1- Governance

Financial Institutions (FIs)[1] shall:

i. Formulate Digital Fraud Prevention Policy to protect their account holders and ensure effective communication of such policy.
ii. Promote a risk control culture through prudent and ethical practices as well as behaviors across all levels of the people, processes and technology components to ensure customers' protection against digital frauds.
iii. Establish and strengthen digital fraud risk management units under the supervision of senior management official with an effective management control and oversight of the Board or its designated committee.
iv. Allocate and provide necessary resources, systems and people, to build and update the capacity by making adequate investment in digital fraud risk management.
v. Ensure identification and implementation of digital fraud risk controls through compliance assurance and implement fraud control related KPIs.
vi. Ensure that the customer education and awareness by the FIs' management and operations gain special focus from top to bottom to combat frauds in digital banking services through cyber channels.

2- Management Control

FIs shall:

i. Design, review and continuously improve end-to-end processes of digital fraud risk management and customer complaint management in consultation with relevant stakeholders.
ii. Identify and implement digital fraud risk controls to continuously monitor, prevent, detect, respond and remediate incidents of fraud.
iii. Clearly inform their expectations, roles, responsibilities and liabilities to all internal and external participants of the processes for digital fraud risk management including third party vendors/service providers, Financial Market Infrastructures (FMIs) regarding fraud prevention including fraud detection, reporting, investigating and monitoring requirements.
iv. Enforce security mechanisms commensurate with the risks in the respective areas of digital banking and payments products and services (such as using Card, Browser, App, Voice or e-Commerce) through channels like (Internet or Mobile Banking etc.).
v. Ensure that the overall product and service design, development and operations shall strictly follow the core principles of information security i.e., confidentiality, availability and

[1] FIs include Banks and MFBs

integrity. Further, any of these principles shall not be neglected or violated at any stage or step of the product / service.

vi. Implement ISMS[2] using applicable standards of ISO27000 family on the service components.

vii. Conduct comprehensive information security reviews of new digital products and services and for any modification in their existing digital products and services including but not limited to people, complete process and technology.

viii. Ensure that the weaknesses and all critical/high and medium vulnerabilities identified from the information security reviews shall be rectified and controlled through validation before deployment to the production/operations and launch of products/services.

ix. Ensure that the applications, payment cards and channels used by the FIs for such services have to be PCI/DSS [3]and PCI/SSF [4]certified as applicable.

x. Conduct regular and spot fraud risk assessment(s) to ensure implementation of policies and processes governing initial and ongoing fraud risk management.

xi. Use internal and external sources of information to develop insight into the instances of fraud happening in financial sector both in Pakistan and other countries.

xii. Ensure effective mutual coordination by efficient mechanism of sharing required logs and exchange of information to trace illegitimate transfers, payments and withdrawals made through suspected accounts and wherever applicable use such authentic information to resolve customer claims and / or complete legal enforcement actions.

xiii. Maintain oversight of the fraud investigations through senior management periodic reporting.

3- Operational Controls

A. <u>Enablement of Digital Banking Channels [5]& Device Registration:</u>

i. FIs shall conduct NADRA biometric verification of customers (preferably digitally), with the exception for USSD channel, in the following cases:
   a. At the time of digital banking channels activation/sign–up;
   b. New device registration;
   c. Modification of customer email address and phone numbers.

Alternatively, for the following types of customers/ scenario, FIs shall implement a combination of at least two controls i.e. facial recognition, in-app live original identity document verification, in-app live picture verification, and call back verification shall be implemented:

   a. Non-resident customers;

[2] ISMS: Information Security Management System
[3] Payment Card Industry Data Security Standard
[4] Payment Card Industry Software Security Framework
[5] Digital Banking Channel: Mobile Banking, Internet banking, USSD Banking and payment Card (as applicable)

b. Customers with physical disabilities (like limbs disability, uneven texture/ erased / unclear fingerprints, etc.);
c. Customer's having temporary issue (e.g. wounded/ bandaged hands/ mehndi, etc.);
d. Foreign nationals;
e. Non-financial services.

However, where these alternate controls are difficult to implement, in-person verification shall be implemented.

ii. In case where, customer maintains multiple accounts with a single FI, customer's explicit consent for enabling each account(s) on digital channels shall be obtained.

iii. FIs shall ensure that the credential reset (such as change in user ID/password of mobile banking/internet banking channel of customers) is only performed using customers' registered device. Further, for credential reset, FIs shall implement One Time Password (OTP) auto-fetch or auto-fill functionality, with sender binding control[6] restricting manual entry of OTP. However, where the FIs face limitation(s) or other concerns (such as customer inconvenience) in implementation of aforementioned controls then Robo Call Back (RCB) or Call Back Confirmation (CBC) or in-app NADRA biometric verification must be implemented in order to authenticate genuine customers through a foolproof mechanism for ensuring non-repudiation by the customers.

iv. While implementing RCB confirmation, the FIs shall customize its implementation to mitigate the risk of social engineering frauds by adopting intelligent and randomized confirmation process (instead of employing predefined confirmation steps). In this regard, the RCB confirmation shall include: seeking negative confirmations, obtaining step-wise confirmations, etc. Upon failing the confirmation process, the call/ case should be routed to call center agents for manual confirmation.

v. Customer devices (such as computer, laptop, tablet or mobile etc.) shall be registered using device finger-printing / device binding[7] for authenticating customer access. The functionality of managing the devices by the customers in their internet banking/mobile application shall also be provided. The FIs shall work with Third Party Service Providers (TPSPs) to make available the device identification functionality within USSD channel.

vi. Any new device registered shall be notified to the customer immediately on its registered contact number and if available, on registered email address.

vii. FIs shall define a reasonable limit on number of accounts accessed per device, and implement additional authentication controls (i.e. CBC, obtaining and recording the justification for exceeding the limit along with customer verification) for devices exceeding the defined limit.

[6] Mobile App of the FI only uses/recognizes OTPs received from the FIs' SMS short code for auto-fetch or auto-fill

7 Device Finger-Printing / Device Binding: Using unique set of identification features such as Device ID, Universal Unique Identifier (UUID), Integrated Circuit Card Identifier (ICCID), International Mobile Equipment Identity (IMEI) Number or International Mobile Subscriber Identity (IMSI) Number.

viii. FIs shall apply a reasonable limit on the maximum number of registered devices. FIs shall implement a 2-hours cooling-off period before activation of mobile apps for newly registered customers. Further, cooling-off period shall also be introduced before implementation of requests for key account changes such as device, customer's mobile number, email ID, transaction limits, password reset etc. Customer may be intimated beforehand in this respect through SMS, as well as through alternate channels such as email.

ix. Registration/ sign up process for digital channels enablement shall not provide affirmation regarding existence of the customer account(s) with the FIs until completion of the process.

B. Transactional Control:

i. FIs shall employ transactional controls commensurate to the risks identified in the digital banking.

ii. FIs shall set reasonable default transaction limits on the digital channels and permit the customers to enhance or reduce these limits after due authentication. Further, the customers shall also be provided with the option to manage transaction limits for all digital channels.

iii. FIs shall define and enforce reasonable limits on the number of utility bill payments made to a utility company/ vendor through digital channel from a particular account (excluding bill payments by branchless banking agents). However, the said limit may be enhanced upon customer specific request.

iv. For transactions initiated using FIs accounts including branchless banking accounts/ wallets, from third party internet portal or mobile application, the FIs shall implement additional controls such as RCB/ CBC/verification through USSD /in-app verification. These requirements shall not apply to the subscription based services.

v. FIs shall ensure that data / information is encrypted in transit and at rest in all stages of transaction based on classification and sensitivity of data which shall inter alia include customers' Personally Identifiable Information (PII), payment card related data, etc.

x. For branchless banking accounts, FIs, upon receipt of a successful credit, shall allow cash out, on-line purchases or mobile top-up against the transferred funds after two (02) hours. During this period, funds will remain on "in-progress" status. Customer may be intimated beforehand in this respect through SMS, as well as through alternate channels such as email. However, for their trusted customers, beneficiary FI may allow cash withdrawal, online purchases or mobile top-up.

C. Post Incident Follow-up:

i. FIs shall realign their processes for fraud risk management and complaint management to ensure that the dispute against the fraudulent transactions are immediately (not more

than 30 minutes after receiving complaint from the customer), raised in Fraudulent Transaction Dispute Handling (FTDH) system.

ii. The beneficiary FIs shall temporarily hold the fraudulent proceeds received from the sender FIs where any supplementary/ secondary information in the FTDH dispute request is invalid. In all such cases where supplementary/ secondary information is invalid, the sender FIs shall rectify the supplementary information within reasonable time (not more than 30 minutes from the time FTDH dispute request is marked invalid).

iii. Beneficiary FIs, upon receipt of complaint in FTDH, shall immediately contact the account holder in whose account fraudulent funds are transferred and obtain the source of incoming funds and in case of unsatisfactory response the beneficiary FIs may generate suspicious transaction report (STR) against the beneficiary account.

iv. For digital frauds where the proceeds are routed to multiple FIs, each beneficiary FIs in the layering process, on receiving FTDH dispute request from the sender FIs, shall be responsible for raising FTDH dispute request against the next beneficiary FIs in the chain within reasonable time (not more than 30 minutes of acknowledging the dispute).

v. Beneficiary FIs, upon receipt of dispute in the FTDH shall immediately (not more than 30 minutes after receiving complaint from the customer) block withdrawal of disputed funds and suspend the digital channels to prevent further use of the said account for digital frauds. Subsequently, the relevant FIs shall complete the investigation within ten days of lodgment of dispute in FTDH and after establishing the fraud, reverse the funds within three days to the account of the victim.

vi. In case of e-Commerce transaction, FIs shall immediately report disputed fraudulent online transactions to respective domestic merchants either directly or through their acquiring institutions after being reported by the customers. The acquiring institution shall ensure that the information about the disputed transaction is conveyed to the merchant immediately with the request to block the shipment of physical goods. Further, the FIs shall also make all possible efforts for recovery of customers' funds.

vii. FIs shall identify the CNICs and accounts of the fraudsters or collusive beneficiaries (itself not victim(s)) established to be involved in fraudulent activity, after due investigation. The details of such fraudulent accountholders as well as of those who are used in routing fraud proceeds will be shared across the industry for enhanced monitoring.

viii. As a result of digital fraud investigations, where appropriate, FIs may approach Law Enforcement Agencies (LEAs) for necessary action.

ix. FIs shall use FTDH for raising disputes against all type of fraudulent transactions including those conducted using RAAST.

x. FIs shall continue the reporting of Digital Fraud under BC&CPD Circular Letter No. 03 of 2022.

D. <u>Monitoring Control:</u>

i. FIs shall ensure continuous monitoring of the services extended to the customer for which FIs shall implement an Enterprise Fraud Management (EFM) solution that should support detection, analysis and management of fraud across users, accounts, products, processes and channels.

ii. The scope of real-time fraud monitoring tools and alerts mechanism specified in the PSD Circular No. 09 of 2018 related to payment card systems shall be enhanced to include all digital products. Further, FIs shall implement fraud risk scenarios which shall be periodically reviewed, require additional authentication from the customers based on digital fraud risk score, and for taking timely actions such as suspending transactions/accounts, etc. For this purpose, FIs may use Intelligent Algorithm based Customer's Transaction Behavior Profiling techniques for detection of suspected transactions. Some fraud risk scenarios may include but not limited to:
    a. Change of device followed by credential reset request;
    b. Change of device followed by addition of number of beneficiaries and IBFT transactions;
    c. Addition of multiple beneficiaries followed by multiple debit transactions not in line with the historical pattern;
    d. Change of geographic region;
    e. Value, number and time of transactions;
    f. Deviation in mean time to carry out transactions;
    g. Transfer of funds to accounts, suspected to be involved in fraudulent transactions;
    h. Suspected IPs and geo locations;
    i. Multiple transactions in quick succession.

iii. FIs on an ongoing basis or at least quarterly, shall also identify and review devices (e.g. mobile phones, computers, tablets, etc.) used to digitally access significant number of accounts (especially victims' accounts, layering accounts and fund utilization accounts) and take necessary action against such devices including blocking access of digital services through the device. FIs shall also develop internal procedures for unblocking devices on case-to-case basis. Further, all devices found used in fraudulent transactions shall be immediately reported to PTA for necessary action, and shall be immediately blocked by the FIs.

iv. FIs shall assess the effectiveness of the controls by reviewing the number of digital banking frauds, and enhance control(s) or implement additional control(s) in case of increase in number of digital banking frauds

v. FIs shall ensure that their systems are capable of maintaining sufficient logs/information about digital channel activities such as device IDs, accounts, date and time of activity, transactions, mobile number, agent ID, agent location, device location, etc.

E. <u>Encryption and confidentiality of customer information:</u>

i. Throughout the service chain at all stages, the customer information should be stored or transmitted in hashed or encrypted as applicable form using non-obsolete cryptographic algorithms, such as AES 256 and SHA256 or the updated versions, duly vetted by subject matter experts.

ii. FIs shall design the process and application in such a way that the chances of disclosure of customer information - in whole or partially in a manner that makes it possible to be collated to reconstruct - are eliminated or minimized.

iii. FIs shall strictly ensure that the information so collected shall not appear or be disclosed in whole to any individual processing officer/staff/third party and shall appear in partially anonymized/tokenized/hashed/masked form as applicable, while rendering assisted banking services or reporting and management of banking service operations - to minimize its disclosure. Any information required to be displayed internally shall be strictly on Need-to-Know basis.

iv. FIs shall ensure that biometric information of customers should not be stored or transmitted in unencrypted form.

v. FIs shall ensure masking of critical information [8](e.g. PAN) during any stage of the end-to-end process of the service e.g. in the bank (account) statements/credit card statements or messages to the customers, unless specifically requested by the customer or vital for operations.

vi. The information of customers, individual or in bulk, shall never be in the personal possession or personal access[9] of the FIs' staff or transportable by the staff, third parties and any other service provider to prevent its possible misuse.

vii. FIs shall ensure to place sufficient controls and measures to safeguard the confidentiality of customer's PII under their outsourcing arrangements, and where such data is stored and processed outside the FIs software/ applications (i.e. in office productivity software/tools).

viii. FIs shall ensure equally effective process and procedural controls to protect confidentiality of the customers' data at their branches and ensure safe collection, use and disposal of customers' documents/data/records under a defined policy.

F. <u>Call Center</u>:

i. Authorized call center agents and branch staff shall be provided with the functionality to block individual as well as all digital channels of a customer with a single option, after obtaining consent of the customer.

[8] **Critical Information** includes account number, credit card number and any combination of person identifiable information which uniquely identify that person such as name and CNIC number.

[9] **Personnel access** include all types of access which is not provided officially to employee(s), whereas the official access should be provided based on Principle of Least Privilege (PoLP) access

ii. The requirement of BC&CPD Circular No. 03 of 2021, regarding call wait times of not more than one minute for card block request shall also apply to blocking request for all digital channels including branchless banking accounts/ wallets, mobile and internet banking channels, etc. Further, the FIs shall also provide self-service IVR based functionality for blocking digital channels through their call centers.

iii. FIs shall ensure that their officials conducting customer verification on the phone are vigilant. FIs may consider implementing technology based solutions to ensure authentication of the customers and spoofed call at the call centers and management of the associated risks.

iv. FIs shall not require the customers to provide verbally OTPs to their officers including the call center agents.

G. <u>Branchless Banking Agents:</u>

i. FIs shall analyze the digital frauds data, identify and investigate suspected branchless banking agents, and initiate action against the agents involved in digital frauds, including where appropriate approach/ cooperate with LEAs for taking action(s) against such agents. Further, FIs themselves shall physically inspect the suspected branchless banking agents, which have not been blacklisted.

ii. As advised in Framework for Branchless Banking Agent Acquisition and Management issued vide BPRD Circular No. 06 of 2016, background check of branchless banking agents is primary responsibility of the FIs. In this regard, FIs shall not rely on any evaluations conducted by their related or third parties without sufficient evidence. Moreover, FIs shall ensure capacity building of their agents through trainings/ seminars/ awareness sessions etc.

iii. FIs shall maintain sufficient oversight of the biometric verification devices provided to their agents. In this regard, FIs shall also review the biometric verification logs to identify and investigate abnormal instances such as multiple biometric verifications, at one agent, within short span of time.

iv. FIs shall maintain complete trail of their agent based banking transactions (identification of sender and/or beneficiary in every transaction). In the light of SBP's existing Branchless Banking Regulations, it is reiterated that:

   a. FIs shall keep all necessary record on transactions for at least ten years following completion of the transaction;

   b. FIs shall maintain sufficient transaction record that can facilitate reconstruction of individual transactions so as to provide, if required, evidence of prosecution of criminal activity;

   c. FIs shall keep record of all attempted transactions for at least ten years from the date of transaction.

H. Communication and Customer Education:

i. The customers should be provided option to select the languages primarily Urdu and English in which they want to receive the notifications.

ii. The messages (SMS and emails) should be composed of the context, substance and date and time logs along with contact information of the Bank in a clearly understandable format.

iii. In addition to the existing requirements of PSD Circular Letter No. 01 of 2019 regarding sending free of cost transaction alerts on SMS and email (where email IDs are available), the FIs shall also send instant (free of cost) alerts on: sign-in from a new device not already registered, password reset, failed login attempts and request for availing lending products. FIs shall prioritize these alerts and also arrange for sufficient capacity/bandwidth for instantly sending these alerts.

iv. FIs shall never communicate the balance available in the account, while sending transaction alerts,

v. FIs shall develop a strategy and program to improve customers' awareness about digital frauds and implement it through active campaigning including awareness regarding ongoing methods of digital frauds happening in the industry and preventive guidance to the consumers. In this regard, FIs shall utilize electronic, print and digital media effectively.

I. Other Operational Controls:

i. FIs shall conduct comprehensive investigations of the digital banking frauds and prepare formal investigation reports and engage with the customer to transparently present/explain bank's findings. The scope of the investigation shall be end to end (from victim to ultimate beneficiary) and at least include validation of customer assertions, potential of internal staff involvement, role of branchless banking agents (including those responsible for conducting biometric verification), review of PII access logs, gaps or weaknesses in FI's systems, applications and processes, etc. Further, FIs shall take action against the branchless banking agents involved in the digital frauds and staff delinquent in conducting proper KYC and CDD.

ii. FIs shall implement Data Loss Prevention Controls to prevent compromise of data including specially the customer data.

iii. FIs for convenience of their domestic customers travelling overseas and RDA accountholders may exempt certain digital channel controls on customers' request.

iv. FIs shall ensure that the OTPs used for authentication are of reasonable length with appropriate validity (i.e. time out).

4- Liability Framework

FI shall:

i. Offer transactional insurance to their customer at reasonable and competitive charges, the insurance should be activated upon explicit customer's consent or request.

ii. Be responsible for loss of any customer funds due to delay on their part in taking timely remedial and control measures such as delay in blocking digital channels, delay in raising dispute requests, etc. In this regard, the FIs shall compensate in whole the customers for such losses.

iii. Observe the following liability structure subsequent to a fraudulent transaction/social engineering scam:

   a. Complete liability to make good of all customer loss would lie with originating bank (sender FI) in case dispute is not lodged in FTDH within the stipulated time.

   b. Originating bank (sender FI) shall bear the complete liability in case affected customers were not able to lodge dispute complaint due to unavailability of complaint lodgment channel.

   c. Complete liability to make good of all customer loss would lie with beneficiary bank (receiving FI) in case funds are withdrawn while lien for the involved amount was not marked on the account within the stipulated time after receiving the dispute in FTDH.

   d. All beneficiary FI(s) shall share proportionate liability in case FTDH timelines are breached for marking lien on the suspected beneficiary account and funds are withdrawn.

   e. In case of ab initio false registration of the customer, the concerned FI shall be completely liable if the required controls related to registration were not in place or not properly implemented.

   f. FIs shall be liable to compensate the customers, in case where they are unable to establish that the transactions were executed through the customers' registered device.

   g. Complete liability to make good of all customer loss in case transaction alerts are not timely received by the customer, due to delay in generation of alerts.

iv. In case of a dispute in branchless banking account referred at para 3-B-vi, the liability will reside with the beneficiary bank.

v. In case where any of the stipulated controls are not implemented or failed, originating FIs shall be responsible to compensate the customers.

****