KARANDAAZ

PAKISTAN FINTECH ASSOCIATION

Pakistan Fintech Network

PROBLEM SPACE MANUAL

Digital Account Opening & Onboarding

To Register visit www.karandaaz.com.pk/hackathon

HACKADESIGN

Ideate, Prototype, Pitch

Design a winning account opening & onboarding experience

IDEATE INNOVATION

Contents

Background 2
About customer's digital onboarding framework 2
Digital Account Categories 3
The Problem Space 4
Why design Hackathon on account onboarding? 5
Customers Voice - Opportunities to Improve Experience 6
State Bank Circular on Digital Onboarding Framework 7
The Original Customers' Digital Onboarding Framework 8

Background

For the longest time customers had to visit the bank branches to open a bank account, moreover, it was nearly impossible for unemployed individuals, housewives, or students to open a bank account in their name without a valid source of income proof and other time-consuming documentation. Similarly, freelancers had to get services from third parties to easily receive their payments from their clients in other countries. The new Customer digital onboarding framework by State Bank for banks and MFBs is addressing all these barriers and providing greater flexibility and ease to access banking services digitally and remotely.

While few banks have designed a basic user journey for remote digital account opening, a lot more can be done to deliver an excellent onboarding experience to different segments. HACKADESIGN aims to utilize the imagination and creative streaks of the problem solvers to break the barriers of digital account opening & onboarding experience.

About customer's digital onboarding framework

The new customer digital onboarding framework by State Bank of Pakistan has introduced an extreme level of flexibility that will enable the previously neglected and underserved segments to easily open their accounts digitally and remotely, e.g.

- A housewife or an unemployed can now provide a self-declaration
- A student can provide a student ID
- A freelancer can provide a receipt of payment against the work or self-declaration

to fulfill the proof of income requirements and can open a local or foreign currency bank account through digital channels such as a website, app or kiosks, etc. As a result of collaboration between State Bank of Pakistan & NADRA, banks would be able to use NADRA APIs for App-based biometric verification, and a customer will not have to visit any branch for biometric verification at a later time.

Digital Account Categories

There are four main categories of digital accounts that are classified according to the monthly limits of deposits and withdrawals, currency, and the availability of proof of profession and source of funds.

Account Category	Currecny	Transaction Limits	Customer Information Documents
Asaan Digital Account	PKR	Balance Limit : 1 Million Withdrawl: 1 Million per month	Identity documents & other requirements • Identity document • Picture • Mobile sim pairing with CNIC Proof of Work/Profession and source of income funds • Self declaration • Undertaking
Asaan Digital Remittance Account	PKR	Balance Limit : 3 Million Withdrawl: 5 Lac daily Fund Transfer: 5 Lac daily Local Depost: 1 Million	
Freelancer Digital Account	PKR / Foreign	Balance Limit : No Limit Withdrawl: $5,000 monthly Depost: $5,000 monthly Withdrawal: PKR 5 Lac daily	
Digital Account	PKR / Foreign	Balance Limit : None Other Limits : None	In addition to customer information/identity document, relevant documents for profession & source of income will be required

For a housewife, who do not earn, perhaps the best suitable option can be an Asaan Digital account, that requires only a self-declaration. Similarly, a freelancer can have Freelancer digital account and can retain his earnings in the foreign currency account by providing a self-declaration or last payment receipt. Depending on the fund's limits, and the available proof, one can remotely open an account of his choice.

On the right is the indicative list of documents, any one of the document is sufficient to open an account.

Annexure - C

Indicative List of Documents to Assess the "Profession and Source of Income/Fund"

Self-employed/ Non-Salaried / Unemployed Persons		Employed/ Salaried Persons	
Proof of Business/ Work* (Any one of the following documents should suffice)	**Source of Income/ Funds* (Any one of the following documents should suffice)**	**Proof of Profession* (Any one of the following documents should suffice)**	**Source of Income/ Funds* (Any one of the following documents should suffice)**
• Business/ Proprietor Letter Head; or any other Proof of Self Employment (e.g. Lawyer/ Doctor/ Consultant/ Freelancers/ Grocery Store/ Medical Store/ Labor Work etc.), OR • Partnership/ Business Deed, OR • Self-employed or unemployed women – Self-declaration, OR • Valid Student ID Card/ Letter from Educational Institute, OR • Valid Work Permit showing Business/ Nature of Work etc., OR • Self-declaration (In case of ADA, ADRA and Freelancer Digital Account), OR • Any other Document evidencing the Profession	• Receipt of Payment against the Work, OR • Account Statement, OR • Particulars of Income/ Funds Providers (e.g. Family Members/ Guardian/ Stipends/ Social Benefits etc.), OR • Tax Statement/ Return/ Certificate, OR • Self-declaration (In case of ADA, ADRA and Freelancer Digital Account), OR • Any other Document evidencing Source of Income	• Valid Job/ Employee Card, OR • Employer/ Job Certificate, OR • Employment Contract, OR • Employer Letter, OR • Work Permit showing Profession/ Employment Details, OR • For Retired Persons, a copy of Retirement Letter/ Proof of Retirement, OR • Self-declaration (In case of ADA, ADRA and Freelancer Digital Account), OR • Any other Document evidencing the Profession	• Latest Salary Slip, OR • Salary Certificate, OR • Payment Slips/ Record, OR • Account Statement, OR • Tax Statement/ Return/ Certificate, OR • For Retired Persons, an evidence of Terminal Benefits/ Pension Book etc., OR • Self-declaration (In case of ADA, ADRA and Freelancer Digital Account), OR • Any other Document evidencing Source of Income
As an alternate to above, customer can provide the following as source of income/ funds:			
• Inheritance, OR • Agriculture income, OR • Investment in securities, bonds, shares, etc., OR • Investment in property, OR • Rental Income, OR • Interest income		Both Salaried/ Non-Salaried/ Self-employed/ unemployed may derive their income funds from these sources as well.	

***A single document showing "Proof of Profession and Source of Income/ Funds" may also suffice both** the requirements.

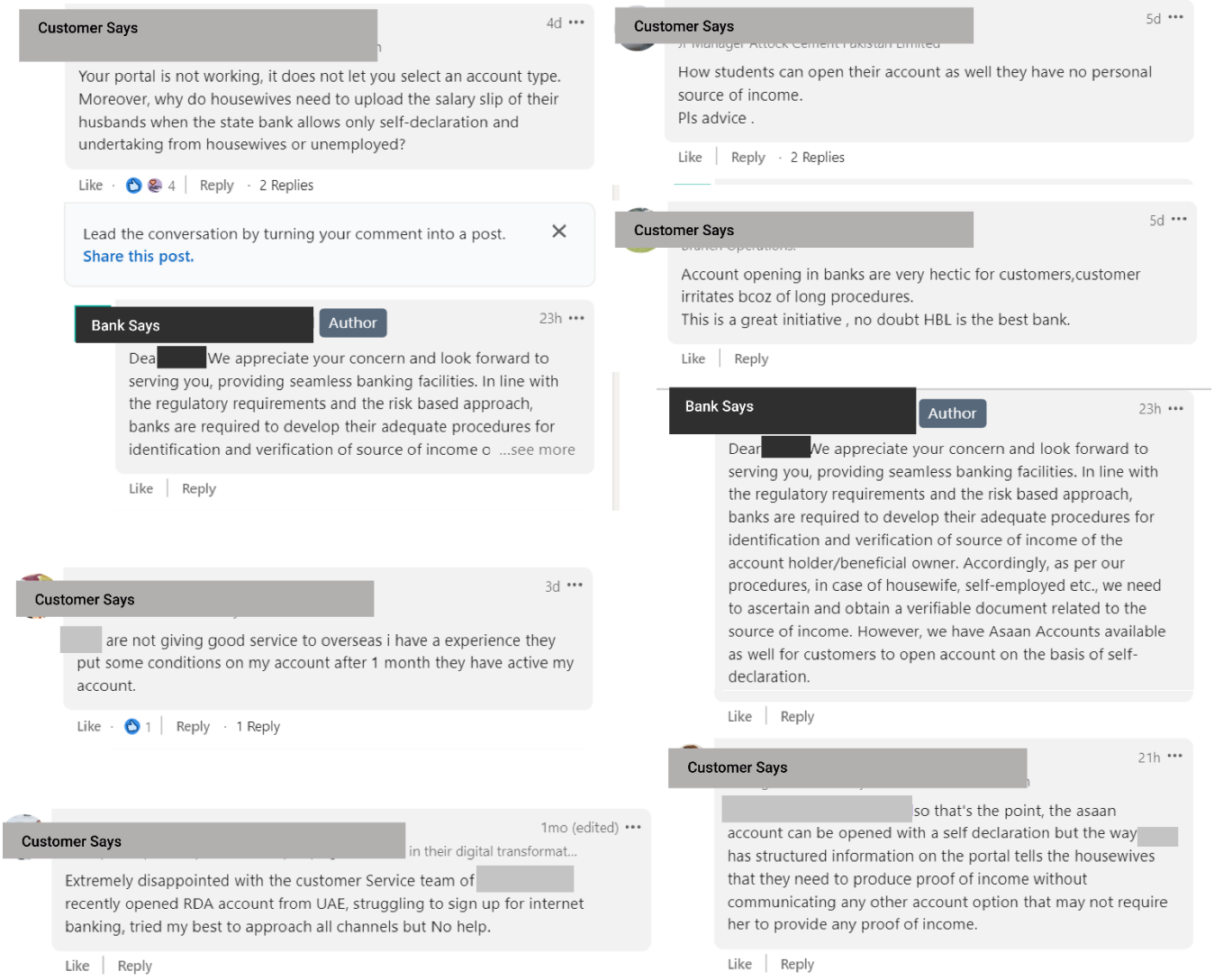
The Problem Space

Why design Hackathon on account onboarding?

Financial institutions need to have a seamless digital account opening experience. This means stripping out areas of frustration, such as manual ID checks and branch visits, and replacing them with modern efficient solutions and onboarding processes through digital identity verification, paperless document delivery, e-signatures, and a personalized experience centered around the user.

Opening an account should be an intuitive interaction like sending a text message	Customers are unwilling to wade through time-draining application processes	A large part of the population is non-English speakers and are intimidated by online experiences designed for digital-savvy and literate users
Application abandonments are not free of cost for the banks	An iron-clad account opening experience increases operational efficiency, reduces costs, and mitigate risks	Account opening experience influences customer choice of new banking partner
Customers expect a simple journey where they feel heard and understood	Globally, online conversions for bank account opening are extremely low due to a lack of awareness and poor online experience	A bank can lose a potential customer due to inefficient supporting processes for digital account opening

Customers Voice - Opportunities to Improve Experience



State Bank Circular on Digital Onboarding Framework

BPRD Circular No. 02 of 2021 **September 15, 2021**

The Presidents/Chief Executives,
All Banks/Microfinance Banks

Dear Sir/Madam,

Customers' Digital Onboarding Framework

1. With the rapid growth in adoption of digital banking channels, more so after the pandemic, the expectations of banking sector and their customers for contactless interactions have increased manifold. To enhance the coverage of digital onboarding process and bring efficiency and effectiveness in the account opening process using technology, State Bank of Pakistan (SBP) has decided to issue "Customers' Digital Onboarding Framework" for opening of bank accounts digitally by Resident Pakistanis.

2. This Framework sets minimum requirements and standards that banks/Microfinance Banks (MFBs) have to meet while designing and implementing a seamless and standardized digital onboarding experience for their customers. The Framework is envisaged to promote SBP's digitization efforts and it is expected that the banking industry would also welcome and support these efforts, resulting in increased convenience for the customers to fulfil their financial needs through swift and secure digital infrastructure in Pakistan. This initiative would also help in achieving SBP's financial inclusion objectives.

3. For "Customer Due Diligence", banks/MFBs shall utilize available technological and other resources for customer identification and verification, while complying with the enclosed Framework along with all applicable laws and regulations including but not limited to AML Act 2010, AML/CFT/CPF Regulations, Foreign Exchange Regulations and Enterprise Technology Governance & Risk Management Framework for Financial Institutions, as amended from time to time.

4. The banks/MFBs shall implement this Framework at the earliest but not later than December 31, 2021. In this regard, banks/MFBs are advised to submit their tangible plans along with concrete timelines for the implementation of this Framework within 30 working days from the issuance date of this Circular.

5. Please acknowledge receipt.

Enclosure: Customers' Digital Onboarding Framework

Customers' Digital Onboarding Framework

September 15, 2021

Banking Policy & Regulations Department

State Bank of Pakistan

Customers' Digital Onboarding Framework

September 15, 2021

Banking Policy & Regulations Department

State Bank of Pakistan

State Bank of Pakistan (SBP) has developed a "Customers' Digital Onboarding Framework" for banks/ MFBs which inter alia elaborates the basic parameters for opening of bank accounts for Resident Pakistanis through digital channels. Broad areas of this framework are as follows:

1	**Applicability and Scope**	The framework is applicable to: a. Banks and MFBs b. All types of local currency (Pak Rupee) Accounts c. Foreign Currency (FCY) Accounts as permissible under Foreign Exchange Regulations
2	**Eligible Customers**	a. Only natural persons b. Resident Pakistanis
3	**Onboarding Channels**	a. Banks/MFBs are permitted to onboard customers through the following secured digital channels: i. Website/portal; ii. Mobile application; iii. Digital kiosks; iv. Any other technological/digital medium as per bank's approved policy. b. Moreover, to facilitate customers, onboarding is also allowed through banks'/MFBs' employee(s) visiting the customer, on request.
4	**Account Categories**	**a. <u>Asaan Digital Account (ADA)</u>**: i. Currency: PKR ii. Maximum credit balance limit of PKR 1,000,000; iii. Monthly debit limit of PKR 1,000,000; iv. Self-declaration as required in **Annexure - C**. **b. <u>Asaan Digital Remittance Account (ADRA)</u>**: i. Currency: PKR ii. Maximum credit balance limit of PKR 3,000,000; iii. Cash withdrawal limit of PKR 500,000 per day; iv. Fund transfer limit of PKR 500,000 per day from ADRA to any other account; v. This account may also be fed through local credit to the extent of PKR 1,000,000 per month; vi. No commercial remittances shall be deposited in the account; vii. Self-declaration as required in **Annexure - C**. For accounts mentioned under category "a" and "b", the limits and specifications/ documents mentioned herein will be observed while complying with other procedural requirements provided in SBP's applicable instructions on the subject. **c. <u>Freelancer Digital Account:</u>** i. Currency: PKR/ FCY ii. Monthly limit of USD 5,000 or equivalent (debit & credit limits shall be applied separately); iii. Cash withdrawal limit of PKR 500,000/- or equivalent per day; iv. Self-declaration as required in **Annexure - C**.

		d. <u>Digital Account:</u> For opening all Digital Accounts, other than accounts mentioned under a, b & c above, specifications/ documents mentioned herein will be observed while complying with other applicable SBP instructions.
5	**Customer Information/ Documents**	Banks/MFBs shall ensure compliance with "Customer Due Diligence (CDD)" requirements stipulated in AML Act 2010 (Section 7A). For this purpose, banks/MFBs shall obtain: a. Customer information, as per **Annexure - A** for Asaan Digital Account/ Asaan Digital Remittance Account /Freelancer Digital Account and **Annexure - B** for Digital Account. b. Scanned copy or photo of valid original Computerized / Smart National Identity Card issued by National Database and Registration Authority (NADRA). In case of expired identity card, NADRA token/ receipt for renewal purposes may also be used. c. Live photo of the customer, captured through digital channels. d. Proof of business/work and source of income/funds of the customer **(as per Annexure – C** whereby <u>Self-declaration</u> for ADA, ADRA and Freelancers Account will suffice the purpose**)**. e. Signature (wet/digital/electronic) or any other authentication method as per bank's/MFB's approved policy/procedure.
6	**Customer Declarations/ Consents**	Banks/MFBs shall obtain: a. An undertaking from customer(s) to confirm beneficial ownership of funds/controlling rights, source of funds and other information uploaded/provided digitally during the opening of account. b. Foreign Account Tax Compliance Act (FATCA)/ Common Reporting Standard (CRS) Declaration digitally, wherever required. c. Digital/ online consent for account opening and use of information/ documents provided through the above process for due diligence and supervisory functions. d. Digital acceptance of Terms and Conditions (T&Cs) of the account and shall provide a copy of such T&Cs to the customers on their registered email address or any appropriate medium accessible to the customers.
7	**Customer Identity Verification and Screening**	Banks/MFBs shall: a. Verify customer's identity through NADRA Verisys or conduct Biometric Verification (BV) with liveness checks from NADRA at the time of account opening. However, in case of NADRA Verisys, BV of the customer from NADRA will be required within sixty (60) days from the date of account opening. In case, BV is not conducted within the stipulated time, banks/ MFBs shall impose debit block on such accounts after serving ten (10) days prior notice/ intimation to the customers. However, debit block shall be removed immediately after successful BV of the customer. b. Verify customer's any two particulars, which are not available on customer's identity card but provided by the customer during account opening process, from NADRA's information. c. Conduct mobile SIM ownership verification (CNIC – MSISDN Pairing Authentication) to ensure the pairing of customers' provided mobile number with their Computerized / Smart National Identity Card number.

		d. Collect and record geo-location coordinates of digital gadgets through which, customer has requested for digital onboarding. e. Carry out pre-screening of customers' particulars against lists of persons designated by the United Nations Security Council (UNSC) and proscribed under Anti-Terrorism Act, 1997. **Video KYC/Interview:** Banks/MFBs, as part of CDD, may conduct KYC of the customer through a recorded video call facility based on their internal risk assessment and compliance framework. For high-risk customers requiring Enhanced Due Diligence (EDD) in line with AML/CFT/CPF Regulations, video KYC/ interview is mandatory. The minimum parameters for conducting the video KYC should be covered in the Digital Onboarding Policy of bank/ MFB. Video KYC data shall be retained as per record retention requirements stipulated in relevant laws and regulations.
8	**Requirements for Minor Accounts**	a. In case of minor accounts, all requirements stipulated above shall be observed for the parent/ guardian as per the prescribed categories of bank account covered in this framework. b. Additionally, banks/MFBs shall also obtain: i. Scanned copy of original Juvenile Card / Form-B/ Child Registration Certificate (CRC) of the minor; ii. Live photo of the minor.
9	**Activation of Dormant/In-operative & Blocked Accounts**	a. Accounts marked dormant/in-operative as defined in AML/CFT/CPF Regulations shall be activated after customer's request along with date of issuance of CNIC/SNIC through registered medium (e.g. registered email address or mobile number). b. Accounts blocked due to expired CNIC/SNIC as required in AML/CFT/CPF Regulations shall be activated after obtaining date of issuance of CNIC/SNIC through registered medium (e.g. registered email address or mobile number). c. The banks/MFBs shall retain the NADRA Verisys for record keeping requirements.
10	**Customer Facilitation**	a. The maximum Turn-Around Time (TAT) for decision to open or decline an account shall be two (02) working days from the day of completion of all the requirements. A tracking number shall also be provided to the applicant for status updates. b. Banks/MFBs shall provide necessary trainings to their relevant staff in order to facilitate customer in digital onboarding. c. Banks/MFBs must ensure 24/7 availability of customer support services and are encouraged to deploy chatbox and chatbots for customer facilitation. d. Banks/MFBs are encouraged to make illustrative demos available on their onboarding channels i.e., banks/MFBs' website/ portal, mobile app etc. for the digital onboarding process to guide customers in English and local languages. e. Banks/MFBs shall continuously monitor feedback, queries and complaints received through their website, portals and platforms including social media and shall define TATs and escalations matrix in order to resolve queries and complaints.
11	**Other Operational Features**	a. Banks/MFBs, if satisfied with the CDD/EDD, shall allow opening of the account, in any branch as per the customers' choice. For selecting the branch, where possible, banks/MFBs may show the list of branches to the customers.

		b. Banks/MFBs may share customers' KYC related information, with any SBP/SECP regulated entity including Central Depository Company (CDC) of Pakistan and/or National Clearing Company of Pakistan Limited (NCCPL) in compliance with applicable laws, rules and regulations, after obtaining customer's consent.
12	**Security and Infrastructure Requirements**	a. Banks/MFBs shall put in place the necessary technological infrastructure and operational controls to ensure data integrity, privacy, security and confidentiality of customers' particulars/documents, collected and transmitted through their mobile applications/websites and other digital channels. Banks/MFBs, in this regard, shall ensure to adopt the minimum controls and procedures mentioned in **Annexure - D** of this framework. b. Banks/MFBs shall deploy necessary technical infrastructure and systems to comply with AML/CFT/CPF regime of the country. c. Banks/MFBs shall take appropriate security measures to eliminate the risks of impersonation of the customers or identity theft. d. Banks/MFBs may deploy adequate controls to ensure that customer is not a robot (e.g. CAPTCHA codes). e. Banks/MFBs are encouraged to utilize artificial intelligence for facial recognition, fraud detection and liveness detection to ensure integrity of the digital onboarding process as well as the information/ documents furnished by the customers. f. Banks/MFBs shall ensure that no data is stored on the devices, used to collect customer's information during the account opening process. The data must be kept in encrypted form and banks/MFBs shall ensure real time transfer of data from mobile devices/websites or other gadgets to banks'/MFBs' systems. g. Banks/MFBs shall conduct annual audit of their digital on-boarding arrangements.
13	**Compliance with AML/CFT Regime and other Applicable Laws and Regulations**	Banks/MFBs shall ensure effective compliance with AML Act, 2010 (particularly Sections 7, 7A – 7H), AML/CFT/CPF Regulations and all other applicable laws/ regulatory instructions including but not limited to Foreign Exchange Regulations, Outsourcing to Cloud Service Providers (CSPs) Policy and Enterprise Technology Governance & Risk Management Framework (ETGRMF).
14	**Policy for Digital Onboarding of Customers**	a. Based on the minimum set of parameters listed under this framework, banks/MFBs shall develop a comprehensive policy for digital onboarding of customers, which shall be duly approved. b. The policy, at minimum, shall include target segments, periodic assessment of existing technological infrastructure, parameters/ specifications for conducting the video KYC and overall risk assessment of digital onboarding. c. While implementing the approved policy, the strategy shall include key milestones along with their timelines including service provider selection, development of technological infrastructure, information system and security review of the digital onboarding infrastructure, user acceptance and penetration testing, marketing campaign, contingency plan in case of any disruptions and digital data governance policy etc.
15	**Pre-Launch Essentials**	a. To ensure readiness of systems and controls and address any gaps, banks/MFBs shall invariably conduct a pilot run of their digital onboarding solutions for at least two months. During pilot phase, following parameters shall be observed: i. Minimum 500 and maximum 2,000 accounts to be opened;

		ii. Only select group of customers to be included; iii. It shall be clearly communicated to the customers that the product is under pilot phase. b. Banks/MFBs, in addition to above, shall also develop their own parameters to assess the overall readiness of their technological infrastructure. c. Banks/MFBs shall inform SBP about their plan on pilot launch at least one week prior to its commencement. d. Prior to the commercial launch, Chief Compliance Officer and Chief Information Security Officer of banks/MFBs shall confirm in writing that the digital onboarding arrangements are compliant with all the applicable laws and regulations, especially related to AML/CFT/CPF and information security. e. Banks/MFBs will share results of pilot operations with SBP along with aforesaid confirmation, at least one week prior to the commencement of commercial operations, for information purposes.

Annexure - A

Customer Information – Asaan Digital Account (ADA)/ Asaan Digital Remittance Account (ADRA)/ Freelancer Digital Account

#	Field Name
1	Full Name as per Computerized/ Smart National Identity Card
2	Father/ Spouse Name as per Computerized/ Smart National Identity Card
3	Gender
4	Computerized/ Smart National Identity Card Number
5	Date of Issuance of Computerized/ Smart National Identity Card
6	Date of Birth
7	Place of Birth
8	Mother's Maiden Name
9	Contact Numbers: Mobile number (mandatory), Landline Number(optional)
10	Personal eMail Address (optional)
11	Current/ Mailing Address
12	Purpose of Account
13	Source of Income/Occupation as per Self-Declaration
14	Name(s) and Relationship(s) with Prospective Remitter(s) **(For ADRA only)**

Annexure - B

Customer Information – Digital Account

#	Field Name
1	Full Name as per Computerized/ Smart National Identity Card
2	Father/ Spouse name as per Computerized/ Smart National Identity Card
3	Gender
4	Computerized/ Smart National Identity Card Number
5	Date of Issuance of Computerized/ Smart National Identity Card
6	Date of Birth
7	Place of Birth
8	Mother's Maiden Name
9	Contact Numbers: Mobile number (mandatory), Landline Number(optional)
10	Personal eMail Address (optional)
11	Current/ Mailing Address
12	Permanent Address
13	Purpose of Account
14	Other Nationalities/ Residencies (list all)
15	Profession/ Source of Income/ Funds, Salary, Business, investment income or any other as mentioned in **Annexure – C**
16	Expected Monthly Turnover

Note: Any additional information, if required by the banks/MFBs, shall be specified in their approved policies/procedures, along with the purpose/justification of obtaining such information.

Annexure - C

Indicative List of Documents to Assess the "Profession and Source of Income/Fund"

Self-employed/ Non-Salaried / Unemployed Persons		**Employed/ Salaried Persons**	
Proof of Business/ Work* (Any one of the following documents should suffice)	**Source of Income/ Funds* (Any one of the following documents should suffice)**	**Proof of Profession* (Any one of the following documents should suffice)**	**Source of Income/ Funds* (Any one of the following documents should suffice)**
• Business/ Proprietor Letter Head; or any other Proof of Self Employment (e.g. Lawyer/ Doctor/ Consultant/ Freelancers/ Grocery Store/ Medical Store/ Labor Work etc.), OR • Partnership/ Business Deed, OR • Self-employed or unemployed women – Self-declaration, OR • Valid Student ID Card/ Letter from Educational Institute, OR • Valid Work Permit showing Business/ Nature of Work etc., OR • Self-declaration (In case of ADA, ADRA and Freelancer Digital Account), OR • Any other Document evidencing the Profession	• Receipt of Payment against the Work, OR • Account Statement, OR • Particulars of Income/ Funds Providers (e.g. Family Members/ Guardian/ Stipends/ Social Benefits etc.), OR • Tax Statement/ Return/ Certificate, OR • Self-declaration (In case of ADA, ADRA and Freelancer Digital Account), OR • Any other Document evidencing Source of Income	• Valid Job/ Employee Card, OR • Employer/ Job Certificate, OR • Employment Contract, OR • Employer Letter, OR • Work Permit showing Profession/ Employment Details, OR • For Retired Persons, a copy of Retirement Letter/ Proof of Retirement, OR • Self-declaration (In case of ADA, ADRA and Freelancer Digital Account), OR • Any other Document evidencing the Profession	• Latest Salary Slip, OR • Salary Certificate, OR • Payment Slips/ Record, OR • Account Statement, OR • Tax Statement/ Return/ Certificate, OR • For Retired Persons, an evidence of Terminal Benefits/ Pension Book etc., OR • Self-declaration (In case of ADA, ADRA and Freelancer Digital Account), OR • Any other Document evidencing Source of Income
As an alternate to above, customer can provide the following as source of income/ funds:			
• Inheritance, OR • Agriculture income, OR • Investment in securities, bonds, shares, etc., OR • Investment in property, OR • Rental Income, OR • Interest income		Both Salaried/ Non-Salaried/ Self-employed/ unemployed may derive their income funds from these sources as well.	

*A single document showing "Proof of Profession and Source of Income/ Funds" may also suffice both the requirements.

Annexure - D

Minimum Information Security and Technological Controls and Procedures

a) Banks/MFBs shall ensure that their portals/apps/other digital channels are safe and customer data/on-boarding process is secured from the threats posed by cyber criminals. Banks/MFBs information security team shall be involved in the design, development and deployment of digital portals/apps including performing:

   i. Application Security Controls
   ii. Architecture Review
   iii. Servers Hardening
   iv. Configuration Reviews
   v. Penetration and Vulnerability Testing
   vi. Security risk assessment during changes
   vii. Business Security Controls
   viii. Secure Code Review
   ix. Obfuscation of Source Code for Mobile Application
   x. Software Quality Assurance Procedures
   xi. Segregated Environment for Production and Testing
   xii. Network Security Controls such as anti-DDoS & DNS security
   xiii. High Availability and Load Balancing, if required
   xiv. Mobile Application shall not be installed on Rooted or Jail-broken Devices

b) Moreover, Banks/MFBs shall also be required to take measures to build preventive, detective and corrective technical security measures for their digital portals/apps to ensure confidentiality and privacy of customer data including but not limited to:

   i. 24/7 Security Operation Center(SOC) monitoring the security audit logs
   ii. Implementation of Web Application Firewall (WAF) on customer facing interfaces
   iii. Vulnerability Assessment and system hardening of digital onboarding portals/mobile apps
   iv. Penetration testing of the applications
   v. Implementation 2FA solution to verify the customer communication channel
   vi. Implementation of advance malware protection solution on Server(s) and user PCs of staff handling these requests
   vii. Implementation of DLP/Email protection controls to limit the movement of customer documents
   viii. Only authorized staff to process the account opening requests
   ix. Logging and Monitoring
   x. Application validation checks
   xi. Secure session management and encrypted client-server communication
   xii. Strong Password Enforcement
   xiii. Multiple layers of protection at network and application levels such as network traffic passing through IDS / IPS and multiple firewalls including parameter firewall.
   xiv. Cybersecurity & data privacy related awareness campaigns for customers and employees.

c) Further, Information Security teams/departments of banks/MFBs shall also review the security assessment reports (vulnerability assessment and penetration testing) of their technological

deployment of both front-end and back-end systems and customer interfaces and make sure that identified gaps, if any, are adequately addressed.

d) Information Security teams/departments of banks shall publish proper security guidelines, which should inform end-users about the threats, misconduct of using the application/portal and legal action, which may be taken by the banks/ MFBs. Further security guidelines should mention clauses that would show misuse of mobile application by end-users e.g. (installing of mobile application on rooted phone, installing of mobile application on antivirus free cell phones, installing of application on malicious emulators, reverse-engineering of mobile application etc.)

****