FSF - Customer Identification and Verification Guidelines for Fintech Stakeholders
Financial Sector Forum

24 August 2021

Introduction

The member supervising authorities (SAs) of the Financial Sector Forum ("FSF")[1] – Financial Technology Committee ("FinTech Committee") are jointly issuing these guidelines to establish standards for **remote electronic customer identification and verification processes for all financial institutions that engage in FinTech ("Covered FIs") under the regulatory authority of the member SAs of the FSF**. This is in recognition of the significant and evolving changes in the financial system and the Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT) landscape with respect to the verification and protection of customer information and safeguards against money laundering, terrorist financing, proliferation financing, and other financial crimes.

These guidelines, as agreed upon by the member SAs of the FSF, are designed to guide both the SAs and Covered FIs on the basic principles and requirements of remote electronic customer due diligence measures for customers, their agents and beneficial owners in relation to FinTech. These Guidelines do not, in any way, prescribe a "one size fits all" framework. Hence, the principle of proportionality is considered in the application of the provisions hereof. SAs may set additional requirements specific to the Covered FIs under their jurisdiction and pursuant to their own respective customer due diligence and risk management policies and procedures.

These guidelines do not endorse any particular technology, and shall apply to customers, whether natural or juridical persons, of all covered FIs under the regulatory purview of the member SAs of the FSF.

Section 1. Definition of Terms[2] – For purposes of these Guidelines, the following definitions shall apply, unless the context otherwise requires:

a. **Covered Financial Institutions ("Covered FIs")** refer to covered persons[3], as defined by AMLA, and other entities performing multiple regulated activities, such as, but not limited

[1] The FSF, composed of the Bangko Sentral ng Pilipinas (BSP), Securities and Exchange Commission (SEC), Insurance Commission (IC), and Philippine Deposit Insurance Corporation (PDIC), was created in 2004 as a voluntary inter-agency body to provide an institutionalized regulatory framework for coordinating the supervision and regulation of the financial system, facilitate consultation and the exchange of information and ideas among regulators and provide a platform to harmonize the regulation of financial products offered by the various types of financial institutions.

[2] Definitions were adopted from the 2021 Memorandum of Agreement on the Cooperative Oversight Framework of the FSF.

[3] As provided under Rule 4 of the 2018 AMLA Revised Implementing Rules and Regulations (RIRR), the following are the covered persons under the AMLA: "(a) The following financial institutions: (1) Persons supervised and/or regulated by BSP, including their subsidiaries and affiliates, which are also covered persons, supervised and/or

to, banking, investing, lending, and insurance, operating under a single application platform which fall under the supervision and/or under the regulation of the FSF SAs.

b. **Financial Technology Committee ("FinTech Committee")** refers to the working group designated by the FSF in overseeing the implementation of these guidelines and shall be composed of the Bangko Sentral ng Pilipinas ("BSP"), Securities and Exchange Commission ("SEC"), Insurance Commission ("IC") and Philippine Deposit Insurance Corp. ("PDIC").

c. **Financial Technology ("FinTech")** refers to a software, a service, or a business that provides technologically advanced ways to make financial processes and transactions more efficient compared to traditional methods[4], specifically:[5]

i. FinTech shall also refer to financial operations using digital technology or being delivered through digital means, including electronic money, mobile financial services, and online financial services;

ii. FinTech shall encompass monetary transactions such as depositing, withdrawing, sending and receiving money, as well as other financial products and services including payment, credit, savings, pensions and insurance; and

regulated by the BSP such as: (a) Banks (b) Quasi-banks (c) Trust entities (d) Pawnshops (e) Non-stock savings and loan associations (f) Other Non-bank financial institutions which under special laws are subject to BSP supervision and/or regulation (g) Electronic money issuers and (h) Foreign exchange dealers, money changers, and remittance and transfer companies. (2) Persons supervised or regulated by IC, such as: (a) Insurance companies (b) Pre-need companies (c) Insurance agents (d) Insurance brokers (e) Professional reinsurers (f) Reinsurance brokers (g) Holding companies (h) Holding company systems (i) Mutual benefit associations and (j) All other persons and their subsidiaries and affiliates supervised or regulated by the IC. (3) Persons supervised or regulated by SEC, such as: (a) Securities dealers, brokers, salesmen, investment houses, and other similar persons managing securities or rendering services, such as investment agents, advisors, or consultants (b) mutual funds or open-end investment companies, close-end investment companies or issuers, and other similar entities; and (c) other entities, administering or otherwise dealing in commodities, or financial derivatives based thereon, valuable objects, cash substitutes, and other similar monetary instruments or properties, supervised or regulated by the SEC. (b) The following DNFBPs: (1) Jewelry dealers (2) Dealers in precious metals, and dealers in precious stones (3) Company service providers, which, as a business, provide any of the following services to third parties: (a) acting as a formation agent of juridical persons; (b) acting as (or arranging for another person to act as) a director or corporate secretary of a company, a partner of a partnership, or a similar position in relation to other juridical persons; (c) providing a registered office; business address or accommodation, correspondence or administrative address for a company, a partnership or any other juridical person or legal arrangement; and (d) acting as (or arranging for another person to act as) a nominee shareholder for another person. (4) Persons, including lawyers, accountants and other professionals, who provide any of the following services: (a) Managing of client money, securities or other assets; (b) Management of bank, savings, securities or other assets; (c) Organization of contributions for the creation, operation or management of companies; and (d) Creation, operation or management of juridical persons or arrangements, and buying and selling business entities. (5) Casinos, including internet-based casinos and ship-based casinos, with respect to their casino cash transactions related to their gaming operations."

[4] Fintech as defined in the 2021 Memorandum of Agreement on the Cooperative Oversight Framework of the Financial Sector Forum

[5] OECD (2017), G20/OECD INFE Report on Ensuring Financial Education and Consumer Protection for All in the Digital Age

iii. FinTech shall also include non-transactional services which are incidental to the financial transaction, such as viewing personal financial information through digital devices.

Section 2. Customer Due Diligence (CDD)

In operating a reliable environment for implementing AML/CFT measures that meet the goal of financial inclusion without compromising their effectiveness in combating crime, Covered FIs shall develop and strengthen their own CDD systems and processes leveraging on the flexibility to adopt specific due diligence measures and processes appropriate to their own circumstances.

a. In conducting CDD, a risk-based approach shall be undertaken depending on the type of customer, business relationship, source of income/wealth or nature of the product, transaction, or activity, among others.

b. Where a Covered FI is unable to comply with the relevant CDD measures, it shall (1) refuse to (i) the opening of an account, (ii) the commencement of business relations or (iii) the performance of the transaction, or (2) terminate the business relationship; and (3) consider filing a suspicious transaction report (STR) in relation to the customer.

c. Covered FIs shall establish and record the true identity of their clients based on official documents or other reliable, independent source documents, data, or information. They shall also establish appropriate systems, methods and adequate internal controls, compliant with the AMLA, its RIRR, other Anti-Money Laundering Council (AMLC) issuances, the rules and regulations issued by the SAs, and internationally accepted AML standards, for verifying and recording the true and full identity and existence of their customers, agents, and beneficial owners.

   Identification document (ID) refers to any of the following evidence of identity:

   (1) For Filipino citizens: Those issued by any of the following authorities:
      (a) Government of the Republic of the Philippines, including its political subdivisions, agencies, and instrumentalities;
      (b) Government-Owned or -Controlled Corporations (GOCCs);
      (c) BSP, SEC, IC, or PDIC, specifically, certificates of registration issued to Covered FIs registered with and supervised or regulated by these SAs; and
      (d) Philippine Statistics Authority (PSA) under the Philippine Identification System (PhilSys);
   (2) For foreign nationals: Passport or Alien Certificate of Registration;
   (3) For Filipino students: Valid school ID card for the current academic year duly signed by the school principal or head of the educational institution;
   (4) For low risk customers: Any document or information reduced in writing which the Covered FI deems sufficient to establish the client's identity; and
   (5) Other identification document that can be verified using reliable, independent source documents, data or information.

Section 3. Customer Identification and Verification

a. Customer Identification

Covered FIs shall establish and verify the true identity of their customers based on official document or other reliable, independent source documents, data or information.

(1) **New individual customers.** Covered FIs shall develop a systematic procedure for establishing the true and full identity of new individual customers, and shall open and maintain the account/ relationship only in the true and full name of the account/relationship owner/s.

(2) **New juridical persons.** Covered FIs shall develop a systematic procedure for identifying corporate and partnership entities, as well as their stockholders/partners/owners, directors, officers and authorized signatories. They shall open and maintain accounts only in the true and full name of the entity and shall have primary responsibility to ensure that the entity has not been, or is not in the process of being dissolved, struck-off, wound-up, terminated or otherwise placed under receivership or liquidation.

The minimum information/documents required for new individual and juridical customers are enumerated under Section 4.f (Average Due Diligence) of this document.

b. Customer verification process

Covered FIs shall verify the identity of the customer and take reasonable measures to verify the identity of the beneficial owner, in the case of juridical persons, before or during the course of originating new customer accounts, establishing a business relationship or conducting transactions for occasional customers remotely. They may complete the verification process after the establishment of the business relationship: Provided, That:

(1) this occurs as soon as reasonably practicable[6];
(2) this is essential not to interrupt the normal conduct of business; and
(3) the money laundering and terrorist financing (ML/TF) risks are effectively managed, taking into consideration risk and materiality.

Covered FIs shall thoroughly assess the risks arising from the remote electronic identification of customers considering the reliability and independence of the sources used for identity verification, the products or services to be provided to customers, as well as geographical and other factors. Covered FIs shall adopt, on the basis of the said risk assessment, the appropriate remote electronic identification process and

[6] The determination of what is reasonably practicable varies depending on the business model of / products offered by the Covered FIs. However, SAs expect Covered FIs to define, document and disclose what is reasonably practicable for their business.

technological solution, and shall ensure their effective implementation and integrity, respectively.

Covered FIs shall carefully examine the validity and authenticity of the data, documentation and information obtained in respect of customers as part of the remote electronic identification process, using an adequate range of data from different, reliable and independent sources, and bearing in mind that the data obtained electronically from the identity document of a customer not physically present are not enough to verify his/her identity unless accompanied by necessary control measures and mechanisms.

c. **Valid identification documents**

(1) Customers and the authorized signatory/ies of a corporate or juridical entity who engage in a financial transaction with a Covered FI for the first time shall be required to present official identification document. This shall include any of the official documents or other identification information which can be verified from reliable, independent source, documents, data or information, such as third-party verified customer information database, such as the PhilSys database.

(2) Covered FIs may classify identification documents based on their reliability and the ability of the Covered FIs to validate the information indicated in the identification document with that provided by the customer. Whenever deemed necessary, Covered FIs may accept other IDs not described herein, provided that these satisfy relevant laws and the regulatory issuances of the SA concerned.

(3) In customer identification process, Covered FIs shall implement appropriate systems of data collection and recording, such as:

(a) scanning of identification document presented; and/or
(b) using Information and Communication Technology (ICT) to capture and record the biometric and other personal information of customers.

d. **Permitted methods of remote electronic identification**

(1) The use of ICT or other remote identification methods may be allowed: Provided, that Covered FIs have measures in place to mitigate the ML/TF risks and that the entire procedure is documented.

(2) As part of the remote electronic identification process and regardless of the method applied, Covered FIs shall apply specific measures and controls, supported by dedicated media, including the following:

(a) They shall document or record or take photographs/snapshots showing clearly:

(i) the face of the applicant/customer under different angles, e.g., in profile, face on, using in parallel techniques to ensure liveness detection (such as eyes opened, eyes shut); and

(ii) the pages/sides of the identity document that bear the photograph, signature and identity data of the applicant/customer, so they can be checked against the specifications and security features of the document;

(b) They shall use biometric algorithms to compare the customer with the photograph on the identity document; and

(c) They shall adopt multi-factor authentication (MFA) methods, subject to relevant rules of the SA concerned.

(3) Covered FIs may opt to use any the following remote electronic identification methods:

(a) Video conference, which consists of an interactive, real-time audiovisual communication/interview between an applicant/customer and a trained employee who are in different locations, and supports the exchange of files and messages; or

(b) Automated identification via a dynamic selfie, without the physical presence of an employee, taken by the applicant/customer in real time (as opposed to a static selfie), so as to ensure liveness detection.

(4) In the context of the video conference method of remote electronic identification, parties concerned shall, in addition to the above:

(a) Check whether the ID card has been damaged or tampered with, or there are indications of attempted falsification of the document; and

(b) Identify any suspicious behaviour of the customer that may indicate that he/she is under the influence of alcohol or prohibited drugs, is under duress or is mentally deranged.

e. **Outsourcing and Third Party Reliance for customer identification and verification procedures**

(1) Covered FIs may outsource to or rely on a third party for the customer identification and verification procedures, subject to relevant rules on outsourcing/third party reliance of their respective SAs, including the relevant provisions and Implementing Rules and Regulations (IRR) of RA 10173 otherwise known as the Data Privacy Act of 2012 particularly Section X of the IRR.

Notwithstanding the foregoing, Covered FIs have the ultimate responsibility for knowing their customer, keeping the customer's identification documents, maintaining the integrity and confidentiality of pertinent information, safeguarding against data breach, managing all other attendant risks, and

ensuring that the third party uses the appropriate level of verification procedures to confirm the customer's identity.

(2) Authenticating new customers

Covered FIs conducting the entire account opening process remotely shall consider using third-party databases to provide:

(a) Positive verification to ensure that material information provided by an applicant matches information available from third-party sources;
(b) Logical verification to ensure that information provided is logically consistent; and
(c) Negative verification to ensure that information provided has not previously been associated with fraudulent activity (e.g., an address previously associated with a fraudulent application).

(3) Authenticating existing customers

The Covered FI should use reliable and appropriate authentication methods to validate and verify the identity and authorization of customers. Authentication is facilitated by the use of factors, which are generally classified into three basic groups:

(a) Knowledge - Something the user knows (e.g., username, password, mobile PlN, card number, account number);
(b) Possession - Something the user has (e.g., payment card, token, one-time password); and
(c) Inherence - Something the user is (e.g., biometrics).

Section 4. Remote Customer Identification Process

a. Covered FIs shall adopt clearly written and graduated customer acceptance and identification policies and procedures, and controls for the operation of remote electronic customer and account opening or onboarding. These include sanctions screening and implementation of targeted financial sanctions, the criteria for determining to whom the services will be made available, and the terms and conditions for such services.

b. Covered FIs shall ensure that adequate and appropriate remote electronic identification processes and technological solutions are adopted for the validation and verification of the identity of customers based on reliable and independent sources, documents, data or information.

c. Before adopting a remote electronic identification process and the relevant technological solution, Covered FIs shall conduct an informed assessment of, among others:

(1) the possibility of fully integrating the adopted technological solution into their existing systems and processes, and the relevant risk management policies and procedures, particularly on technical and operational risks, i.e., the risk that the technological solution may be unreliable, could be tampered with or may suffer irreparable failure;

(2) the risk that the sources of information used for verification purposes are not sufficiently independent and reliable;

(3) the capability of the technological solution to detect impersonation fraud risks, i.e., the risk that a customer is not who he claims to be or that the person is not a real person;

(4) the ability of the technological solution to fully comply with relevant requirements of the Data Privacy Act of 2012, its Implementing Rules and Regulations, and other National Privacy Commission issuances; and

(5) new/emerging risks posed by the digital customer onboarding or account opening platforms.

Covered FIs shall present and/or submit the result of the informed assessment to the SA concerned for evaluation, in accordance with the latter's specific requirements, prior to the adoption of the proposed remote electronic identification process and the relevant technological solution.

d. Covered FIs shall periodically:

(1) Ensure that their remote electronic identification process and technological solution are able to:

(a) Identify and assess the risks associated with internet and mobile-based products and services;
(b) Identify risk mitigation actions, including appropriate authentication strength and security controls to avoid possible breach; and
(c) Measure and evaluate the effectiveness of adopted awareness mechanisms in ensuring that customers understand the risks and learn the proper use of the remote electronic identification process and technological solution;

(2) Adjust, as appropriate, their technological solution amid relevant changes in technology, the sensitivity of customer information, and internal or external threats to information; and

(3) Implement appropriate risk mitigation strategies.

The remote electronic identification process and technological solution must be reviewed at least annually by the Board and Senior Management and regularly updated in line with changes in business strategies, IT infrastructure and services, and operating environment.

e. **Criteria for Type of Customers**

Covered FIs shall formulate a risk-based and tiered customer acceptance, identification, and retention policy, specifying the criteria and description of the types of customers that are likely to pose low, normal or high money laundering and terrorist financing (ML/TF) risk to their operations, as well as the standards in applying reduced, average and enhanced due diligence.

The authentication techniques employed by the Covered FIs should be appropriate to the risks associated with Covered FIs' products and services, as provided below:

Customer Risk Profile	Level of Due Diligence	Authentication
Low	Reduced Due Diligence (RDD)	May consider single-factor
Normal	Average Due Diligence (ADD)	Multi-factor and other controls
High	Enhanced Due Diligence (EDD)	Multi-factor and other controls

In designing a customer acceptance and risk profiling policy where a customer will be assessed as low, normal or high risk, the following criteria relating to the product or service, the customer, and geographical location, at a minimum, shall be taken into account:

(1) The nature of the service or product to be availed of by the customers and the purpose of the account or transaction;

(2) Source of funds, source of wealth/nature of business, employment of the customer;

(3) Public or high-profile position of the customer and, for juridical person, its directors/trustees, stockholders, officers and/or authorized signatory, including the financial risk profile of its beneficiaries and ultimate beneficial owners;

(4) Country of origin and residence of operations or the fact that a customer came from a high risk jurisdiction, screened for a potential match against domestic/local watchlists from the Anti-Terrorism Council (ATC), Philippine National Police, SEC and other entities or organizations;

(5) The existence of suspicious transaction/red flag indicators;

(6) Watchlist of individuals and entities engaged in illegal activities or terrorist related activities, as circularized by the BSP, AMLC, and other international entities or

organizations, such as the Office of Foreign Assets Control (OFAC) of the U.S. Department of the Treasury, and United Nations Security Council; and

(7) Such other factors, e.g., the amount of funds to be deposited by a customer or the size of transactions, and regularity or duration of the transaction, as the Covered FIs may deem reasonable or necessary to consider in assessing the risk of a customer to money laundering/terrorist financing.

In assessing the risk profile of juridical entities, Covered FIs should also consider the financial profile and other relevant information of these entities' active authorized signatories.

Covered FIs shall, on the basis of materiality and risk, ensure that pertinent identification information and documents collected under the CDD process are kept up-to-date and relevant, by undertaking reviews of existing records, particularly for higher risk categories of customers. Covered FIs shall document the actions taken in connection with updating of customer's records/information, and as may be necessary, accordingly update customer's risk profile.

f. Standards for RDD, ADD and EDD

Covered FIs shall formulate graduated levels of risk-based CDD and shall set the standards in applying RDD, ADD, and EDD, including a set of conditions for continuance or discontinuance of service, or business relationship. Measures for the lower level of diligence shall form part of the requirements for the higher diligence levels.

(1) Reduced Due Diligence (RDD)

Where lower risks of ML/TF have been identified, through the Covered FIs' adequate analysis of risks, and based on the results of institutional risk assessment, RDD procedures may be applied commensurate with the lower risk factors.

Whenever RDD is applied, the following rules shall apply:

(a) For individual customers, Covered FIs may open an account/establish relationship under the true and full name of the account owner/s or customers upon these customers' presentation of an acceptable ID card or other reliable, independent source documents, data or information: Provided, That, for accounts used purely for digital or electronic payments, Covered FIs may define appropriate reduced due diligence procedures provided that ML/TF risks are effectively managed.

(b) For corporate, partnership, and sole proprietorship entities, Covered FIs may open an account under the official name of these entities; Provided, That, the following documents are presented by the representative/s of the entities at

the time of account opening: (a) Certificate of Registration issued by the Department of Trade and Industry (DTI) for sole proprietors, or Certificate of Incorporation or Partnership issued by the SEC for corporations and partnerships, respectively ; and (b) a Board Resolution duly certified by the Corporate Secretary, or equivalent document, authorizing the representative/s to sign for and on behalf of these entities.

(c) Covered FIs may apply a single-factor authentication.

Further, verification of the identity of the customer, beneficial owner or authorized signatory may be made after the establishment of the business relationship, but within a reasonable period of time, provided that conditions under Section 4.c are met.

(2) Average Due Diligence (ADD)

ADD requires that Covered FIs (i) obtain from individual customers, at the time of account opening/establishing the relationship, the following minimum information; and (ii) confirm these information against submitted/presented official or valid ID documents:

(a) Name of the customer and/or PhilSys Number (when available);
(b) Date and place of birth;
(c) Address;
(d) Contact number or information;
(e) Citizenship or nationality;
(f) Specimen signature or biometric data of the customer; and
(g) Name, address, date and place of birth, contact number or information and citizenship or nationality of beneficiary or beneficial owner, whenever applicable;

For new juridical persons, ADD requires that Covered FIs obtain the following minimum information and/or documents before establishing business relationships:

(a) Customer information

(i) Name of juridical person;
(ii) Name, address, and citizenship or nationality of beneficial owner, if applicable, and authorized signatories;
(iii) Official address;
(iv) Contact numbers or information;
(v) Nature of business; and
(vi) Specimen signatures or biometrics of the authorized signatory.

(b) Identification Documents

(i) Certificate of Registration issued by the DTI for sole proprietors, or Certificate of Incorporation or Partnership issued by the SEC for corporations and partnerships, respectively, and by the BSP for money changers/foreign exchange dealers and remittance and transfer companies;
(ii) Secondary license or certificate of authority issued by the SA or other government agency concerned;
(iii) Articles of Incorporation/Partnership, for corporations/partnerships;
(iv) Latest General Information Sheet;
(v) Board/Partners' resolution duly certified by the Corporate/Partners' Secretary, or other equivalent document, authorizing the signatory/ies to sign for or on behalf of the entity; and
(vi) For entities registered outside of the Philippines, similar documents and/or information as above listed, which shall be duly authenticated by a senior officer or the designated officer of the Covered FI assigned in the country of registration; or, in the absence of said officer, by the Philippine Consulate, company register or notary public, where said entities are registered.

(3) Enhanced Due Diligence (EDD)

The procedures performed must enable the Covered FI to achieve a reasonable confidence and assurance that the information obtained are true and reliable.

On top of the requirement for ADD, additional validation procedures for individual customers shall include the following:

(a) Confirming the date of birth from a duly authenticated official document;
(b) Verifying the address through evaluation of utility bills, bank, credit card statement or other documents showing address, sending thank you letters, or through on-site visitation;
(c) Contacting the customer by phone or email;
(d) Determining the authenticity of the ID documents through validation of their issuance by requesting a certification from the issuing authority or by any other effective and reliable means; and
(e) Determining the veracity of the declared source of funds.

For corporate or juridical entities, verification procedures shall include the following:

(a) Requiring the submission of and validating source of funds or source of wealth from reliable documents, such as audited financial statements, income tax return, and bank references;
(b) Inquiring the status of the entity from the SA and/or other relevant government agencies which issue or accept registration of entities;
(c) Verifying the address through on-site visitation of the company, sending thank you letters, or other documents showing address; and
(d) Contacting the entity by phone or email.

Covered FIs shall be required to implement multifactor authentication methods or other controls reasonably calculated to mitigate those risks.

Whenever EDD is applied, the Covered FI shall also be required to satisfy all other EDD procedures as provided by relevant laws and the regulatory issuances of the SA concerned, which include obtaining additional information/document, securing senior management approval, requiring the first payment to be carried out through an account in the customer's name and enhancing ongoing monitoring of relationship.

g. Restricted Account

To promote financial inclusion, customers who may not be able to provide any of the required information for valid reasons, or any valid ID document may be allowed to open a restricted account with a Covered FI, subject to the conditions/limits provided by and relevant rules on restricted accounts of the SA concerned.

In lieu of a valid ID, the Covered FI shall obtain the customer's complete name, birth date, address and nationality and ensure that it has in its records a clear photograph and signature or biometric profile of the customer.

The account opening shall be subject to the condition that the customer shall obtain a valid ID within twelve (12) months; otherwise, the account shall be closed, and the remaining balance therein shall be returned to the customer. An extension of another twelve (12) months may be allowed; Provided, That, the customer is able to show to the Covered FI a proof of application for a valid ID.

Covered FIs shall ensure that the above conditions are not breached; otherwise, complete information and valid ID shall immediately be required, or the account shall be closed accordingly.

Section 5. Employee Due Diligence and Continuing Education and Training Program

a. Covered FIs shall ensure that the remote electronic identification process is conducted by qualified and trained staff, to whom they shall make available necessary resources and special technical media for the smooth and secure implementation of the process. Training shall include the practical application of the technological solution and its functionalities; the security features of acceptable identity documents; common counterfeiting and falsification methods; the requirements of these guidelines; identification of unusual or suspicious transactions and reporting in line with the concerned party's internal procedures. Training shall take place before the staff assumes relevant duties, and refresher programs shall be provided to ensure compliance with applicable rules, regulations, and policies on AML, consumer protection, financial inclusion and literacy, bank secrecy and customer data confidentiality.

b. Covered FIs shall ensure through appropriate procedures that the staff engaged in the identification and validation of customers through the technological solution do not collaborate with persons involved in any ML/TF/ proliferation financing (PF) or unlawful activities. These procedures shall include pre-hiring and regular on-the-job fit for duty assessment; random assignment of individual applications for remote electronic identification to the staff, so as to minimize manipulation risk; and sample checks of the staff's communications with applicants/customers during or after the remote electronic identification process.