ශ්‍රී ලංකා මහ බැංකුව
இலங்கை மத்திய வங்கி
CENTRAL BANK OF SRI LANKA

මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதற் பிரிவு
FINANCIAL INTELLIGENCE UNIT

අංක 30, ජනාධිපති මාවත, කොළඹ 01, ශ්‍රී ලංකාව
இல. 30, சனாதிபதி மாவத்தை, கொழும்பு - 01, இலங்கை
No. 30, Janadhipathi Mawatha, Colombo 01, Sri Lanka

Guideline No. 03/2020

Ref: 037/05/006/0009/020

December 30, 2020

To: CEOs / General Managers/Managing Directors of All Financial Institutions

Dear Sir/Madam

Revised Guidelines for Non Face-to-Face Customer Identification and Verification Using Electronic Interface Provided by the Department for Registration of Persons, No. 3 of 2020

Further to the Guideline issued dated October 22, 2020 on the above.

The above revised Guideline will comes in to force with immediate effect and shall be read together with the Financial Transactions Reporting Act, No. 6 of 2006, Financial Institutions (Customer Due Diligence) Rules, No. 01 of 2016 and Insurers (Customer Due Diligence) Rules, No. 1 of 2019 as amended from time to time.

Accordingly, the Guideline issued on 22.10.2020 will be withdrawn w.e.f. 30.12.2020.

Yours sincerely,

E H Mohotty
Director
Financial Intelligence Unit

Cc;

1) Director, Bank Supervision Department of Central Bank of Sri Lanka
2) Director, Department of Supervision of Non-Bank Financial Institutions of Central Bank of Sri Lanka
3) Director, Payments and Settlements Department of Central Bank of Sri Lanka
4) Director General, Securities and Exchange Commission of Sri Lanka
5) Director General, Insurance Regulatory Commission of Sri Lanka
6) Commissioner General, Department for Registration of Persons
7) Compliance Officers, all Financial Institutions

☎ 011-2477125 011-2477509 | 011-2477692 011-2477708 | fiu@cbsl.lk dfiu@cbsl.lk | www.fiusrilanka.gov.lk

Guidelines for Non Face-to-Face Customer Identification and Verification Using Electronic Interface Provided by the Department for Registration of Persons, No. 3 of 2020

Part I - Introduction

1. These Guidelines are issued pursuant to section 15(1) (j) of the Financial Transactions Reporting Act, No. 06 of 2006 (FTRA).

2. These Guidelines are issued to Financial Institutions (FIs) and Insurers[1] (INs) to facilitate verification of identity (verification against the original document) when onboarding non face-to-face[2] individual customers (natural persons) using electronic interface provided by the Department for Registration of Persons (hereinafter referred to as DRP).

3. These Guidelines will come into force with immediate effect and shall be read together with the FTRA and Financial Institutions (Customer Due Diligence) Rules, No. 01 of 2016 (FI CDD Rules) and Insurers (Customer Due Diligence) Rules, No. 1 of 2019 (IN CDD Rules)as amended from time to time.

4. These Guidelines may be modified from time to time or withdrawn in the event of any unforeseen risks arising in the future or when more effective and reliable methods for establishing and verifying customer identity in non face-to-face onboarding come into force.

Part II - Scope

5. These Guidelines provide alternate methods to meet the requirement of "verification against original document" for individual customers who are natural persons as detailed in the following:

    a) Schedule to the FI CDD Rules under Rule 27 – Item (1) (b)(i)—verification of identity document
    b) Schedule to the FI CDD Rules under Rule 27 – Item (1) (b)(ii)—verification of address
    c) Schedule to the IN CDD Rules under Rule 26 and 41 – Item (1) (b)(i)—verification of identity document
    d) Schedule to the IN CDD Rules under Rule 26 and 41 – Item (1) (b)(ii)—verification of address

6. All other requirements imposed under CDD Rules will be applicable to customers onboarded using the above method without any exception.

Part III - Methods of Application

7. Verification of individual customer identity document

[1] **Insurers** shall have the same definition as provided for in the Rule 2 of the Insurers (Customer Due Diligence) Rules, No. 1 of 2019,

[2] **Non-face-to-face** interactions are considered to occur remotely, meaning the parties are not in the same physical location and conduct activities by digital or other non-physically-present means.

a. Claimed Identity[3]. FIs must continue to identify their customers in full accordance with CDD Rule 27(1)(a) and obtain all information described in Rule 27(1)(b) from the customer.

   Claimed identity information may be obtained by the FI/IN in any manner that safeguards its integrity during the process of transmission. Potential modes of obtaining identity information include but are not limited to electronic forms, mobile app, video conferencing, secure email, kiosks/ ATMs/ CDMs, registered post, etc.

b. Existence of Claimed Identity. FIs may use electronic interface published by the DRP to obtain information to independently validate the customer's claimed identity, provided:

   i. The interface is accessed with the unique credentials assigned to the FI/IN by the DRP;
   ii. The interface is accessed strictly in accordance with its terms of use;
   iii. The interface returns to the FI/IN:
      (a) a record that uniquely matches the claimed identity information provided by the customer in a form suitable for verification of customer identity claims, and
      (b) such record includes an image of the person to whom the identity has been assigned to, and
      (c) the image rendered is suitable for the purpose of associating the record with the claimed identity of the customer;
   iv. The FI/IN has no reasonable indication to believe that the interface, or the effectiveness thereof, has been maliciously compromised in any way.

c. Associating Claimed Identity with Customer. The following steps must be performed in order to associate the claimed identity with the customer:

   i. Obtaining Customer Imagery and other documents from the Customer:
   High-quality still images[4] of the customer, ID documents and address verification documents must be obtained. For customers not physically present in Sri Lanka, passport images must also be obtained containing customer biographical data, a current visa and an entry stamp or any other entry permitting official document for the country where they are located. The imagery should be of sufficient quality to read details and to inspect generic security features[5]of the identity document, to identify unique facial features of the customer, and to detect any potential alterations to the document. Ideally, the imagery should be obtained from a device known to be associated with the customer (e.g. a mobile phone) or from a dedicated device operated by, or on behalf of, the FI/IN (e.g. kiosk devices).

   ii. Obtaining Customer Real-Time Video from the Customer

[3] **Claimed Identity** refer to an applicant's declaration of not validated and unverified personal attributes.
[4] **High-quality still images** refer to resolution equivalent to 300 PPI/ DPI (Pixels Per Inch / Dots Per Inch) or higher.
[5] **Generic security features** refer to features of the identity document generally visible when the physical document is inspected

A staff member of the FI/IN must engage in a high-quality real-time video[6] conference with the customer and verify the possession of his identity documents and address verification documents during this real-time video conference. For customers not physically located in Sri Lanka, passport and visa data from (i) must also be verified. The customer should respond via real-time video conference to FI/IN inquiries in order to establish the authenticity of the imagery and the accuracy of other customer provided information.

iii. Obtaining Customer Imagery from DRP

FIs must use electronic interface published by DRP in order to obtain information to authenticate the validated identity information against the customer claimed identity, in accordance with the provisions detailed in paragraph 7(b). As a practical matter, the only currently available information for this purpose is a photographic image associated with a National Identity Card (NIC).

FI/IN must maintain a record on identity information obtained through DRP electronic interface for each customer (eg. audit log, unique reference, or screenshot).

iv. Authenticating Claimed Identity to Customer

The following modes shall be used to authenticate the claimed Identity to the Customer:

1. Algorithmically: FIs that intend to authenticate a claimed identity algorithmically using data and images obtained from both the customer and DRP must obtain prior approval from the FIU in the form of an "enforcement forbearance" by submitting an application to the CBSL "Regulatory Sandbox" and completing the FIU's addendum to the application. Without such forbearance obtained and followed up by entering to an FI/IN agreement with the FIU to abide by the terms of the forbearance, FIs/INs are not permitted to authenticate claimed identities using this mode.

   The Sandbox Framework documents along with the Sandbox application form can be downloaded at https://www.cbsl.gov.lk/en/public-notices. For any inquiries or clarification contact Payments and Settlements Department of Central Bank of Sri Lanka on 2477542, 2477642 or e-mail to sandbox@cbsl.lk.

2. Manually: Manual comparison by employees of the FI/IN should be made in all cases when an algorithmic comparison has not been approved by the FIU through guidelines or specific letters of forbearance [e.g. obtained through the CBSL Regulatory Sandbox]. The standard for successful non face-to-face authentication should be at least as rigorous as for the FI/IN's face-to-face mode.

3. A combination of algorithmic and manual modes may also be used. However, if the algorithmic mode employed has not been approved by the

[6] **High-quality real-time video** refers to consistent resolution equivalent to 360p (pixels) or higher with minimal frame droppage.

FIU through guidelines or specific letters of forbearance then the manual mode must function as the sole determinative.

When the claimed identity cannot be verified or authenticated the FI/IN must not enter into a business relationship with the customer or process transactions on behalf of the customer using this alternative verification method.

8. Verification of Individual Customer Address

   Individual Customer addresses may be verified using data matching the customer's claimed identity obtained by the FI/IN through a DRP electronic interface. If the residential address provided by the customer differs from the address obtained through a DRP electronic interface, the FI/IN must instead verify the customer's address using independent data or services provided electronically FI/IN from one or more sources[7] or obtaining high quality images of the address verification documents or obtaining e-statements of address verification documents specified in Schedule to the FI CDD Rules under Rule 27- Item (1)(a)(a1)(iii) or IN CDD Rules under Rule 26 and 41- Item (1)(a)(a1)(iii).

9. Instances where FIs should refrain from opening accounts or establishing business relationships non face-to-face.

   a. When non face-to-face customer uses any other identification document other than national identity card such as passport or driver's license to identify himself.

   b. When high quality interactive real time video of the customer cannot be obtained.

   c. When high quality data and still images of customer identity documents cannot be obtained.

   d. When identity documents presented by the customer appear to be damaged or degraded to the point that the documents are no longer fit for the purpose of identification.

   e. When identity documents presented by the customer appear altered or when document's generic security features cannot be validated or when the integrity of the document is suspected under any other reason.

   f. When the customer refuses or unable to comply with any aspect of the FI/IN's established non face-to-face onboarding procedures. The customer cannot be on boarded using the non-face-to-face mode if customer fails to cooperate with full completion of the FI/IN's established non face-to-face onboarding procedure. Such non-compliance can take many different forms including but not limited to a refusal or inability to adjust ambient lighting, a refusal or inability to remove anything that obscures a clear view of the customer's face, customer's refusal or

[7] **Independent data or services provided electronically from one or more sources** (for address verification) refer to use of utility service providers websites or mobile applications for bill payments which indicate the address with the name

inability to remain still or to still the image capturing device, customer's refusal or inability to answer questions posed by the onboarding officer(s).

g. When a failure of FI/IN systems prevents the FI/IN from fully executing their established non face-to-face onboarding procedures to include, for example, recording and secure storage of onboarding video and image captures of identity documents.

h. When the claimed identity cannot be shown to exist using the DRP electronic interface.

i. When details of the customer's claimed identity are not consistent with details obtained for the claimed identity through the DRP electronic interface.

j. When a non face-to-face customer presents a NIC with a photo image, which the onboarding officer matches with data and imagery from the DRP, but unable to positively match with the current appearance of the customer claiming the identity.

k. When a non face-to-face customer appears to have intentionally modified his appearance in a manner intended to compromise the ability of the FI/IN to accurately identify and verify the customer and to fully complete its established non face-to-face onboarding procedure.

l. When a claimed identity cannot be authenticated to the customer due to an inability to match, with a high degree of confidence, the images obtained of the customer and of the customer identity documents with corresponding images obtained from DRP.

m. When the FI/IN has reason to doubt the veracity of any customer claims, whether related to identity or otherwise.

n. When customer behavior causes the FI/IN to doubt the legal intents or purposes of the customer in establishing business relations.

o. When the FI/IN is unable to identify the current location (eg. using Global Positioning System (GPS) or any other suitable mechanism to identify the location[8] and to determine whether customer is a resident or a non-resident) of the customer by the FI.

p. Where the FI/IN has a reasonable suspicion on the authenticity of the document(s) in any manner.

10. Policies, Training, Record Keeping and Audit

[8] **any other suitable mechanism to identify the location** refer to use of IP address, calling landline phone number, calling foreign phone number, current visa and an entry stamp or any such mechanism to identify resident, non-resident status. However, obtaining customer declaration on resident and non-resident status is not acceptable.

a. The FI/IN must establish clear policies and procedures for non face-to-face customer identification and onboarding prior to applying the alternate methods described herein.
b. The FI/IN must conduct at least an entry level training programme and carry out ongoing training for relevant onboarding staff prior to applying the alternate methods described herein. The FI/IN should extend adequate training to staff relevant to the functions other than onboarding, where the FI/IN is of the view that such training would be beneficial for the success of the operations directly or indirectly associated with customer relations.
c. FI/IN records that are unique to the alternate methods of customer identification and onboarding contained herein are fully subject to CDD rules regarding record keeping and must be retained in a form sufficient for an internal or external auditor to independently reconstruct the full identification process for any specific customer. Retention of video images is recommended. In the case where a suspicion is formed related to customer's identity, the retention of video is mandatory.
d. FI/IN customer identification programmes using the alternate methods described herein must be included in the FI/IN's internal audit scope under Anti Money Laundering and Combating the Finance of Terrorism (AML/CFT) aspects in order to determine efficacy of the programme and to detect operational deviations from policy.

Part IV - Risk Management

11. The non face-to-face methods of identity verification described herein must be considered in the context of the FI/IN's "risk-based approach" prior to use. The FI/IN's risk assessment must be updated to reflect the impact of the non face-to-face methods.

12. Customer risk profiles must reflect any non face-to-face methods of identification used for the purpose of their identification.

13. The risks related to customers identified using non face-to-face methods described herein should be managed in accordance with the risk management measures outlined in the FI/IN CDD Rules.

14. Risks of the customers located outside of Sri Lanka must be managed in accordance with the known risks of the jurisdiction where the customer is located.

Part V – STR Reporting

15. The entirety of the circumstances, most especially those related specifically to non face-to-face customer identification, must be considered in order to determine whether filing a suspicious transaction report with the FIU is warranted in relation to non face-to-face customer onboarding.

16. Such circumstances may include but not limited to impersonation, any doubt on document authenticity, forged ID and address verification documents, altered ID or address verification documents, altered images, spoofing, reluctance to cooperate or provide additional information for verification, suspicious behavior, discrepancies in information provided.

Part VI - Enforcement

17. The FIU will forbear on enforcement of Schedule to the FI CDD Rules under Rule 27- Items (1) (b)(i) and Schedule to the CDD Rules under Rule 27- Item (1) (b)(ii) and IN CDD Rules under Rule 26 and 41- Items (1) (b)(i) and Schedule to the IN CDD Rules under Rule 26 and 41- Item (1) (b)(ii) when:
    a. the non face-to-face methods of customer identification contained herein are applied to a particular individual customer, and;
    b. these Guidelines are strictly followed in its entirety by the FI; and
    c. until such time that this Guidance remains in force.

22 December 2020