Qualified Capital as per the following terms and conditions:

(i) the NBFC shall not take any exposure against the Qualified Capital unless it has obtained a certificate from its statutory auditor that all the requirements specified above have been complied with;

(ii) the certificate shall be supported by a legal opinion from a reputed law firm and copy of the certificate along with the legal opinion shall be submitted to the Commission; and

(iii) with regard to its Qualified Capital, the NBFC, in relevant notes to its financial statements, shall make disclosures, which are necessary for the users to understand its salient features:

Provided further that a non-deposit taking NBFC that is not involved in retail lending and provides finance to other NBFCs or financial institutions, may exceed the above limits by up to five percent and ten percent of its equity, respectively.";

(ii) for sub-regulation (2), the following shall be substituted, namely: -

"(2) The total outstanding Exposure (fund based and non-fund based) by an NBFC to any group shall not exceed twenty-five per cent (25) of the equity of an NBFC (as disclosed in the latest financial statements):

Provided that the maximum outstanding fund-based Exposure does not exceed twenty per cent (20) of the equity of an NBFC:

Provided further that the limits prescribed in sub-regulation (1) and (2) shall not be applicable to exposure taken by an NBFC in its own subsidiaries out of its surplus equity;

Provided that the total outstanding Exposure (non-fund based) by a credit guarantee institution to any group shall not exceed fifty per cent (50%) of the equity, subject to that its contingent liability shall not exceed five time of its equity

(as disclosed in the latest financial statements) and Qualified Capital as per the following terms and conditions:

(i) The NBFC shall not take any exposure against the Qualified Capital unless it has obtained a certificate from its statutory auditor that all the requirements specified above have been complied with;

(ii) The certificate shall be supported by a legal opinion from a reputed law firm and copy of the certificate along with the legal opinion shall be submitted to the Commission; and

(iii) With regard to its Qualified Capital, the NBFC, in relevant notes to its financial statements, shall make disclosures, which are necessary for the users to understand its salient features.

Provided further that an NBFC that is not involved in retail lending and provides finance to other NBFCs or financial institutions, may exceed the above limits by up to five percent and ten percent of its equity, respectively.]"

(iii) for sub-regulation (3),

(a) in clause (a), for the expression "1,500,000", the expression "3,000,000" shall be substituted; and

(b) in clause (b), for the expression "1,500,000", the expression "3,000,000" shall be substituted;

(iv) for sub-regulation (4), for clause (c), the following shall be substituted, namely: -

"(c) 85% of the unconditional financial guarantees, payable on demand, issued by the scheduled banks/DFIs [or NBFCs engaged exclusively in the business of issuance of gurantees,] rated at least 'A' or equivalent by a credit rating agency registered with the Commission, accepted as collateral by NBFCs shall be deducted from the Exposure. Same weightage shall apply to the guarantees of similar nature issued by the International Finance Corporation (IFC), Commonwealth Development Corporation (CDC) Deutsche Investitions und Entwicklungsgesellschaft mbH (DEG), Nederlandse Financierings-Maatschappij voor Ontwikkelingslanden N.V (FMO), GuarantCo Limited, Asian Development Bank (ADB) and US International Development Finance Corporation (DFC) or any other institution notified by the Commission."; and

(v) sub-regulation 5 shall be omitted;

(6) in regulation 20, after the words “Investment Finance Company”, the words “or non-bank micro finance company or Housing Finance Company” shall be inserted;

(7) in regulation 21, -

(i) in sub-regulation (2), for the words “In case of micro financing, the NBFC shall”, the words “All lending NBFCs including Non-Bank Micro Finance Companies shall:” shall be substituted;

(ii) for sub-regulation (4), the following shall be substituted, namely: -

“(4) An NBFC shall not provide finance to a borrower whose CIB report reflects any unsettled default or write-off from any credit institution during the last three years.

Explanation: - For the purpose of this regulation credit institutions means as defined in the Credit Bureaus Act, 2015”;

(iii) in sub-regulation (8), after the word “The”, in the beginning, the word “lending” shall be inserted, and after the word “NBFC”, the words “involved in Micro Financing” shall be omitted;

(iv) after sub-regulation (9), the following new sub-regulation shall be inserted, namely: -

“(10) An NBFC engaged in digital lending shall ensure that the information required in the basic fact sheet is provided by the Borrower digitally as given in Schedule XIIAB.]”;

(8) in regulation 22 ,-

(i) in sub-regulation (2), after the word “NBFC”, the words “or a listed NBFC” shall be inserted and after the word “interests.”, occurring at the end, the following table shall be inserted, namely: -

“

| | |
|---|---|
| Shares of listed companies | 30% of their current market value. An NBFC shall monitor the margin on at least weekly basis and shall institute a robust top-up and automatic sell-out process at 25% and 50% erosion in the margin held respectively. An NBFC may choose different percentages on the basis of the documented credit policy approved by their |

| | |
|---|---|
| | board |
| Listed TFCs | Exposure against listed TFCs which are rated 'A' (or equivalent) or above by a credit rating agency registered with the Commission shall be subject to a minimum margin of 10% Exposure against listed TFCs rated 'A–' and 'BBB' shall be subject to a minimum margin of 20%. |
| Bank deposits and Certificate of Deposit of NBFCs or DFIs and Certificates of Musharaka issued by Modarabas with minimum credit rating of A- by a credit rating agency registered with the Commission. | 15% |
| Government backed securities | 10% |
| Pledge of trading stocks | 25% |
| Hypothecation of trading stocks | 50% |

";

(9) in regulation 25, in sub-regulation (8), for the words "Section 234(3) of the Ordinance", the words "Section 225(1) of the Companies Act, 2017" shall be substituted;

(10) for regulation 28, in sub-regulation (1),-

(i) after clause (da), the following new clauses shall be inserted, namely:-

"(db) Existing Lending NBFC that hold valid license from the Commission may apply for the conversion of its license to digital lending NBFC.";

"(dc) Lending NBFCs shall comply with the guidelines issued by the Commission on Grievance Redressal System and report to the Commission the information specified in the guidelines."; and

"(dd) Lending NBFCs shall maintain a website containing following

minimum information;

(i) latest financial statements;

(ii) profile/List of Board of Directors;

(iii) complaint handling mechanism and related details;

(iv) addresses/contact details of branches (if applicable); and

(v) SECP investor complaints and web addresses;" and

(ii) in clause (g), sub-clause (vii) shall be omitted;

(11) in regulation 35A, -

(i) in sub-regulation (2),

(a) after the word "A", in the beginning, the words "non-deposit taking" shall be inserted;

(b) for clause (i), the following shall be substituted, namely:

"(i) It shall have a minimum equity of Rs. 150 million or such higher amount as the Commission may notify, including the minimum equity requirement as specified under schedule I of Non-Banking Finance Companies and Notified Entities Regulations, 2008."; and

(c) after clause (i), amended as aforesaid, the following new clauses shall be inserted, namely: -

"(ia) shall be eligible to obtain the approval of P2P service provider after operating for a minimum period of one year from the date of business commencement and obtaining a credit rating of at least BBB.

Provided that NBFC shall submit 12 Month Audited Accounts."; and

"(ib) It shall have minimum five directors on the board.";

(12) for regulation 35B, in sub-regulation (1), for the expression "XVI", wherever occurring, the expression "XVIA" shall be substituted;

(13) in regulation 35C, in sub-regulation (2), after the word "valid", the words "for single platform" shall be inserted;

(14) in regulation 35D, -

(i) in sub regulation (1),

(a) in clause (a), after the word "borrowing", the words "for BNPL and working capital finance or any other activity as may be allowed by Commission on case to case basis;" shall be inserted;

(b) in clause (b), for the word "fifteen", the word "twenty" shall be substituted;

(c) in clause (e), for the word "Users", the word "participants" shall be substituted;

(d) in clause (i), for the word "investors", the word "lender's" shall be substituted; and

(e) after the clause (i), amended as aforesaid, the following new clause shall be inserted, namely: -

"(j) shall create a "platform contingent fund" wherein at least 5% of its after-tax profits shall be credited and the platform contingent fund shall be separately disclosed in the statement of financial position.

P2P Service Provider may invest platform contingent fund into liquid assets.";

(ii) in sub-regulation (2), clause (c) shall be omitted;

(15) in regulation 35E,-

(i) in sub-regulation (1),

(a) after clause (a), the following proviso shall be inserted, namely: -

"Provided that this requirement shall not be applicable in case of secured lending backed by tangible security with adequate insurance coverage";

(b) after clause (b), the following proviso shall be inserted, namely: -

"Provided that in case of secured lending backed by tangible security with adequate insurance coverage, exposure of a single lender to the same borrower shall not exceed Rs. 5,000,000/-";

(c) after the clause (b), amended as aforesaid, the following new clause shall be inserted, namely: -

"(ba) the exposure of a single borrower from multiple lenders on a P2P

Lending Platform, shall not exceed Rs. 1,000,000/-

Provided that this requirement shall not be applicable in case of secured lending backed by tangible security with adequate insurance coverage;"

(d) for clause (c), the following shall be substituted, namely: -

"(c) maximum limit for a single lender on all P2P Lending Platforms, shall be as under or any other limit specified by the Commission from time to time:

(i) for an individual: Rs. 1,000,000;

(ii) sole proprietor, and section 42 company: Rs. 5,000,000; and

(iii) other Lenders: Rs. 50,000,000.";

(e) in clause (d), for the words "12", the words "36" shall be substituted;

(f) for clause (e), the following shall be substituted:-

"(e) lenders shall meet the following eligibility criteria;

(i) high net worth persons having net worth of at least Rs. 15 million excluding personal residence;

(ii) person having taxable income exceeding Rs. 4,100,000 per annum

Provided that such lender shall only be allowed to extend credit for the loan ticket size not exceeding to Rs. 100,000, with a loan tenor not exceeding 12 months.

Provided further if the non-performing loans on the P2P platform exceeds 5% of the outstanding principal amount of the platform and 10% of the outstanding principal amount of the P2P service provider, the service provider shall cease onboarding the individual lenders.

Explanation: For the purpose of this sub-regulation, "non-performing loans" refer to outstanding loans, including principal and markup payments, where the days past due (DPD) exceed 30 days.

(g) in clause (f), the word "and", occurring at the end, shall be omitted; and

(h) after clause (g), the word "and", at the end, shall be inserted and the following new clause shall be inserted, namely: -

"(h) lenders' outstanding lending exposure on a P2P lending platform shall not exceed five times of the P2P Service Provider's equity.";

(ii) in sub-regulation (4), after the word "conditions", the full stop, at the end, shall be substituted with a colon and the following proviso shall be inserted, namely: -

"Provided that in case of auto disbursal, a pre-approved risk assessment

algorithm, based on lender's past transactions, has been applied and the lender(s) have pre-authorized such transactions under specific and explicit conditions outlined in the agreement with the P2P Lending Platform";

(16) in regulation 35F,-

(i) in sub-regulation (1), after clause (d), the following new para shall be inserted, namely: -

"The decision for revocation of permission shall be taken after providing the NBFC an opportunity of being heard.";

(ii) in sub-regulation (2),-

(a) for the word "cancelled", the word "suspended" shall be substituted; and

(b) after clause (b), the following para shall be omitted; and

(iii) in sub-regulation (3), clause b., the word "and Users", at the end, shall be omitted;

(17) in regulation 35G,-

(i) in sub-regulation (1), after clause (g), the following new clause shall be inserted, namely: -

"(h) internal audit plan to assess the controls and system readiness of the platform. Implementation of the audit plan shall be under the oversight of audit committee of the board."; and

(ii) in sub-regulation (2), after the word "deceptive", the full-stop shall be omitted and the following words shall be inserted, namely: -

"and comply with the guidelines for advertisement as applicable on NBFCs engaged in digital lending;";

(18) in regulation 35I,-

(i) in sub-regulation (1), in clause (a), after sub-clause (ii), the following new sub-clauses shall be inserted, namely: -

"(iii) potential impact on loan servicing and portfolio management if the platform ceases to operate;";

"(iv) the nature of the investment, associated risks, and the platform's role in providing services;" and

"(v) that peer to peer lending is not an investment product with features like tenure linked assured minimum returns, liquidity options, etc.";

(ii) in sub-regulation (2), after clause (v), the following new clause shall be inserted, namely: -

"va. information on loan buy-back options offered to lenders, if any, and mechanism in case a lender opts to exit the P2P Lending Platform or a particular transaction;" and

(iii) after sub-regulation (2), the following new sub-regulation shall be inserted, namely: -

"(3) P2P service provider shall be required to obtain explicit declaration from the lender stating that he/she has understood all the risks associated with the lending transactions and that P2P platform does not assure return of principal/payment of interest. The declaration shall also state that there exists a likelihood of loss of entire principal in case of default by a borrower. The P2P platform shall not provide any assurance or guarantee for the recovery of loans.";

(19) in regulation 35K,-

(i) for sub-regulation (1), the following shall be substituted, namely: -

"(1) Fund transfer between the participants on the P2P Lending Platform shall be through trust or escrow accounts mechanisms as per specified terms and conditions of trust or escrow. Such accounts shall be maintained and operated by a licensed bank in Pakistan that is at least an 'A' rating from a credit rating agency. At least two trust or escrow accounts, one for funds received from lenders and disbursal, and the other for collections from borrowers, shall be maintained. All fund transfers shall be through bank accounts and cash transactions shall be prohibited.";

(ii) in sub-regulation (2), for the word "escrow", the word "trust or escrow" shall be substituted; and

(iii) after sub-regulation (3), the following sub-regulation shall be inserted, namely: -

"(4) Trust or escrow accounts shall be audited annually by the statutory auditor of the NBFC and same shall be submitted to Commission and uploaded on P2P Lending Platform";

(20) in regulation 35L,-

(i) in sub-regulation (1), in clause (iii), for the word "User's", wherever occurring, the word "participants" shall be substituted; and

(ii) after sub-regulation (2), the following new sub-regulations shall be inserted, namely: -

"(3) P2P Service Provider shall comply with the relevant requirements of information technology, cybersecurity and data protection as given in the schedule

XVIIB; and

(4) P2P service provider shall have the adequate winding down plan in place for the P2P platform and plan shall be disclosed to lenders before entering into the arrangement of business.";

(21) for regulation 35M, the following shall be substituted, namely: -

"**35M. Reporting Requirements**. - P2P Service Provider shall submit quarterly accounts to the Commission and periodical statements, reports, statistics and data in such forms, time and manner as may be specified by the Commission from time to time.";

(22) in regulation 67AC, sub-regulation (3), in clause (b), -

(i) in sub-clause (i), for the words "or 1/3 members, whichever is higher," the word "member" shall be substituted;

(ii) in sub clause (ii), -

(a) after the word "a", the words "BOD level" shall be omitted;

(b) after the word "representation", for the word "of", the words "from the board and" shall be substituted;

(c) after the words "Compliance Department; and", the word "and" shall be omitted; and

(d) after the words "BOD", the word "and" shall be inserted and the following new para shall be inserted, namely: -

"• Co-opted experts, possessing knowledge, advanced expertise, and work/business experience in emerging technologies and the digital domain, may also be included in the committee, if deemed appropriate."

(23) in schedule IX, in para "ASSESSMENT OF FITNESS AND PROPRIETY", -

(i) in clause (c) "Competency and Capability", in sub-clause (iii), after word "sector", the following new provisos shall be inserted namely: -

"Provided that chief executive officer of a lending NBFC offering services through digital mode should have a minimum experience of three years in a senior management position, preferably in the regulated financial services sector;

Provided further that such lending NBFC shall have at least one non-executive director with experience of seven to ten years preferably in the regulated

financial services sector";

(ii) in clause (d), "Conflict of interest", in sub-clause (v), after the word "any", for the word "entity", the words "NBFC or entity" shall be substituted;

(24) in schedule XIIA, -

(i) in clause (1), for the word "two", the word "one" shall be substituted;

(ii) in clause (2), after the word "similar", the words "form of " shall be inserted and after the word "business", the word "Pakistan" shall be omitted;

(iii) after clause (4), the following new clause shall be inserted, namely: -
"(4A), The chairman and the CEO shall not be the same person.";

(iv) for clause (5), the following shall be substituted, namely: -
"Lending NBFC except NBMFCs shall have at least one female director on their board.

Provided that, NBMFCs shall have at least two female directors on their board, one of whom shall be the independent director";

(25) after schedule XIIA, the following new schedule shall be inserted, namely: -

**"Schedule XIIAB**

**(Borrowers Fact Sheet for the lending NBFCs engaged in Digital Lending)**

**See Regulation 21(10)**

**1. For the consumer loans;**

**Personal Information;**

a) Name of the applicant
b) Fathers Name
c) Computerized National Identity Card Number (CNIC)
d) CNIC expiry date
e) Address (Residential/Business)
f) Contact Details (Personal/Business)
g) Email Address

**Reference Details (at least two):**

a) Name

b) Contact Details

c) CNIC Number

d) Address

**Financing request:**

a) Amount

b) Tenor

c) Product category (i.e BNPL, Nano lending, EWA, Education finance etc.

d) Purpose of the financing

**Existing credit exposure:**

a) Name of credit institution

b) Loan Amount

c) Outstanding Balance

d) Maturity Date

**2. For the business loans;**

**Business Information;**

a) Name of the Business:

b) Address:

c) Phone Number

d) CNIC# of owner/CEO

e) National Tax Number (if applicable)

f) Business Type:

(i) Manufacturing

(ii) Agricultural

(iii) Services

(iv) Commercial

(v) Any other

g) Registration Status;

(i) Sole proprietorship

(ii) Partnership

(iii) Single Member Company

(iv) Private/Public Company

**Management Information;**

a) Name

b) Address

c) Status (i.e Director/CEO/Sponsor)

d) Contact Number

**Financing request:**

a) Amount

b) Fund based/ non-fund based

c) Tenor

d) Purpose of the financing

**Existing credit exposure;**

a) Name of credit institution

b) Loan Amount

c) Outstanding Balance

d) Type of financing (i.e running financing, asset financing, operating/financial lease etc)";

(26) Schedule XVI, occurring second time, shall be renumbered as "Schedule XVIA" and thereafter, for the expression "Annexure to Schedule XVI", the expression "Annexure to Schedule XVIA" shall be substituted;

(27) in schedule XVIA, renumbered as aforesaid, -

(i) in clause (1), after sub-clause (a), the following new sub-clause shall be inserted, namely: -

"ab. Auditor certificate confirming the latest equity position of the Lending NBFC;";

(ii) in clause (1), sub-clause (d), after the words "identification of", the expression "Users" shall be substituted with the expression "participants";

(iii) in clause (1), in sub-clause (f), the expression "Rs.250,000" shall be substituted with expression "Rs. 500,000"; and

(iv) in clause (2), sub-clause (vi), for the words "Users", the word "participants" shall

be substituted; and

(28) after schedule XVII, the following new schedule shall be inserted, namely: -

**"Schedule XVIIA**

**Requirements of Information Technology, Cyber Security and Data Protection for P2P Service Provider**

**[See Regulation 35L(3)]**

**1.** P2P service provider 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: -**

(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;

**(b) 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;

**(c) 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;

**(d) 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.

**(e) 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.

**(f) 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.

**(g) 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.

**(h) 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.

**2.** P2P service provider 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.** P2P service provider may develop mobile Apps in-house, through outsourcing or by a combined approach. To manage mobile App development projects, P2P service provider 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 P2P service provider

**4.** P2P service provider shall ensure compliance with the requirements relating to the mobile App, as provided in Annexure-A to this Schedule;

**5.** P2P service provider not be stored on any cloud infrastructure outside the jurisdiction of Pakistan;

**6.** P2P service provider shall arrange at least once every three years from the date approval, IT audits of its IT infrastructure including the platform including but limited to web application/mobile application 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.

**7.** P2P service provider shall ensure compliance of all applicable laws in force in Pakistan related to cyber security, personal data protection, cloud usage and data privacy; and

**8.** P2P service provider 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.

## Annexure-A of Schedule XVIIA

### A. Architecture of Apps

(i). P2P service provider 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). P2P service provider 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). P2P service provider 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) P2P Service Providers 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). P2P service provider shall ensure that explicit customer consent in a convenient manner is obtained before allowing registration of Apps;

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

(ii). P2P service provider 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). P2P service provider 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). P2P service provider shall ensure that confidential data is deleted from caches and memory after it is used and/or uninstalled. Further, P2P service provider 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). P2P service provider 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). P2P service provider 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). P2P service provider 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). P2P service provider shall ensure that Apps have automatic user-logoff functionality after a configurable idle time-period not exceeding thirty minutes;

(ii). P2P service provider shall ensure that Apps have an easy to use and clearly visible logoff method;

(iii). P2P service provider 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). P2P service provider 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). P2P service provider shall implement necessary checks on the server-side to verify Apps integrity and to detect any manipulation.

(ii). P2P service provider shall ensure that installation of Apps is not allowed on rooted/jail broken devices;

(iii). P2P service provider 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, P2P Service Providers shall not allow any third party to debug the application during runtime.

**H. App Permissions**

(i). P2P service provider shall ensure to restrict data shared with other applications on the device through fine-grained permissions;

(ii). P2P service provider 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, P2P Service Providers 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). P2P service provider shall ensure that their Apps developers adhere to industry accepted secure coding practices and standards;

(ii). P2P service provider 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, P2P service provider shall only use necessary and secure services, protocols, components, and dependent software and hardware, including those provided by third parties.

(iii). P2P service provider shall document all required protocols, services, components, and dependent software and hardware that are necessary for any functionality of the application.

(iv). P2P service provider shall have knowledge of all off-the-shelf libraries/modules/components utilized in the development of Apps;

(v). P2P service provider 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). P2P service provider shall ensure that private key used for code signing is generated, securely stored and appropriately backed-up;

(vii). P2P service provider shall ensure that minification and source code obfuscation techniques are used in the Apps;

(viii). P2P service provider shall ensure to review application code prior to release to customers after any significant change, to identify any potential coding vulnerabilities;

(ix). P2P service provider shall verify that apps are not vulnerable to common coding vulnerabilities by performing manual or automated penetration testing.

**J. Input and Output Handling**

(i). P2P service provider shall ensure that any input coming from the client that is to be stored in databases is properly validated;

(ii). P2P service provider 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. P2P service provider 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). P2P service provider 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). P2P service provider 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). P2P service provider shall implement appropriate security safeguards to protect the logs from unauthorized modification or destruction;

(v). P2P service provider shall ensure that all the ecosystem logs are available for audits;

(vi). P2P service provider 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). P2P service provider 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). P2P service provider 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). P2P service provider 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, P2P service provider 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. P2P service provider 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 P2P service provider 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. P2P service provider shall ensure to perform a robust security screening and testing of the API between the P2P service provider 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 P2P Service Providers;

(ii). P2P service provider 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). P2P service provider 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). P2P service provider 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). P2P service provider 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.

---

[No. SY/SECP/8/13]

( Bilal Rasul )
Secretary to the Commission