BANGKO SENTRAL NG PILIPINAS

OFFICE OF THE GOVERNOR

CIRCULAR NO. 1170
Series of 2023

Subject: **Amendments to Section 921/921Q of the Manual of Regulations for Banks (MORB)/ Manual of Regulations for Non-Bank Financial Institutions (MORNBFI) on Customer Due Diligence, including Guidelines on Electronic Know-Your-Customer**

The Monetary Board, in its Resolution No. 402 dated 23 March 2023, approved the amendments to the provisions of Section 921 of the Manual of Regulations for Banks (MORB) and Section 921Q of the Manual of Regulations for Non-Bank Financial Institutions (MORNBFI) on customer due diligence, including guidelines on electronic Know-Your-Customer (e-KYC) using digital identity (ID) system.

Section 1. Section 921 of the MORB and Section 921Q of the MORNBFI on customer due diligence is hereby amended to read, as follows:

921 CUSTOMER DUE DILIGENCE

a. In conducting customer due diligence (CDD), a risk-based approach shall be undertaken depending on the type of customer, business relationship or nature of the product, transaction or activity. In this regard, a covered person shall maintain a system that will ensure the conduct of CDD which shall include:

(1) xxx;
xxx
(4) xxx.

Where a covered person is unable to comply with the relevant CDD measures, considering risk-based approach, it shall (a) not open the account, commence business relations, or perform the transaction; or (b) terminate the business relationship; but in both cases, it shall consider filing a suspicious transaction report (STR) in relation to the customer.

xxx

Customer Identification. *xxx*

a. Minimum information/documents required:

(1) *New individual customers. xxx*

Unless otherwise stated in this Part, average CDD requires that the covered person obtain from individual customers, at the time of account opening/establishing the relationship, the following minimum information and verify the customer's identity with the official or valid identification documents or other reliable, independent source documents, data, or information:

(a) name of customer and/or PhilSys Card Number (PCN) or the PhilSys Number (PSN) derivative;

xxx
(g) xxx;

Pursuant to Republic Act No. 11055 or the Philippine Identification System Act and its Revised Implementing Rules and Regulations (RIRR), the Philippine Identification System (PhilSys) is the government's central identification platform for all citizens and resident aliens of the Philippines. An individual's records in the PhilSys shall be considered as an official and sufficient proof of identity. Considering its identity proofing, enrolment, authentication and identity life cycle management processes, the PhilSys is considered a reliable and independent source of verifying the customer's identity. Where the PCN or PSN derivative, or the Philippine Identification (PhilID) card, in physical or digital form, is presented by the customer, it shall be accepted as official and sufficient proof of identity, subject to proper authentication, and the covered person shall no longer require additional document to verify the customer's identity.

xxx

b. Customer Verification Process. Covered persons shall xxx
xxx

(1) this occurs xxx
xxx
(3) the ML/TF risks xxx

Covered persons shall adopt appropriate risk management measures with respect to how the customer may use the business relationship prior to verification. These measures may include, among others, setting up of transaction limits and monitoring of transactions that are beyond the expected activities or norms for the type of relationship.

c. Valid identification documents.

(1) Customers and the authorized signatory/ies of a corporate or juridical entity xxx

(2) If the official document presented is not the PhilID, PCN or PSN derivative, a covered person may classify identification documents based on its reliability and ability to validate the information indicated in the identification document with that provided by the customer and ensure that risks are mitigated.

In case the identification document presented xxx

In customer identification process, covered persons shall implement appropriate systems of data collection and recording, such as: (1) photocopying/scanning of identification document presented; (2) using Information and Communication Technology (ICT) to capture and record the biometric and other personal information of customers; and/or (3) manual recording of identification information.

In cases where the PhilID is presented, only the front portion/face should be photocopied/scanned. The PSN located at the back portion of the PhilID must remain confidential subject to applicable laws and regulations. In this regard, covered persons may only obtain either the PCN or PSN derivative indicated in the PhilID presented as part of customer identification and verification.

Covered persons shall also comply with the required digitization of customer records, as applicable, pursuant to relevant BSP and AMLC issuances.

Relief in case of calamity. In case of a disastrous calamity xxx

(a) The amount of transactions xxx
xxx
(d) The customer's account activities xxx with the prescribed period.

d. Face-to-face contact. xxx

The use of ICT in the conduct of face-to-face contact and/or interview may be allowed: *Provided*, That the covered person has measures in place to mitigate the ML/TF risks and that key CDD processes are documented or with adequate audit trail.

xxx

g. Electronic Know Your Customer (e-KYC). e-KYC refers to the process of electronically verifying the credentials of a customer.

Covered persons may use different methods to conduct customer identification and verification including e-KYC through digital ID system. For this purpose, digital ID systems are systems that cover the process of identity proofing/enrolment and authentication. Identity proofing and enrolment can be either digital or physical (documentary), or a combination, but binding, credentialing, authentication, and portability/federation must be digital. The digital ID system to be used in conducting CDD must be supported by robust technology, adequate governance, processes and procedures that provide appropriate level of confidence that the system produces accurate results. It should also be soundly protected against cyber-attacks and internal malfeasance or external manipulation/ falsification by unauthorized users to fabricate false or synthetic identities.

When employing e-KYC using a digital ID system, the covered person should ensure that it is anchored on, among others, robust, effective, and reliable information and communication technology architecture. Where the tiering is based on, among others, level of access and authentication assurance levels, it shall adopt a tiered or risk-based e-KYC policies and procedures (e.g., low tier level has access to basic authentication which requires minimum assurance levels or controls; access to subsequent tier level and additional services requires higher assurance/controls). Assurance levels refer to the extent of trustworthiness or confidence in the reliability of each of the three (3) stages of the digital ID process, from identity proofing and enrolment to authentication, and identity lifecycle management. In implementing e-KYC through digital ID system, the covered person shall:

(1) Understand the basic components of the digital ID system, particularly how they apply to the CDD requirements, as these will support customer identification and verification process.
   (a) Identity proofing and enrolment. This involves the collection, validation, deduplication and verification of identity evidence and information provided by the person; and establishing an identity account (enrolment) and binding the individual's unique identity to authenticators possessed and controlled by the person;
   (b) Authentication. This establishes, based on possession and control of authenticators, that the person asserting an identity (the on-boarded customer or claimant) is the same person who was identity proofed and enrolled; and
   (c) Identity lifecycle management. This refers to the actions that should be taken in response to events that can occur over the identity

lifecycle and affect the use, security and trustworthiness of authenticators, for example, loss, theft, unauthorized duplication, expiration, and revocation of authenticators and/or credentials.

(2) Apply informed risk-based approach to reliance on digital ID system for CDD that includes the requirement under item "(1)" above and ensure that the assurance level/s are appropriate for the ML/TF risks presented by the customer, product, delivery channel, geographical location, among others. This will enable the implementation of a tiered customer identification and acceptance process that leverages digital ID systems with various assurance levels to support financial inclusion. For example, in case of non-face-to-face channels, if the customer identification and verification depend on reliable, independent digital ID system with appropriate risk mitigation measures, this may pose normal risk, or even lower risk where higher assurance levels are implemented. The assurance level will determine if the digital ID system is reliable and independent for AML/CFT purposes.

(3) Utilize anti-fraud and cyber-security processes to support digital identity proofing and/or authentication for AML/CFT measures such as customer identification/verification at onboarding and ongoing due diligence and transaction monitoring.

A covered person may rely on another entity in the conduct of customer identification and verification, using a digital ID system, subject to existing rules on outsourcing and third-party reliance requirements, as applicable. Moreover, the relying party should ensure that the third party's digital ID system enables the former to (i) immediately obtain the necessary information concerning the identity of the customer (including the assurance levels, where applicable); and (ii) take adequate steps to satisfy itself that the third party will make available copies or other appropriate forms of access to the identity evidence (documents, data and other relevant information) upon request without delay.

In any case, the relying covered person has the ultimate responsibility for the customer identification/verification process, and effective authentication, using the digital ID system provided by the digital ID service provider, and ensure that risk-based approach is applied in the use of the digital ID systems for customer identification/verification and authentication.

The covered person shall ensure that its conduct of e-KYC complies with relevant user consent and data sharing and protection/privacy laws, rules and regulations for data processing, storage, and management. All related transaction/s and their attendant risks or obligations, including the roles and responsibilities of each party involved, must be explicitly, clearly, and adequately provided by the covered person, and are explained to, understood, and accepted by the customer.

In this regard, pursuant to R.A. No. 11055 and its IRR, the PhilSys-enabled e-KYC is recognized as an acceptable system for e-KYC using digital ID system in the Philippines, including the PhilSys-issued credentials in physical or digital form, or authentication against the PCN, PSN derivative, or other tokens that will be issued by PhilSys, and an authentication factor such as biometric or demographic information. Further, covered persons, as relying parties, must comply with the onboarding and other e-KYC related guidelines issued by the Philippine Statistics Authority (PSA) prior to use of or access to the PhilSys-enabled e-KYC. For covered persons that will utilize the PhilSys-enabled e-KYC, they shall ensure compliance with the applicable guidelines and full implementation of the authentication procedures/methods and other related systems under the PhilSys.

Covered persons implementing e-KYC must perform customer identification and verification process under the same standards equivalent to those for face-to-face basis, and shall establish appropriate risk management processes.

Consistent with Section 002 of the MORB/Section 002Q of the MORNBFI, the BSP may deploy appropriate supervisory enforcement actions to promote adherence with the requirements set forth in this Section and bring about timely corrective actions.

h. Trustee, nominee xxx

i. Prohibited accounts. xxx

xxx

Section 2. The following transitory provision shall be incorporated as footnote to item "g." on e-KYC under Section 921/921Q of the MORB/MORNBFI:

Covered persons with existing e-KYC, using a digital ID system, at the time of the effectivity of this Circular shall comply with the requirements prescribed herein within one (1) year from effectivity of this Circular. For covered persons without existing e-KYC and intend to adopt the same, they shall ensure strict compliance with the e-KYC requirements prescribed in this Circular prior to implementation.

Section 3. This Circular shall take effect fifteen (15) calendar days following its publication either in the Official Gazette or in a newspaper of general circulation.

FOR THE MONETARY BOARD:

EDUARDO S. BOBIER
Officer-in-Charge

30 March 2023