



Bangladesh Bank

Head Office
Motijheel, Dhaka-1000
Bangladesh
website: www.bb.org.bd

Banking Regulation & Policy Department-1

BRPD-1 Circular No.08

Date: 26 Falgun, 1432
11 March, 2026

Managing Director/Chief Executive Officer
All Scheduled Banks/Finance Companies/MFS Providers/PSPs/PSOs/other Payment Services

Dear Sir,

Guidelines on Electronic Know-Your-Customer (e-KYC)

Please refer to BFIU Circular No. 25; dated 08 January 2020 on the captioned subject.

2. In recent years, customer preferences for technology-based banking services and use of various digital payment instruments have increased significantly. While this trend has contributed to accelerating the country's economic development and financial inclusion, it has also raised concern for authenticity and fraudulent activities. Therefore, it is imperative to promote efficient and risk-mitigated banking and delivery channels to bring more people under formal banking and financial services. In this context, Bangladesh Bank has issued the updated **“Guidelines on Electronic Know-Your-Customer (e-KYC)”** for all Scheduled Banks, Finance Companies, Mobile Financial Service (MFS) Providers, Payment Service Providers (PSPs), Payment Systems Operators (PSOs), and other Payment Services.
3. Scheduled Banks are hereby instructed to submit updated information on the progress of implementation of the e-KYC Guidelines in the prescribed format (as per Annexure-A) to the Supervisory Data Management and Analytics Department, while Finance Companies shall submit the same to the Department of Financial Institutions and Market (DFIM) on a quarterly basis. However, in the case of MFS Providers, PSPs, PSOs, and other Payment Services, the reporting instructions issued by the Payment Systems Department-1 from time to time shall be followed accordingly.
4. This directive has been issued by Bangladesh Bank in exercise of its power conferred under Section 45 of the Bank Company Act, 1991; Section 41 of the Finance Companies Act, 2023; and Section 8 of the Payment and Settlement System Act, 2024.
5. This circular shall come into force from 01 September 2026 and any other circulars/instructions in this regard shall be replaced.

Yours faithfully,

(Gazi Md. Mahfuzul Islam)

Director (BRPD-1)

Phone: 9530252

Appendix-A
Data Format for Quarterly Statement of Implementing e-KYC

Name of the Bank/FC :

Name of the Quarter:

Date of Implementation of e-KYC	Number of Customer onboarded						Comments (If any)
	Simplified e-KYC		Regular e-KYC		Total		
	Current Quarter	Cumulative	Current Quarter	Cumulative	Current Quarter	Cumulative	
1	2	3	4	5	6(2+4)	7(3+5)	
Total							

Current Quarter refers to the reporting period; **Cumulative** refers to the sum of current quarter and all previous quarters

Guidelines on Electronic Know Your Customer (e-KYC)



**Banking Regulation and Policy Department -1
Bangladesh Bank**

March, 2026

ABBREVIATIONS

Acronyms	Full Forms
AI	Artificial Intelligence
AFI	Alliance for Financial Inclusion
API	Application Programming Interface
ATM	Automated Teller Machine
BB	Bangladesh Bank
BBO	Bangladesh Bank Order
BFIU	Bangladesh Financial Intelligence Unit
BIS	Bank for International Settlements
CDD	Customer Due Diligence
EDD	Enhanced Due Diligence
e-KYC	Electronic Know Your Customer
EC	Election Commission
FATF	Financial Action Task Force
FC	Finance Company
KYC	Know Your Customer
GoB	Government People's Republic of Bangladesh
G2P	Government to Persons
IFC	International Finance Corporation
IP	Influential Persons
MFS	Mobile Financial Services
ML/TF	Money Laundering & Terrorism Financing
NID	National Identification Database
NRB	Non-Resident Bangladeshi
OCR	Optical Character Recognition
PEP	Politically Exposed Person
PSP	Payment Service Provider
PSO	Payment System Operator
P2G	Persons to Government
SDD	Simplified Due Diligence
SIM	Subscriber Identity Module
PS	Payment Service (refer to MFS, PSP, PSO and other payment services together/separately)

Introduction

1.1 Background

At the backdrop of advancing digital customer onboarding, Bangladesh Bank (BB) formed an e-KYC Working Group in October 2016, led by Executive Director of Bangladesh Bank with representation from the NID Wing Election Commission (EC), the a2i Program of ICT Division, and six commercial banks. The group reviewed legal frameworks, examined international best practices, and conducted pilot programs using fingerprint and facial-recognition technologies across 19 institutions (16 banks, one FC, and two MFS providers), with evaluation support from the International Finance Corporation (IFC) during which 1,573 accounts were opened. The findings and recommendations on e-KYC/KYC were served as the basis for BFIU circular no. 25; dated: 08 January 2020. Later, e-KYC procedures were further reviewed under a memorandum of understanding (MoU) between IFC and BFIU, and the resulting inputs have been incorporated into this revised e-KYC Guidelines.

In Bangladesh, the EC holds citizens' (18 years and above) identity data with their biometrics (facial image and 10 fingerprint slaps), providing a high level of assurance and authenticity. Banks/FCs/PS providers may access this database to verify the authenticity of customer identity. Therefore, this e-KYC Guideline is based on the National Identity Card (NID) and the bio-metrics data associated with each NID. However, no citizen shall be deprived of the right to receive any service solely on the basis of not possessing a NID¹. In such cases, additional measures or regular KYC procedures may be applied to ensure compliance.

This Guideline highlights risk mitigation measures that banks, finance companies (FCs), mobile financial service (MFS) providers, payment services providers (PSPs), payment systems operators (PSOs) and other payment services should apply commensurate with the nature and level of risks identified. It also presents different customer due diligence (CDD) approaches which can be implemented to facilitate financial inclusion and remove obstacles related to customer identity verification, either through reliable and independent source of information or through simplified due diligence measures (SDD). Lower money laundering and terrorism financing (ML/TF) risk situations may permit the use of digital ID systems for simplified due diligence, while in higher ML/TF risk situations, banks/FCs/PS providers may adopt additional independent and reliable means to verify customers' identity.

This e-KYC Guideline set out instructions for banks, FCs, and PS providers to enable them to conduct customer due diligence digitally.

1.2 Regulatory Context for KYC

Bangladesh Bank, as the country's central bank, is entrusted with managing the monetary and credit system in a manner that supports national growth, development, and financial stability. Under the Bangladesh Bank Order (BBO), 1972, the Bank Company Act, 1991 and the Finance Company Act, 2023, and Payment and Settlement System Act, 2024 it is empowered to regulate and supervise banks, FCs, and PS providers and license their operations, and prescribe standards

¹ Section 12(2), National Identity Registration Act, 2023

for customer on-boarding. To safeguard the financial system, BB identifies six core risk areas—credit, asset-liability, foreign exchange, internal control and compliance, money laundering, and ICT risks—and issues macro-prudential and operational guidelines accordingly.

ML/TF is recognized as critical threats to financial integrity. The Money Laundering Prevention Act (MLPA), 2012 (Section 25) requires banks/FCs/PS providers to collect complete and accurate customer identification information at the time of establishing a business relationship. The Money Laundering Prevention Rules 2019 outline the framework for customer due diligence, with Rule 10 providing the legal basis for a risk-based approach, including simplified measures for low-risk customers and enhanced measures for high-risk categories.

Globally, regulators are moving toward risk-based and simplified KYC. The Alliance for Financial Inclusion (AFI) recommends removing rigid proof-of-address requirements, adopting outcome-based KYC standards, and reducing due-diligence burdens to enhance financial inclusion, particularly for women and marginalized groups. The Bank for International Settlements (BIS), in its *General Guide to Account Opening (2015)*, prescribes a minimum set of information—name, permanent address, nationality, unique ID number, and date/place of birth. The Financial Action Task Force (FATF) emphasizes risk-based KYC, simplified due diligence, and robust record-keeping. Although Bangladesh is not an FATF member, it aligns its regulatory framework with FATF recommendations.

1.3 Scope

This Guideline shall be known as the Electronic Know Your Customer (e-KYC) Guidelines which govern electronic customer onboarding, by identification and verification of customer identity, creation of a customer's digital KYC profile as well as risk grading of customers through digital means. The scope of this Guideline will be as follows:

- (a) This Guideline shall apply to natural persons with valid NID;
- (b) The requirements under this Guideline shall be based on the risk exposures of the customers of banks/FCs/PS providers. For example, for an assessed low-risk scenario, banks/FCs/PS providers shall be required to conduct simplified e-KYC which includes electronic customer on-boarding, verifying customer identity, and preserving customer profile digitally, whereas, banks/FCs/PS providers shall be required to conduct regular and enhanced e-KYC which includes electronic customer on-boarding, verifying customer identity, digitally preserving KYC and risk grading for a customer with a regular and higher risks scenario;
- (c) The e-KYC requirement of this Guideline is based on biometric verification; therefore, a client whose status is a legal person or legal arrangement is excluded from the e-KYC obligation. However, KYC and CDD norms for the legal person or legal arrangement shall be undertaken as per the provisions of the MLPA 2012, Anti-Terrorism Act (ATA), 2009, the MLP Rules, 2019, Anti-Terrorism (AT) Rules 2013; and instructions through circulars and guidelines issued by the BB time to time;
- (d) The customer's identity shall be verified electronically using a trusted, reliable, and independent source documents, data, or information, and e-KYC shall be completed immediately. If e-KYC onboarding attempt failed due to any technical reason, the traditional KYC procedure should be followed; and

- (e) Non-resident Bangladeshis (NRBs) can be onboarded through e-KYC if they have valid NID, and banks/FCs PS providers have the requisite system in place (through their app/web platform). Other information/documents shall be obtained from NRBs as instructed in the relevant circulars of Bangladesh Bank and BFIU.

1.4 Objectives

The key objective of promoting e-KYC is to simplify the onboarding process digitally by verifying customer identity through trusted and reliable means, thereby saving time and ensuring ease of access and convenience for both customer and service providers. In addition, e-KYC reduces institutional costs and fosters customer base compared to traditional methods. Therefore, the objectives of implementing e-KYC are to:

- a) Enhance and foster financial inclusion;
- b) Safeguard the financial sector against criminal abuse;
- c) Ensure the integrity and stability of the financial system;
- d) Manage ML/TF risks;
- e) Reduce costs associated with customer onboarding and CDD;
- f) Promote the adoption of fintech services;
- g) Foster innovation in financial products and services; and
- h) Support national macroeconomic stability and well-being.

2. Electronic Know Your Customer (e-KYC)

2.1 Definitions

- (a) “e-KYC Process” refers to a combination of paperless customer onboarding, promptly identifying and verifying customer identity, maintaining a KYC profile in a digital form, and determining customer risk grading through digital means.
- (b) “Simplified e-KYC” refers to an electronic customer onboarding process whereby customer identity is verified using a simplified digital KYC form in case of a proven lower-risk scenario with limited transactions prescribed in Section 2.3.1. Risk grading shall not be required while onboarding the customer. However, sanction screening shall be undertaken, and a periodic KYC review shall be conducted every five years.
- (c) “Regular e-KYC” refers to an electronic onboarding process applicable for customers who exceed limited transactions prescribed in Section 2.3.1. Under this process customer identity is verified electronically using a prescribed digital KYC form which must be filled in and stored. In addition, a risk grading exercise is required to be documented electronically, where the customer is rated as high risk or in some specific scenarios (for example, influential persons-IPs), enhanced customer due diligence (EDD)² shall be undertaken in accordance with the

² The EDD measures should include collection of additional information, monitoring of account activity and approval from Chief AML/CFT Compliance officer.

sample provided in section A2 of these Guidelines.

- (d) “Transaction” refers to any purchase, sale, loan, pledge, gift, transfer, delivery, or related arrangement, including but not limited to:
- The deposit, withdrawal, exchange, or transfer of funds in any currency, whether conducted in cash, by cheque, payment order, other instruments, or through electronic or other non-physical means;
 - The use of a safe deposit box or any similar secure storage facility;
 - The establishment of any fiduciary relationship;
 - Any payment made or received, wholly or partially, in fulfillment of a contractual or other legal obligation; or
 - The formation or creation of a legal person or legal arrangement.
- (e) “Suspicious transaction” means such transactions which deviate from usual transactions and/or transaction potentially involve money laundering, funding suspected to be linked, or to be used for terrorism, terrorist acts, or by a terrorist, terrorist organization, or those who finance or are attempting to finance terrorism.
- (f) “Customer” means any person who engages in, or seeks to engage in, a financial transaction or activity with an institution and includes a person on whose behalf such transaction or activity is conducted.³
- (g) “Customer Due Diligence (CDD)” means identifying and verifying the customer and the beneficial owner.
- (h) “Face-matching” refers to a biometric-based model of customer onboarding where customer facial biometrics will be used as a main identifier of a person’s identity along with the NID number.
- (i) “Fingerprint matching” refers to another biometric-based model of customer onboarding where the customer fingerprint data stored within the NID will be used as a main identifier of a person’s identity along with the NID number.
- (j) “Periodic Review and Updation” means steps taken to ensure that documents, data, or information collected under the CDD process are kept up-to-date and relevant by reviewing existing records.
- (k) “Influential Persons (IPs)” refers to individuals who are or have been entrusted domestically with prominent public functions, for example head of state or of government, senior politicians, senior government officials, judicial or military officials, senior executives of state owned corporations, important political party officials.

2.2 Process

The traditional KYC process requires the KYC form to be filled out and then photo ID and customer’s signature along with required documents are collected. However, e-KYC is a digital

³ The payment service providers shall follow the definition provided in the Payment and Settlement System Act, 2024.

process where banks/FCs/PS providers can open a customer account by filling up the digital form, taking photographs on the spot, and authenticating the customer's identification data (ID No., biometric information, address proof) instantaneously. Such biometric information or digital signatures or electronic signatures may be used for transaction authentication as well. The customer onboarding process may undertake via the following means:

- (a) Assisted Customer Onboarding:** Where a bank/FC/PS provider or its nominated agent or third-party visits the customer or the customer visits the bank/FC/PS provider or its nominated agent or third party's premises and opens an account with the direct assistance of the bank/FC/MFS provider or its nominated agent or the third party; and
- (b) Self-Check-in:** Where the customers can onboard on their own by using a kiosk, smartphone, or personal computer. Self-check-in shall be allowed only for the face-matching model as described in Section 3.3.

2.3 Applicability

e-KYC shall only be applicable to natural persons who have valid NID. Natural persons without NID and a legal entity or arrangement have to follow the regular KYC norms as prescribed by the BB from time to time. Therefore, 'simplified' and 'regular' e-KYC norms shall be applicable to banks, FCs, and PS providers licensed by the BB. Applicability will be determined by the thresholds and risk levels specified in this Guideline, which may be amended from time to time by the BB. The banks/FCs/PS providers shall conduct paper-based customer onboarding and simplified or regular KYC and CDD measures if any customer is unable to onboard with this e-KYC mechanism.

2.3.1. Products under Simplified e-KYC

The simplified e-KYC covers the following financial services, which may be revised by the BB based on identified risks and consultation with relevant stakeholders from time to time:

(a) Payment Services Products

The products and services offered by the following payment service providers:

- Mobile Financial Services (MFS) Providers
- Payment Service Providers (PSPs)
- Payment Systems Operators (PSOs)
- Other Payment Services licensed under the Payment and Settlement Systems Act, 2024

The transaction limits applicable to products and services offered by the PS providers above shall be determined and notified by the BB from time to time.

(b) Financial Inclusion Products

- Subsidy and allowances paid by the GoB under its safety net programs (Government to Person);
- All receipt by the GoB (Person to Government);
- Any other No-Frills accounts.

(c) Agent Banking Products

- Existing agent banking products within the transaction limits set by the BB from time to time through circulars.

(d) Banking Products

The Limited Transactions Account is designed for underprivileged customers. Considering the associated risk factors, this account shall be subject to the following transaction ceilings and turnover limits:

(i) Deposit and Withdrawal Limit for Simplified e-KYC

Deposit Limit (in BDT)		
Type of Transaction	Single Transaction Amount	Monthly Total Amount
Cash	100,000	300,000
Transfers	250,000	500,000
Foreign Remittance	No limit	
G2P	No limit	
Withdrawal Limit (in BDT)		
Cash/ATM	100,000	300,000
Transfers	250,000	500,000
Electronic Payments	100,000	300,000
Foreign Remittance	No limit	
G2P	No limit	

(ii) Other Limit for Simplified e-KYC

FDR/Other Scheme Account	Amount that deemed to be safe to banks
--------------------------	--

(e) Finance Companies' Products

- Any type of FC products not exceeding BDT 10,00,000;

2.3.2 Products Under Regular e-KYC

The scope of regular e-KYC covers the following:

(a) Agent Banking Accounts

- When agent banking customer performed transactions with the branch as a regular customer and exceed the prescribed limit mentioned in Section 2.3.1(c);

(b) Banking Products

- Other banking products excluding the banking products mentioned Section 2.3.1(d)

(c) Finance Companies' Products

- Any type of FC products exceeding BDT 10,00,000;

(d) PS Providers' Products

- Transaction limit for PS providers will be set by the BB

3. Customer Onboarding-Simplified e-KYC

3.1 Customer Onboarding Models

Banks, FCs and PS providers shall conduct customer onboarding in accordance with this Guideline using national identification documents, information stored within a specific NID and bio-metric verification, either fingerprint or face matching⁴. The customer onboarding should include self-check-in, assisted check-in with service providers/agents, and other relevant approved means as required. If a customer fails to complete the onboard at any phase due to a technical error, the traditional paper-based KYC process must be made available to the customer.

Electronic customer onboarding involves multiple activities. An efficient onboarding process starts with clients' identity information and can be segmented into the following steps:

- (i) Data capture and generation;
- (ii) Identity verification;
- (iii) Sanction and other screening;
- (iv) Account opening;
- (v) Customer profiling (e-KYC Profile); and
- (vi) Customer risk grading (as applicable).

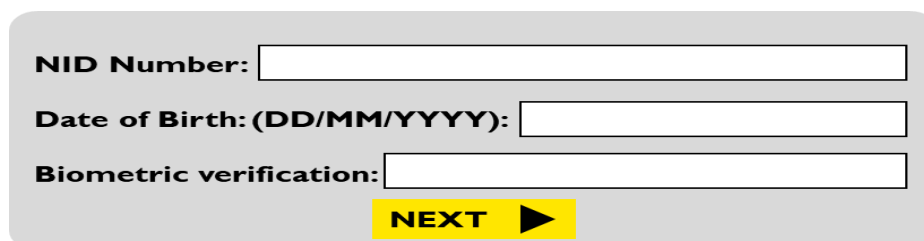
Any of the following two biometric-based models of customer onboarding can be used:

- (a) Customer onboarding by using fingerprint matching; or
- (b) Customer onboarding by facial recognition.

3.2 Customer Onboarding by Using Fingerprint

With this method customer fingerprints will be used as the main identifier of a person's identity. The minimum generic approach to be followed under this model shall be as follows:

a. First Step



NID Number:

Date of Birth: (DD/MM/YYYY):

Biometric verification:

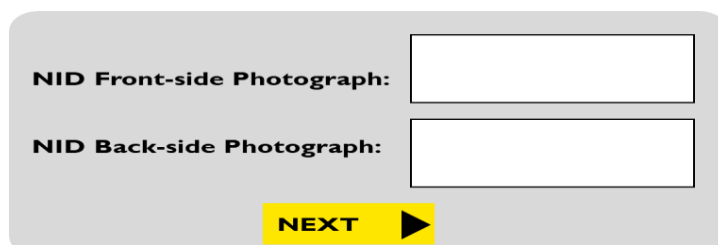
NEXT ►

In this step, a customer approaches to a bank/FC/PS provider or its agent or a bank/FC/PS provider or its agent approaches a customer for account opening process using e-KYC. The bank/FC/PS provider or its agent inserts the NID number and date of birth (DOB) into the specified template, collects the fingerprint of the customer, and then presses the Next button to match information with the EC database. The EC database holds data for all 10 fingers, however,

⁴ The financial institutions are free to choose any model based on their preparation and infrastructure.

for e-KYC purposes, matching one finger should suffice (the customer may use any preferred finger). A maximum of 10 (ten) fingerprint attempts is allowed per session. Two sessions are the maximum limit for a day. If the fingerprint matching fails in the sessions, the customer can re-try after 24 hours. If fingerprint verification fails in 03 (three) sessions, the bank/FC/PS provider must offer the customer face recognition. Once the bank/FC/PS provider or its agent presses the Next button the information of NID number, DOB, and fingerprint data will be matched with the NID database, if the data is matched, then the next template will appear.

b. Second Step⁵



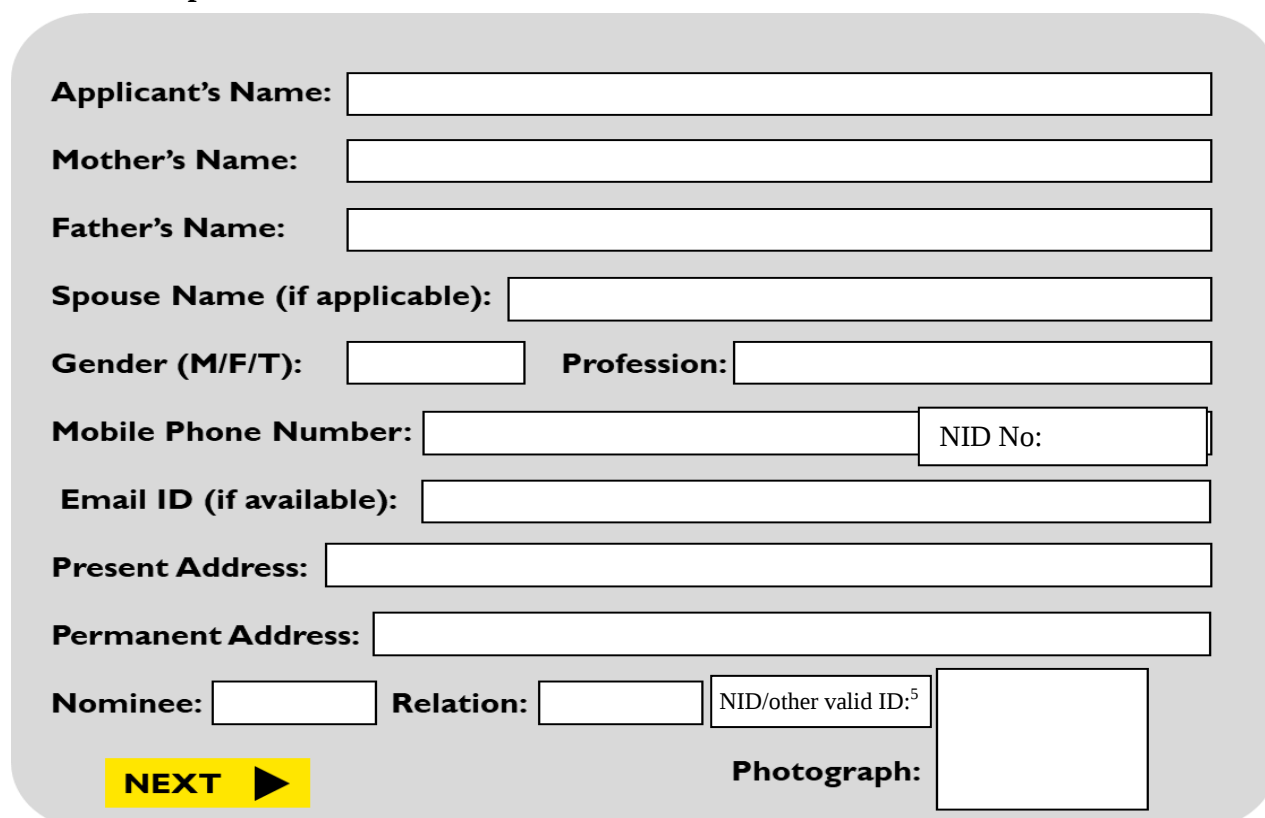
NID Front-side Photograph:

NID Back-side Photograph:

NEXT 

In step two, the banks/FCs/PS providers shall scan the front side of the NID, followed by the back side. Optical character recognition (OCR) should be used to capture the NID data.

c. Third Step



Applicant's Name:

Mother's Name:

Father's Name:

Spouse Name (if applicable):

Gender (M/F/T): **Profession:**

Mobile Phone Number: **NID No:**

Email ID (if available):

Present Address:

Permanent Address:

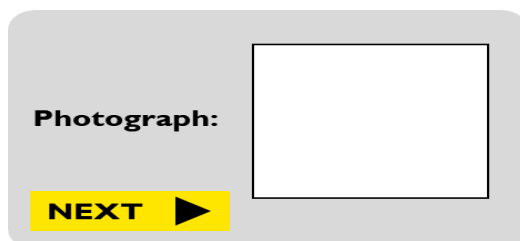
Nominee: **Relation:** **NID/other valid ID:⁵**

NEXT  **Photograph:**

⁵ The template given here is for the minimum required information. The financial institutions may add a few more fields where necessary, financial institutions may add additional fields for the additional nominee(s) and/ or where additional guardian information is required for the minor account.

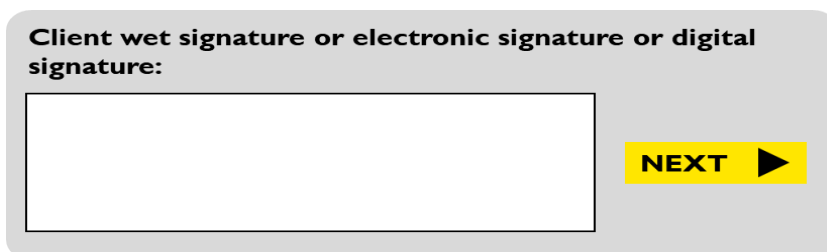
In this step, all necessary information will be fetched up in the digital format and additional input shall be punched to fulfill the whole template. The NID data should be captured in both Bangla⁶ and English. The nominee's name, date of birth, NID or other valid ID, relation to the customer, and photo can be entered by the bank/FC/PS provider's agent. The phone number or email ID (if available) should be mandatory for account opening notifications. Alternatively, banks/FCs/PS provider's agent may input the information manually after consulting the customer. On completion of personal information, banks/FCs/PS providers or their agent will press the Next option.

d. Fourth Step



In step four, banks/FCs/PS providers or their agents or clients will capture or upload the customer's live photograph, then press the Next option.

d. Fifth Step⁷



In step five, the customer's signature-either electronic (signature using devices), digital, or image of wet signature collected through verified channels shall be preserved for future reference.⁸ A digital signature or a Personal Identification Number (PIN) may be generated and used if the customer is unable to provide a wet signature. However, the use of digital signature or PIN is only allowed for low-risk accounts whereas wet or electronic signatures must be provided for high-risk accounts.

e. Sixth Step

In step six, after all processes are completed, the system will generate a notification that the account opening is in progress. After completion of the necessary sanction checks and other screenings, an account opening confirmation notification should be sent to the customer.

⁶ If OCR failed to capture Bangla names, it can be edited.

⁷ Where necessary, the financial institutions may collect physical signatures at a later stage and preserve them for further future use.

⁸ BRPD Circular Letter No.16; dated: 11 March 2021.

Account Opening Notification

.....

.....

.....

The simplified customer onboarding process will be completed once the customer receives notification from banks/FCs/PS providers. The notification should include the account name and number, the customer's branch (if applicable), type and customer's identification number. The notification shall be sent via registered mobile number (SIM) and email ID (if available). In case of a failed e-KYC, a failure notification shall be sent. At any point in the relationship, considering the risk exposure, banks/FCs/PS providers may ask for additional information from the customer following their approved policies and preserve it in the customer's digital KYC profile. If the customer does not receive any notification due to technical reasons, they should contact the help desk to report the problem. The customer care number should be visible on the bank/FC/PS provider's website/app.

For joint customers (more than one) onboarding, a same process should be followed. All fields mentioned in this Guideline are the minimum requirements, however, banks/FCs/PS provider may add additional fields as necessary according to their approved policies.

3.2.1 Required Technology

Electronic customer onboarding and the e-KYC process require a technology platform. Therefore, the following technology and instruments may be employed at a minimum, to complete the process:

- a. Software/App/Program compatible with the above process;
- b. Internet connection;
- c. Online connection to the NID verification server⁹;
- d. Fingerprint capturing devices;
- e. Electronic signature capturing devices (where necessary) etc.

3.2.2 Sanction and Other Screening

The full-fledged account procedures will be completed by completion of sanction checks and other necessary screening which includes as follows:

- a. UNSCRs screening;
- b. Adverse media screening (where necessary); and
- c. Internal or external exit list (where necessary).

⁹ Refers to the NID database either held by the NID Wing of the Election Commission and/or any other Government-vetted Authority for identity verification.

3.2.3 Audit Trail of Customer's KYC Process

To maintain an audit trail, a bank/FC/PS provider is required to preserve digital KYC profile and relevant logbook, even for low-risk or financial inclusion products, which should include the following:

- a. Customer details (name, contact, address) with photograph;
- b. Customer ID image (both sides);
- c. Customer signature (where necessary); and
- d. Customer risk review process;

The bank/FC/PS provider should maintain a digital log of all successful client onboarding, matching parameters, etc. for further work and audit trail. All data must be retained digitally for further internal and external audit purposes. At a minimum, the sample e-KYC profile should confirm to A1.

3.2.4 Matching parameters

As the electronic onboarding requires matching the customer's ID stored data with the NID database, the following elements or information are required to be matched as follows:

Particulars	Parameter¹⁰
Applicant's Name	Yes
Date of Birth	Yes
Fingerprint	Yes
NID number	Yes
Fathers' Name (If Available)	Yes
Mothers' Name (If Available)	Yes

3.2.5. Security Measures

The bank/FC/PS provider may use additional security measures in the customer onboarding process which must include two/multi-factor authentication (2FA/MFA) and/or checking the registered phone number (SIM)/email through one-time PIN code and any other measures deemed necessary. Additionally, the security and confidentiality of data recorded and preserved under this e-KYC must be ensure by the bank/FC/PS provider. The bank/FC/PS provider shall preserve customer data on locally hosted servers or private cloud servers and ensure necessary data protection and security measures as prescribed by BB and GoB.

3.3 Customer Onboarding by Using Face-Matching

The bank/FC/PS provider may alternatively adopt customer onboarding using a face-matching model where customer facial recognition will be used as a main identifier of a person's identity along with the NID number and date of birth. The following steps are required for the onboarding of a customer by using face matching model:

¹⁰ Where a spouse's name is recorded in lieu of the father's or mother's name, such entry shall be accorded the same matching parameter as that of the father or mother.

a. First Step¹¹

The interface for the first step of the e-KYC process. It features a light gray rounded rectangle containing two white rectangular input fields. The top field is labeled "NID Front-side Photograph:" and the bottom field is labeled "NID Back-side Photograph:". Below these fields is a yellow button with the text "NEXT" and a black right-pointing triangle.

In this step, a customer approaches a bank/FC/PS provider or its agent or a bank/FC/PS provider or its agent approaches a customer or customer engages in self-check-in for account opening process using e-KYC procedures. The front side of the customer's NID shall be captured, followed by the back side. Optical character recognition (OCR) shall be used to extract the NID data both in Bangla and English. All extracted NID data shall be stored in the backend system in appropriate textual format.

b. Second Step¹²

The interface for the second step of the e-KYC process. It features a light gray rounded rectangle containing a single white rectangular input field. To the left of the field is the label "Customer's Photograph:". Below the field is a yellow button with the text "NEXT" and a black right-pointing triangle.

In step two, banks/FCs/PS providers or their agents or customers shall capture an appropriate photograph of the customer's face using a high-resolution camera or webcam. While capturing the photograph, the agent or the customer shall take face only and ensure that the image is clearly visible. After the photograph is captured, it shall be matched against the customer's photograph stored in the EC server. A maximum of 10 (ten) tries are permitted in a single session. Two sessions are the maximum limit for a day within 24 hours. The bank/FC/PS provider shall allow maximum 03 (three) sessions for a customer onboarding. If the face matching fails, fingerprint verification or paperbacked KYC options shall be offered as an alternative onboarding option. In the case of self-check-in, the customer is required to capture a live selfie with proper lighting and camera frame¹³.

For further clarification regarding photo capture, refer to Annexure-3.

¹¹ The system should be capable enough to capture front page of NID first, followed by back page.

¹² There should be a mechanism that system only captured real persons' picture only.

¹³ There should be a mechanism that the system only captures real persons' pictures only.

c. Third Step¹⁴

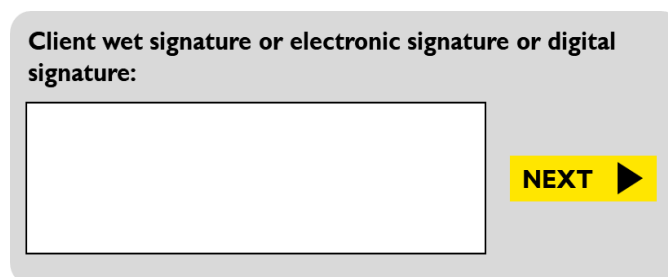
Applicant's Name:			
Mother's Name:			
Father's Name:			
Spouse Name (if applicable):			
Gender (M/F/T):		Profession:	
Mobile Phone Number:		NID No:	
Email ID (if available):			
Present Address:			
Permanent Address:			
Nominee:		Relation:	
		NID/Other Valid ID ¹⁵	
NEXT 		Photograph:	

In step three, all necessary information shall be extracted up from the NID through OCR in the above digital format. Additional inputs such as the nominee's name, relationship with the customer, and the nominee's photo shall be inserted by the bank/FC/PS provider's agent or by the customer to complete the whole template. Alternatively, banks/FCs/PS providers' agent may enter all of the information manually after consulting the customer. The registered phone number (SIM) or email (if available) shall be mandatory for account opening notifications.

¹⁴ This template given here is the minimum information. The financial institutions may add a few more fields where necessary. Where necessary, reporting entities may add additional fields for the additional nominee(s) and/ or where additional guardian information is required for the minor account.

¹⁵ NID mandatory for adult nominee; incase of minor nominee birth certificate can be used. In both cases, IDs to be preserved but verification is not mandatory.

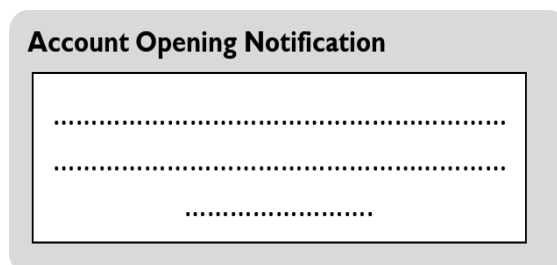
d. Fourth Step¹⁶

A screenshot of a digital interface for the fourth step of customer onboarding. It features a light gray background. At the top, the text "Client wet signature or electronic signature or digital signature:" is displayed in a bold, black font. Below this text is a large, empty white rectangular box for the signature. To the right of the box is a yellow button with the word "NEXT" in black capital letters and a black right-pointing triangle icon.

In step four, the customer's signature-either electronic (signature using devices), digital, or image of wet signature collected through verified channels shall be preserved for future reference. A digital signature or a Personal Identification Number (PIN) may be generated and used if the customer is unable to provide a wet signature. However, the use of digital signature or PIN is only allowed for low-risk accounts whereas wet or electronic signatures must be provided for high-risk accounts.

e. Fifth Step

In step five, after all processes are completed, the system will generate a notification that the account opening is in progress. After completion of the necessary sanction checks and other screenings, an account opening confirmation notification should be sent to the customer.

A screenshot of a digital interface for the fifth step of customer onboarding. It features a light gray background. At the top, the text "Account Opening Notification" is displayed in a bold, black font. Below this text is a large white rectangular box containing three horizontal dotted lines, indicating a space for a notification message.

The simplified customer onboarding process will be completed once the customer receives notification from banks/FCs/PS providers. The notification should include the account name and number, the customer's branch (if applicable), type and customer's identification number. The notification shall be sent via registered mobile number (SIM) and email ID (if available). In case of a failed e-KYC, a failure notification shall be sent. At any point in the relationship, considering the risk exposure, banks/FCs/PS providers may ask for additional information from the customer following their approved policies and preserve it in the customer's digital KYC profile. If the customer does not receive any notification due to technical reasons, they should contact the help desk to report the problem. The customer care number should be visible on the bank/FC/PS provider's website/app.

For joint customers (more than one) onboarding, a same process should be followed. All fields mentioned in this Guideline are the minimum requirements, however, banks/FCs/PS provider may add additional fields as necessary according to their approved policies.

¹⁶ Where necessary, the reporting entity may collect a physical signature at a later stage and preserve it digitally for further future use.

3.3.1 Required Technology

The same technologies mentioned in Section 3.2.1 shall be required that are capable enough to complete the procedure. In addition, smartphone or desktop computer with a high-resolution webcam shall be required to capture photograph for face matching.

3.3.2 Sanctions and Other Screening

The account procedure shall complete the same sanctions checks and other screening as mentioned in Section 3.2.2.

3.3.3 Audit Trail of Customer Profile

The same audit trail shall be maintained by the bank/FC/PS provider as mentioned for fingerprint matching method in Section 3.2.3.

3.3.4 Matching Parameters

The same matching parameters shall be maintained by the bank/FC/PS provider as mentioned in Section 3.2.4. The only exception is that face instead of fingerprint shall be matched.

3.3.5 Security Measures

The same security measures shall be maintained by the bank/FC/PS provider as mentioned in Section 3.2.5.

4. Customer Onboarding- Regular e-KYC

Banks/FCs/PS providers are encouraged to use electronic onboarding and e-KYC procedures for all financial products and services which do not fall under proven low-risk or limited risks categories. This means electronic onboarding and e-KYC procedures are also applicable for any sort of financial product. Both the technology-based models i.e., fingerprints and facial recognition technologies are applicable for regular onboarding and managing e-KYC. Similarly, biometric authentication technologies, i.e., fingerprint and facial recognition must be used for regular onboarding. Such onboarding process is applicable only for a natural person with a valid NID.

Initially, the regular e-KYC onboarding process is similar to simplified e-KYC, however, it requires the collection of additional information and applicable CDD. The reporting entities must create digital customer KYC profiles and perform risk grading as a part of the process. This means similar step-by-step¹⁷ procedures have to be followed both models as discussed above to complete the regular e-KYC procedures.

Therefore, regular e-KYC includes the following elements:

- a. A digital template containing more information than simplified e-KYC;
- b. A more stringent KYC profile of the customer;

¹⁷ All steps mentioned in this Guideline are generic; banks/FCs/MFS providers/PSPs/PSOs may reorganize this step-by-step process where necessary.

- c. Screening of customers in addition to the UN Sanctions (for example IPs, Beneficial Owner, Adverse Media, Internal External list checking, etc.);
- d. Risk grading exercise; and
- e. Ongoing monitoring

The minimum digital information template required for regular e-KYC shall be as follows:

Applicant's Name:			
Mother's Name:			
Father's Name:			
Spouse Name:			
Gender (M/F/T):		Date of Birth:	
Profession:		Monthly income:	
		Sources of Fund:	
Mobile Phone Number:		NID	
Present Address:		Nationality:	
Permanent Address:			
Nominee :		Date of Birth:	
		Relation:	
Photograph:		NID/Other Valid ID	
NB: i. If the applicant is minor then they should proceed with traditional methods of account opening; ii. Incorporate 'add' the following field if the nominee is 'Minor' iii. Name of minor nominee iv. Name of Guardian v. Address vi. Relation vii. NID of Guardian viii. Photograph of Guardian			

The customer onboarding process and instructions as discussed above for the simplified measures will be similar to regular e-KYC. After opening an account, the bank/FC/PS provider may collect additional information and a customer wet signature to create a full digital profile of the client.

4.1 Required Technology

The same technologies that are mentioned in Section 3.2.1 and Section 3.3.1 shall apply to regular e-KYC.

4.2 Sanctions and Other Screening

The screening mechanism for regular e-KYC is quite stringent compared to the simplified e-KYC as mentioned in Section 3.2.2 and Section 3.3.2. The full-fledged account procedures will be completed by completion of following additional sanctions and other necessary screening:

- a. IPs Screening;
- b. Identification of beneficial ownership (if any);
- c. Risk grading of the customer;
- d. CDD template; and
- e. EDD template (if applicable).

4.3 Audit Trail of Customer Profile

To maintain an audit trail, a bank/FC/PS provider is required to preserve a digital KYC profile and relevant log book or data in more stringent means than that of simplified e-KYC as mentioned in Section 3.2.3 and Section 3.3.3. They shall include the following additional information:

- a. Risk grading of the customer;
- b. CDD template; and
- c. EDD template (if applicable).

The bank/FC/PS provider should maintain a digital log for all successful e-KYC onboarding processes for further work and audit trail. All technical data must be preserved and stored digitally for audit purposes. The sample e-KYC profile, at minimum, look as per format provided in A2. For customers whose risk-grading has change from low-risk to high-risk, banks/FCs/PS providers shall follow the relevant circulars/instructions issued by BFIU.

4.4 Matching Parameters

The matching parameters mentioned for simplified e-KYC in Section 3.2.4 and 3.3.4 shall also apply to regular e-KYC.

4.5 Security Measures

In addition to the security measures mentioned for the simplified e-KYC in Section 3.2.5 and Section 3.3.5, following instructions shall be followed to ensure enhanced protection of the stored data:

- (i) The e-KYC system should use HTTPS for communication.
- (ii) “HTTP” should not be allowed and should be forced to redirect to HTTPS.

- (iii) The e-KYC system application and external APIs should only be accessible via authorization using standard authorization methods such as login credentials, bearer token, and JWT token.¹⁸

5. Other Relevant Issues

5.1 Record Keeping

The bank/FC/PS provider shall maintain all sorts of digital KYC data and log as per the Payment and Settlement Systems Act 2024. The digital data shall contain customer onboarding, customer identity verification, KYC profile, risk grading exercise, transaction-related data and their analysis, all sorts of correspondence with the customer, data collected later for CDD purposes, and all other relevant files.

The authorized maker (customer in case of self-check-in, and the Bank/FC/PS provider's agent conducting e-KYC) and checker in the e-KYC system can access e-KYC data stored in a bank/FC/PS provider. For system management purposes, the system administration team and the system auditor can access the stored e-KYC data through an authorized channel.

Digital footprint and the log should contain but not be limited to information collected during clients' identity verifications. Other relevant information related to the screening measures is also required to be preserved. The bank/FC/PS provider also may collect other complementary data (such as geo-location, IP addresses, etc.) which could also support ongoing due diligence.

5.2 Reliance on Third Parties

Banks/FCs/PS providers may rely on third-party technology providers either fully or partially to implement the e-KYC, however, the ultimate responsibility remains with the banks/FCs/PS providers. The third-party technology provider shall conduct the following CDD:

- (i) Customer identification and verification of data from independent and reliable sources;
- (ii) Identification and understanding of beneficial owner(s); and
- (iii) Determination of the purpose and intended nature of the business along with relevant digital CDD measures.

The bank/FC/PS provider shall ensure the reliability and authenticity of all data collected. The following conditions shall apply while engaging with any third party:

- Immediately obtain the necessary information concerning the customer's identity as mentioned in (i)–(iii) above.
- Take adequate steps to ensure that the third party will make available copies of identity evidence or other appropriate forms of access to the data or digital log as mentioned (i)–(iii) in the above without delay.

¹⁸ A JSON Web Token (JWT) is a compact, secure way to transmit information between two parties (like a client and a server) as a digitally signed token. It is basically a string that contains some encoded data and a signature to ensure that the data hasn't been tampered with

- The activities of the third party shall be regulated under this e-KYC guideline and shall be monitored by banks/FCs/PS providers.
- The third party shall ensure customer and financial institutions' data protection according to the IT security policy of the GoB and regulations of BB.
- Both the third party and the bank/FC/PS provider shall ensure that data collected from customer shall not be transmitted or transferred outside Bangladesh without prior approval of BB. In such case, BRPD Circular No.2; dated 19/01/2015 shall apply.

5.3 Risk Assessment

The bank/FC/PS provider shall conduct a risk assessment of the new technology-based electronic KYC mechanism to identify potential vulnerability and avenue for misuse and shall put in place appropriate measures to mitigate such risks in accordance with circulars and guidance issued by BB. In addition, banks/FCs/PS providers shall conduct a customer risk assessment as mentioned in Appendix-2 (A3 for banks, A4 for FCs and A5 for MFS providers; A6 for business and professional activity risk assessment of banks/FCs/PS providers) of this Guideline.

5.4 Transformation of Existing Clients CDD

The bank/FC/PS provider may transform their existing clients' CDD-related documents into digital form following the procedures mentioned in this Guideline where applicable.

5.5 Periodic Review and Updation of e-KYC

Banks/FCs/PS providers shall adopt a risk-based approach for periodic review and updation of KYC. However, periodic review shall be carried out at least once in every year for high-risk customers and once in every 05 (five) years for low-risk customers from the date of opening of the account/last KYC updation. Policy in this regard shall be documented as part of the banks/FCs/PS providers' internal KYC policy duly approved by the relevant authority.

No change in KYC information: In case of no change in the KYC information, bank/FC/PS provider shall record 'No Change' in KYC information template.

Address change: In case of a change in customer's address, a self-declaration of the new address shall be obtained from the customer through the customer's email, or customer's mobile phone number (SIM) registered with the bank/FC/PS provider, or ATMs, or digital channels (such as online banking/internet banking, mobile applications), or letter, etc. The declared address shall be verified through positive confirmation within two months, by means such as address verification letter, contact point verification, deliverables, etc. The declaration form shall collect the customer's personal details, i.e. name, NID number, and contact number. Address verification may be done by providing the last utility bill at the customer's new address or rental contract or, any other means deemed satisfactory by banks/FCs/PS providers.

For customers whose risk grading goes up due to a change in income source: If a change in customer's income lead to increase in risk grading, from low-risk to high-risk, bank/FC/PS provider shall undertake EDD in accordance with their approved policies.

Annexure-1
e-KYC Profile - Simplified and Regular

A1. Sample Output of the Simplified e-KYC¹⁹

Photo (Customer)	Photo (Other)
Applicant's Name:	
Mother's Name:	
Father's Name:	
Spouse Name:	
Date of Birth:	Gender (M/F/T):
Profession:	NID No:
Mobile Phone Number:	Present Address:
Permanent Address:	
Nominee:	Relation:
	Photograph:
	Specimen:
NID/Other valid ID no of Nominee	
signature/digital signature (where necessary)	
Front side of NID	Back side of NID
1. Has UNSCRs check been done? (Yes) (No)	
2. Has a review of the customer profile been done (existing customer)? if so, date of review	
3. What is the average range of customer (Inward and Outward) transactions (over 6/12 months)?	
4. Any other relevant field may be added here	

¹⁹ 'Photo Others' shall include the photograph of nominee(s), beneficial owner(s), joint account holder(s), minor(s) or their guardian(s) as applicable.

A2. Sample Output of Regular e-KYC

Photo (Customer)	Photo (Other)						
Applicant's Name:							
Account number:	Unique account number:						
Mother's Name:							
Father's Name:							
Spouse Name:							
Date of Birth:	Gender (M/F/T):						
Profession:	Monthly income: Sources of Fund:						
Mobile Phone Number:	Nationality: Present Address:						
Permanent Address:	NID No:						
TIN (if any):							
Nominee:	Relation: Photograph:						
Front side of NID	Back side of NID						
NID/Other valid ID no. of Nominee							
Specimen signature							
1.	Has the UNSCRs check been done? (Yes) (No)						
2.	Has risk grading been done? If the assessed risk is high then conduct EDD as per the BFIU circular.						
	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <th style="width: 50%;">Risk Type</th> <th style="width: 50%;">Overall Score</th> </tr> <tr> <td>Regular (< 15)</td> <td></td> </tr> <tr> <td>High (≥ 15)</td> <td></td> </tr> </table>	Risk Type	Overall Score	Regular (< 15)		High (≥ 15)	
Risk Type	Overall Score						
Regular (< 15)							
High (≥ 15)							
3.	Is the customer IPs? If the client is IPs with higher risk, then conduct EDD as per the BFIU circular.						
4.	Is there any adverse media news against the customer? If any then conduct EDD.						
5.	Has the source of und verified/justified? (Yes) (No)						
6.	Has the beneficial ownership been checked? If there is any beneficial owner found, then conduct CDD on the beneficial owner. If the beneficial owner is PEPs, then conduct EDD.						
7.	Are any other documents obtained ?						
8.	Nominee details						
9.	Has the review of the customer profile been done (existing customer)? if so, date of review						
10.	What are the average range and usual patterns of customer transactions (over 6/12 months)?						
11.	Any other relevant field may be added here						

Annexure-2

A3. Customer Risk Grading Form for Banks

1. <u>Type of On-boarding</u>	Score
Branch/Relationship Manager	2
Direct Sales Agent	2
Walk-in	3
Internet/Self check-in/Other non-Face to Face	2
2. <u>Geographic Risks:</u>	Score
Client is--	
Resident Bangladeshi	1
Non-resident Bangladeshi	3
Foreign Citizen	3
For Foreigners-	
Risk classification of country of origin	
Does client's country of citizenship feature in FATF/EU/OFAC/UN Black List/Grey List?	
No	0
Yes	5
3. <u>Type of Customer:</u>	Score
Is the client a PEP/Chief or High Official of an International Organization, as per BFIU Circular?	
No	0
Yes	5
Is the client's family/close associates related to PEP/Chief or High Official of International Organization?	
No	0
Yes	5
Is the client an IP? or is his family/close associates related to IP?	
No	1
Yes (based on assessed risk)	5

4. <u>Product and Channel Risk:</u>	Score
Type of Product	
Savings account	1
Current account	4
FDR (without having Saving/Current account)	3
Deposit Scheme upto 12 lac	1
Deposit Scheme above 12 lac	3
Forex account	5
S.N.D.	3
R.F.C.D.	5
5. <u>Business and Activity Risk</u>	Score
(a) Business	
Please pick the applicable option from A6 and put the relevant score in the next column	...
(b) Profession	
Please pick the applicable option from A6 and put the relevant score in the next column	...
6. <u>Transactional Risks:</u>	Score
How much is the client's Average Yearly Transactions Worth?	
<BDT 1 million	1
From BDT 1 million to 5 million	2
From BDT 5 million to 50 million (5 crores)	3
More than BDT 50 million (5 crores)	5
7. <u>Transparency Risk</u>	Score
The client has provided a credible source of funds	
No	5
Yes	1

A4. Customer Risk Grading Form for FCs

1. <u>Type of On-boarding</u>	Score
Branch/Relationship Manager	2
Direct Sales Agent	2
Walk-in	3
Internet/Self check-in/Other non-Face to Face	2
2. <u>Geographic Risks:</u>	Score
Client is--	
Resident Bangladeshi	1
Non-resident Bangladeshi	3
Foreign Citizen	3
For Foreigners-	
Risk classification of country of origin	
Does client's country of citizenship feature in FATF/EU/OFAC/UN Black List/Grey List?	
No	0
Yes	5
3. <u>Type of Customer:</u>	Score
Is the client a PEP/Chief or High Official of an International Organization, as per BFIU Circular?	
No	0
Yes	5
Is the client's family/close associates related to PEP/Chief or High Official of International Organization?	
No	0
Yes	5
Is the client an IP? or is his family/close associates related to IP?	
No	1
Yes (based on assessed risk)	5

4. <u>Product and Channel Risk:</u>	Score
Type of Product	
Corporate Loan/Lease	5
Consumer/SME Loan/Lease	3
CMSME Loan/Lease	4
Equity Participation	5
Guarantee Issuance	2
TDR	3
Deposit Scheme <1 Million	1
Deposit Scheme ≥1 Million	3
5. <u>Business and Activity Risk</u>	Score
(a) Business	
Please pick the applicable option from A6 and put the relevant score in the next column	...
(b) Profession	
Please pick the applicable option from A6 and put the relevant score in the next column	...
6. <u>Transactional Risks:</u>	Score
How much is the client's Average Yearly Transactions Worth?	
<BDT 1 million	1
From BDT 1 million to 5 million	2
From BDT 5 million to 50 million (5 crores)	3
More than BDT 50 million (5 crores)	5
7. <u>Transparency Risk</u>	Score
The client has provided a credible source of funds	
No	5
Yes	1

A5. Customer Risk Grading Form for Payment Service Providers

1. <u>Type of On-boarding</u>	Score
Self check-in	1
From Agent	2
From Customer Service Point	2
Bank a/c tagged with Wallet	1
2. <u>Geographic Risks:</u>	Score
Client is--	
Resident Bangladeshi	1
Non-resident Bangladeshi	3
Foreign Citizen	3
For Foreigners-	
Risk classification of country of origin	
Does client's country of citizenship feature in FATF/EU/OFAC/UN Black List/Grey List?	
No	0
Yes	5
3. <u>Type of Customer:</u>	Score
Is the client a PEP/Chief or High Official of an International Organization, as per BFIU Circular?	
No	0
Yes	5
Is the client's family/close associates related to PEP/Chief or High Official of International Organization?	
No	0
Yes	5
Is the client an IP? or is his family/close associates related to IP?	
No	1
Yes (based on assessed risk)	5

4. <u>Business and Activity Risk</u>	Score
(a) Business	
Please pick the applicable option from A4 and put the relevant score in the next column	...
(b) Profession	
Please pick the applicable option from A4 and put the relevant score in the next column	...
5. <u>Transactional Risks:</u>	Score
How much is the client's Average Yearly Inward Transactions Worth?	
<BDT 1 lac	1
From BDT 1 lac to 1 million	2
More than BDT 1 million	3
6. <u>Transparency Risk</u>	Score
The client has provided a credible source of funds	
No	3
Yes	1

A6. Assessing Business and Professional Activity Risk (for A3, A4 and A5 item no.5)

Client Business	Score	Client Profession	Score
<i>Jeweler/ Gold/ Valuable Metals Business</i>	5	<i>Pilot/ Flight Attendant</i>	5
<i>Money Changer/ Courier Service/ Mobile Banking Agent</i>	5	<i>Trustee</i>	5
<i>Real Estate Developer/Agent</i>	5	<i>Professional (Journalist, Lawyer, Doctor, Engineer, Chartered Accountant, etc.)</i>	4
<i>Promoter/ Contractor of Construction Projects</i>	5	<i>Director (Private/ Public Limited Company)</i>	4
<i>Art and Antiquities Dealer</i>	5	<i>High official of a Multinational Company (MNC)</i>	4
<i>Restaurant/ Bar/ Night Club/ Parlor/ Hotel</i>	5	<i>Homemaker</i>	4
<i>Export/ Import</i>	5	<i>Information Technology (IT) sector employee</i>	4
<i>Manpower export</i>	5	<i>Athlete/ Media Celebrity/ Producer/ Director</i>	4
<i>Firearms</i>	5	<i>Freelance Software Developer</i>	4
<i>RMG/ Garments Accessories/ Buying House</i>	5	<i>Government service</i>	3
<i>Share/ Stocks Investor</i>	5	<i>Landlord/ Homeowner</i>	3
<i>Software/ Information and Technology Business</i>	5	<i>Private Service: Managerial</i>	3
<i>Travel Agent</i>	4	<i>Teacher (Public/ Private/ Autonomous Educational Institution)</i>	2
<i>Merchants with over 10 million takas invested in the business</i>	4	<i>Private Sector Employee</i>	2
<i>Freight/ Shipping/ Cargo Agent</i>	4	<i>Self-employed Professional</i>	2
<i>Automobile's business (New or Reconditioned)</i>	4	<i>Student</i>	2
<i>Leather/Leather Goods Business</i>	4	<i>Retiree</i>	1
<i>Construction Materials Trader</i>	4	<i>Farmer/ Fisherman/ Laborer</i>	1
<i>Business Agent</i>	3	<i>Others (please write down and assigned numerical score as needed)</i>	1-5
<i>Thread/"Jhut" Merchant</i>	3		
<i>Transport Operator</i>	3		
<i>Tobacco and Cigarettes Business</i>	3		
<i>Amusement Park/ Entertainment Provider</i>	3		
<i>Motor Parts Trader/ Workshop</i>	3		
<i>Small Business (Investment below BDT 5 million)</i>	2		
<i>Computer/ Mobile Phone Dealer</i>	2		
<i>Manufacturer (except, weapons)</i>	2		
<i>Others (please write down and assigned numerical score as needed)</i>	1-5		

Annexure-3

Instructions for photo capture for face-matching

For both assisted and self check-in methods, the live photograph of the customer and their original documents shall be captured in proper light so that they are readable and identifiable. A few pointers are to be ensured during the photo capture process:

- (a) **Use a high-resolution camera:** A high-resolution camera, such as a smartphone camera or webcam, should be used to capture the highest-quality picture possible. This ensures that the details on the photo are clear and visible, making it easier to verify the customer's identity.
- (b) **Adequate white lighting:** The room where the photos are taken should have adequate white lighting to ensure that the photo is well-lit, and the details are visible. This is particularly important if the customer is using a webcam in a dimly lit room.
- (c) **Capture photos against a white background:** It is preferable to capture the photos against a white background. This helps to remove distractions in the background, making it easier to focus on the customer's face.
- (d) **Avoid reflection of light:** During the capturing of the NID front and back photo, it must be ensured that there is no reflection of light which may hinder visibility. Reflections can distort the image, making it difficult to verify the customer's identity.
- (e) **Full front side of the face should be visible:** The full front side of the face should be visible during photo capture. This means the customer should be at a forward-facing angle so that the facial features are captured properly. This ensures that the photo is clear and easily recognizable, helping to verify the customer's identity.
- (f) **Educate customers about the photo-capturing process:** Banks/FCs/MFS providers should educate customers about the photo-capturing process to avoid errors during the self-check-in method. This can help customers understand the importance of clear photos and ensure that the photos they submit are of high quality, making it easier to verify their identity.
- (g) **Depth Sensing while photo capturing:** Banks/FCs/MFS providers should ensure the captured photo is of a 3D human body, through depth sensing. Appropriate liveness detection measures (including, but not limited to, eye blinking, smiling, and left- and right-side facial profile verification) shall be implemented in compliance with relevant international standards, including ISO/IEC 30107.
- (h) **Step-by-step instructions for photo capturing are given below:**
 - i. *Find a well-lit area: Look for an area that is well-lit with white lighting. Avoid dimly lit areas or areas with colored lighting, as this can affect the quality of the photo.*
 - ii. *Find a white background: Look for a white background to stand against. This could be a white wall or a white sheet. Avoid busy or cluttered backgrounds, as this can be distracting and affect the quality of the photo.*
 - iii. *Position yourself correctly: Stand facing forward, with your face fully visible in the camera frame. Make sure that your face is not obscured by hair, clothing, or accessories. Keep your head straight and do not tilt it in any direction.*
 - iv. *Hold the camera at eye level: Hold the camera at eye level and make sure it is focused on your face. Avoid holding the camera too high or too low, as this can distort the image and affect the quality of the photo.*
 - v. *Take the photo: Once you are in the correct position and the camera is focused on your face, take the photo. Make sure that there are no reflections or glare on the photo, as this can affect its quality.*