

**921 CUSTOMER DUE DILIGENCE**

a. In conducting customer due diligence, 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 customer due diligence which shall include:

- (1) Identifying the customer and verifying the true identity of the customer based on official documents or other reliable, independent source documents, data or information. In case of corporate and juridical entities, verifying their legal existence and organizational structure, as well as the authority and identification of all persons purporting to act on their behalf;
- (2) Identifying the beneficial owner and taking reasonable measures to verify the identity of the beneficial owner based on official documents, or using relevant information or data obtained from reliable sources, such that the covered person is satisfied that it knows who is the beneficial owner. The covered person should have a system to understand the nature of the customer's business and its ownership and control structure, in case of juridical persons or legal arrangements.

Where the customer, or the owner of the controlling interest is a company listed in a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable means) to ensure adequate transparency of beneficial ownership, or is a majority-owned subsidiary of such a company, the covered person is not required to verify the identity of any shareholder or beneficial owner of such companies. The relevant identification data may be obtained from a public register, from the customer or from other reliable sources.

The covered person shall keep records of the actions taken in order to identify the beneficial owner.

- (3) Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship; and
- (4) Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of the relationship to ensure that the transactions being conducted are consistent with the covered person's knowledge of the customer, their business. and risk profile, including, where necessary, the source of funds.

Where a covered person is unable to comply with the relevant CDD measures, it shall (a) refuse

to open an account, commence business relations or terminate the business relationship or perform the transaction; and (b) consider filing a suspicious transaction report (STR) in relation to the customer.

In cases where a covered person forms a suspicion of ML/TF and associated unlawful activities, and reasonably believes that performing the CDD process will tip-off the customer, the covered person need not pursue the CDD process, but should file an srR, closely monitor the account, and review the, business relationship.

b. A covered person shall be required to undertake customer due diligence when:

- (1) It establishes business relations with any customer;
- (2) It undertakes any occasional but relevant business transaction for any customer who has not otherwise established relations with the covered person;
- (3) There is a suspicion of ML or TF; or
- (4) There is doubt about the veracity or adequacy of previously obtained customer identification data.

c. *"Business relations"* means the opening or maintenance of an account or the provision of financial advice by the covered person to a customer.

d. *"Relevant business transaction"* shall refer to:

- (1) A transaction with a value exceeding P100,000, except money changing or remittance transactions;
- (2) Two (2) or more transactions believed to be linked and with an aggregate value exceeding P100,000; or
- (3) In relation to remittance and money changing transactions, any transaction or two (2) or more transactions believed to be linked, with an aggregate value exceeding P5,000.00

For this purpose, covered persons should have appropriate system to identify and determine occasional customer or transaction.

e. *For existing customers.* Covered persons shall apply CDD requirements to existing customers on the basis of materiality and risk, and conduct due diligence on existing relationship at appropriate times, taking into account CDD measures previously undertaken as well as the adequacy of information and documents obtained.

**Customer acceptance and identification policy.** Every covered person shall develop clear, written

and graduated customer acceptance and identification policies and procedures that will ensure that the financially or socially disadvantaged are not denied access to financial services while at the same time prevent suspicious individuals or entities from opening an account or establishing a relationship. A covered person shall formulate a risk-based and tiered customer acceptance, identification and retention policy that involves reduced customer due diligence (CDD) for potentially low risk clients and enhanced CDD for higher risk accounts.

- a. *Criteria for type of customers: low, normal and high risk; Standards for applying reduced, average and enhanced due diligence.* Covered persons shall specify the criteria and description of the types of customers that are likely to pose low, normal or high ML/TF risk to their operations, as well as the standards in applying reduced, average and enhanced due diligence, including a set of conditions for the denial of account opening or services.

Enhanced due diligence shall be applied to customers that are assessed by the covered person or under this Part as high risk for ML/TF. For customers assessed to be of low risk such as small account balance and transactions, a covered person may apply reduced due diligence. Some entities may likewise be considered as low risk clients, e.g., banking institutions, trust entities and QBs authorized by the Bangko Sentral to operate as such and publicly listed companies subject to regulatory disclosure requirements.

In designing a customer acceptance and risk profiling policy, 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;
- (3) Public or high profile position of the customer or its directors/trustees, stockholders, officers and/or authorized signatory;
- (4) Country of origin and residence of operations or the fact that a customer came from a high risk jurisdiction;
- (5) The existence of ST indicators;
- (6) Watchlist of individuals and entities engaged in illegal activities or terrorist related activities as circularized by the Bangko Sentral, 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 person may deem reasonable or necessary to consider in assessing the risk of a customer to ML/TF.

In assessing the risk profile of customers which are juridical entities, the covered person should also consider the financial profile and other relevant information of the active authorized signatories.

The covered person shall document the risk profiling results as well as how a specific customer was profiled and what standard of CDD (reduced average or enhanced) was applied.

*b. Enhanced due diligence (EDD).* Whenever EDD is applied as required by this Part, or by the covered person's customer acceptance policy, or where the risk of ML/TF are higher, the covered person shall do all of the following, in addition to profiling of customers and monitoring of their transactions:

- (1) Gather additional customer information and/or identification documents, other than the minimum information and/or documents required for the conduct of average due diligence as enumerated in this Section on (*Customer identification*) and Sec. 924.

(a) In case of individual customers:

- (i) supporting information on the intended nature of the business relationship/source of funds/source of wealth (such as financial profile, ITR, Loan Application, Deed of Donation, Deed of Sale, etc.);
- (ii) reasons for intended or performed transactions;
- (iii) list of companies where he is a stockholder, director, officer, or authorized signatory;
- (iv) other relevant information available through public databases or internet; and
- (v) a list of banks where the individual has maintained or is maintaining an account.

(b) In case of entities:

- (i) prior or existing bank references;
- (ii) the name, present address, nationality, date of birth, nature of work, contact number

and source of funds of each of the primary officers (e.g., President, Treasurer);

(iii) volume of assets, other information available through public databases or internet and supporting information on the intended nature of the business relationship, source of funds or source of wealth of the customer (ITR, Audited Financial Statement, Loan Application, Deed of Donation, Deed of Sale, etc.); and

(iv) reasons for intended or performed transactions

- (2) Conduct validation procedures in accordance with this Section on (*Customer acceptance and identification policy*) on any or all of the information provided;
- (3) Secure senior management approval to commence or continue business relationship/transacting with the customer;
- (4) Conduct enhanced ongoing monitoring of the business relationship, by, among others, increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination;
- (5) Require the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards, where applicable; and
- (6) Perform such other measures as the covered person may deem reasonable or necessary.

Where additional information cannot be obtained, or any information or document provided is false or falsified, or result of the validation process is unsatisfactory, the covered person shall deny banking relationship with the customer without prejudice to the reporting of a suspicious transaction to the AMLC when circumstances warrant.

c. *Minimum validation procedures for EDD.* The procedures performed must enable the covered person to achieve a reasonable confidence and assurance that the information obtained are true and reliable.

Validation procedures for individual customers shall include, but are not limited to, the following:

- (1) Confirming the date of birth from a duly authenticated official document;
- (2) Verifying the address through evaluation of utility bills, bank or credit card statement,

sending thank you letters, or other documents showing address or through on-site visitation;

- (3) Contacting the customer by phone or e-mail;
- (4) Determining the authenticity of the identification documents through validation of its issuance by requesting a certification from the issuing authority or by any other effective and reliable means; or
- (5) Determining the veracity of the declared source of funds.

For corporate or juridical entities, verification procedures shall include, but are not limited to, the following:

- (1) Validating source of funds or source of wealth from reliable documents such as audited financial statements, ITR, bank references, etc.;
  - (2) Inquiring from the supervising authority the status of the entity;
  - (3) Verifying the address through on-site visitation of the company, sending thank you letters, or other documents showing address; or
  - (4) Contacting the entity by phone or e-mail.
- d. *Reduced due diligence.* Where lower risks of MWF have been identified, through an adequate analysis of risk by the covered person and based on the results of the institutional risk assessment, reduced due diligence procedures may be applied commensurate with the lower risk factors. The reduced due diligence procedures shall not be applied in cases of suspicion of higher ML/TF risk scenarios.

Whenever reduced due diligence is applied as provided in this Part or in the covered person's customer acceptance policy, the following rules shall apply:

- (1) For individual customers, a covered person may open an account/establish relationship under the true and full name of the account owner/s or customers upon presentation of an acceptable identification card (ID) or official document as defined in this Part or other reliable, independent source documents, data or information: *Provided*, That, for accounts used purely for digital or electronic payments, the covered person may define appropriate reduced due diligence procedures provided that ML/TF risks are effectively managed.

- (2) For corporate, partnership, and sole proprietorship entities, a covered person may open an account under the official name of these entities by presenting a Board Resolution duly certified by the Corporate Secretary, or equivalent document, authorizing the signatory to sign on behalf of the entity, obtained at the time of account opening.

Verification of the identity of the customer, beneficial owner or authorized signatory can be made after the establishment of the business relationship

- e. *Restricted account.* To promote financial inclusion and to ensure that the micro-business owners and the low-income households are able to manage their finances through the financial system, customers who may not be able to provide any of the required information or valid reasons or any valid identification document under this Section on *Customer identification* may be allowed to open a restricted account with a covered person, provided:

- (1) the aggregate credits in a year shall not exceed P100,000; and
- (2) the account shall not be allowed to receive/send foreign remittances.

In lieu of a valid ID, the covered person 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 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 person a proof of application for a valid ID.

The covered person 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.

**Customer identification.** Covered persons shall establish and verify the true identity of their customers based on official document as defined in this Part or other reliable, independent source documents, data or information.

- a. Minimum information/documents required:

- (1) *New individual customers.* Covered persons 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.

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 confirming these information with the official or valid identification documents:

- (a) name of 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 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;

(2) *New juridical persons.* A covered person shall develop a systematic procedure for identifying corporate, partnership and sole proprietorship entities, as well as their stockholders/ partners/owners, directors, officers and authorized signatories. It 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.

Unless otherwise stated in this Part, average due diligence requires that the covered person 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) Certificates of Registration issued by the Department of Trade and Industry (DTI) for single proprietors, or by the Securities and Exchange Commission (SEC) for corporations and partnerships, and by the Bangko Sentral for money changers/foreign exchange dealers and remittance agents and transfer companies;
- (ii) Secondary license or certificate of authority issued by the supervising authority or other government agency;
- (iii) Articles of incorporation/partnership;
- (iv) Latest General Information Sheet which lists the names of directors/trustees/partners, principal stockholders owning at least twenty percent (20%) of the outstanding capital stock and primary officers such as the president and treasurer;
- (v) Board or Partners' resolution duly certified by the corporate/partners' secretary, or other equivalent document, authorizing the signatory to sign on behalf of the entity; and
- (vi) For entities registered outside of the Philippines, similar documents and/or information shall be obtained, duly authenticated by a senior officer or the designated officer of the covered person assigned in the country of registration; in the absence of said officer, the documents should be authenticated by the Philippine Consulate, company register or notary public, where said entities are registered.

(3) *For legal arrangement (e.g., Trust).* The following must be obtained:

- (a) Name of legal arrangement and proof of existence;
- (b) Address and country of establishment;
- (c) Nature, purpose and objects of the legal arrangement;
- (d) The names of the settlor, the trustee, the trustor, the protector, if any, the beneficiary and any other natural person exercising ultimate effective control over the legal arrangement;
- (e) Description of the purpose/activities of the legal arrangement;
- (f) Expected use of the account; and
- (g) Amount, number, type, purpose and frequency of the transaction expected.

In addition, the following rules shall apply for trustees:

- (a) *trustees of any express trust* shall obtain and hold adequate, accurate, and current information on the identity of the trustor/settlor/grantor, the trustee, the beneficiary or

class of beneficiaries, and any other natural person exercising ultimate effective control over the trust

Covered persons shall likewise obtain sufficient information, such as the full name, place and date of birth or date of registration of the beneficiary/ies of these trusts, or of similar legal arrangements. This is to ensure that covered persons will be able to identify and verify the identity of the beneficiary at the time of the payout or at the time of the exercise by the beneficiary of its vested rights.

- (b) *trustees of any trust* shall hold basic information on other regulated agents of, and service providers to, the trust, including investment advisors or managers, accountants, and tax advisors;
- (c) trustees shall disclose their status when forming a business or professional relationship, or in carrying out an occasional transaction above the threshold under Item “d” of this Section; and
- (d) trustees shall make available to competent authorities, to the extent allowed by law, information on the beneficial ownership and the assets of the trust to be held or managed under the terms of the business or professional relationship.

(4) *Identification and Verification of Agents and Authorized Representatives.* Covered persons shall verify that any person purporting to act on behalf of a customer is so authorized and shall identify and verify the identity of that person.

For this purpose, the covered person shall obtain the name, address and citizenship or nationality of agents and authorized representatives.

b. Customer verification process. Covered persons shall verify the identity of the customer before or during the course of establishing a business relationship, or conducting transactions for occasional customers. They may complete the verification process after the establishment of the business relationship: *Provided, That:*

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

c. Valid identification documents.

- (1) Customers and the authorized signatory/ies of a corporate or juridical entity who engage in a financial transaction with covered person for the first time shall be required to present official identification document which shall include any of the official documents as defined in this Part or other identification information which can be verified from reliable, independent source, documents, data or information, such as third-party verified customer information database.
- (2) 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. Whenever it deems necessary, a covered person may accept other IDs not provided herein: *Provided*, That it shall not be the sole means of identification.

In case the identification document presented does not bear any photo of the customer or authorized signatory, or the photo-bearing ID or a copy thereof does not clearly show the face of the customer or authorized signatory, a covered person may utilize its own technology to take the photo of the customer or authorized signatory.

*Relief in case of calamity.* In case of a disastrous calamity and subject to a declaration by the Bangko Sentral on the applicability of this relief, any requirement for the presentation of valid ID shall be relaxed, subject to the following conditions:

- (a) The amount of transactions shall not exceed P50,000.00 per day;
- (b) The customer is either a permanent or temporary resident or who conducts business in a severely affected area which has been declared to be under a state of calamity by a competent authority;
- (c) The customer shall submit a written certification, which need not be notarized, that he/she is a victim of the subject disastrous calamity and has lost his/her valid IDs; and
- (d) The customer's account activities shall be subject to strict monitoring by the covered person to identify potential abuse of the relaxed requirement and any STs shall be reported to the AMLC within the prescribed period.

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.

d. *Face-to-Face contact.* Covered persons shall conduct face-to-face contact and/or personal interview at the commencement of the relationship. Face-to-face contact may likewise be conducted as soon as reasonably practicable so as not to interrupt the normal conduct of business, taking into account the nature of the product, type of business and the risks involved: *Provided, That,* there are policies and procedures to address any specific risk associated with the same including a clear definition of instances when it will be allowed.

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 the entire procedure is documented.

e. *Outsourcing of the customer identification and verification procedures.* Subject to existing rules on outsourcing of specified banking activities, a covered person may, without prior Monetary Board approval, outsource to a counterparty, which may or may not be a covered person as herein defined, the customer identification and verification procedures under Items “a”, “b” and “d” above: *Provided,* That the ultimate responsibility for knowing the customer, keeping the identification documents, and managing attendant risks shall rest with the covered person and the following conditions are complied with

For covered person counterparty:

- (1) There is a written service level agreement approved by the board of directors or senior management of the covered persons and its counterparty;
- (2) The counterparty has a reliable and acceptable customer identification system and training program in place.

For non-covered person counterparty:

- (1) All conditions required for covered person counterparty;
- (2) The covered person outsourcing the activity shall ensure that the employees or representatives of the counterparty gathering the required information/documents of, and/or conducting face-to-face contact with, the customer undergo equivalent training program as that of the covered person’s own employees undertaking a similar activity; and
- (3) The covered person shall monitor and conduct annual review of the performance of the counterparty to determine whether or not to continue with the arrangement.

All identification information and/or documents shall be turned over within a period not

exceeding ninety (90) calendar days to the covered person, which shall carefully review the documents or information and conduct the necessary risk assessment of the customer. The covered person may, however, include in the coverage of the outsourcing agreement the safekeeping of the documents gathered subject to the condition that customer identification documents shall be made available to the covered person or to the competent authorities within three (3) banking days from the date of request.

f. *Third party reliance.* A covered person may rely on third parties to perform the CDD procedures under Item “(a) 1 to 3” of Sec. 921 (*Customer due diligence*) subject to the following rules:

(1) *Where the third party is a covered person specifically defined by this Part and as generally defined by AMLA, as amended, and its RIRR* - The covered person shall obtain from the third party a written sworn certification containing the following:

(a) The third party has conducted the prescribed customer identification procedures in accordance with this Part and its own MLPP, including the face-to-face contact requirement, to establish the existence of the ultimate customer and has in its custody all the minimum information and/or documents required to be obtained from the customer; and

(b) The relying covered person shall have the ability to obtain identification documents from the third party upon request without delay.

(2) *Where the third party is a financial institution operating outside the Philippines that is other than covered persons referred to in Item “(1)” above but conducts business operations and activities similar to them* - All the contents required in the sworn certification mentioned in Item “(1)” above shall apply, with the additional requirement that the laws of the country where the third party is operating has equal or more stringent customer identification process requirement and that it has not been cited in violation thereof.

When determining in which countries the third party that meets the requirements above can be based, covered persons should consider available information on the level of country risk.

(3) For both Items “(1)” and “(2)” above, it shall, in addition to performing normal due diligence measures, do the following:

(a) Gather sufficient information about the third party and the group to which it belongs to understand fully the nature of its business and determine from publicly available information the reputation of the institution and the quality of supervision, including

whether or not it has been subject to ML or TF investigation or regulatory action. Satisfy itself that the third party is regulated, and supervised or monitored for, and has measures in place for compliance with CDD and record keeping requirements;

(b) Document the respective responsibilities of each institution; and

(c) Obtain approval from senior management at inception of relationship before relying on the third party.

(4) Covered persons may rely on a third party that is part of the same financial group under the following circumstances:

(a) the group applies CDD, record-keeping and MTPP requirements;

(b) the implementation of CDD and record-keeping requirements, and the MTPP is supervised at a group level by a competent authority, such as a Group Compliance Officer; and

(c) any higher country risk is adequately mitigated by the group's AML/CFT policies.

A Bangko Sentral-accredited custodian may likewise rely, in accordance with this Part, on the face-to-face contact and gathering of minimum information performed by the seller or issuer of securities or by the global custodian to establish the existence and full identity of the customer: *Provided*, That the said third party has an equivalent customer identification requirements.

Notwithstanding the foregoing, the ultimate responsibility for identifying the customer still lies with the covered person relying on the third party.

In cases where the customer is assessed as high risk by the third party, the covered person shall conduct its separate enhanced due diligence procedure.

g. Trustee, nominee, agent or intermediary account. Where (1) an account is opened by; (2) relationship is established through; or (3) any transaction is conducted by, a trustee, nominee, agent or intermediary, either as an individual or through a fiduciary relationship or similar arrangements, the covered person shall establish and record the true and full identity and existence of both the (1) trustee, nominee, agent or intermediary; and (2) trustor, principal, beneficial owner or person on whose behalf the account/ relationship/transaction is being opened/established/conducted. The covered person shall determine the true nature of the parties' capacities and duties by obtaining a copy of the written document evidencing their relationship and apply the same standards for assessing the risk profile and determining the

standard of due diligence to be applied to both.

In case of several trustors, principals, beneficial owners, or persons on whose behalf the account is being opened/ relationship is being established, where the trustee, nominee, agent or intermediary opens a single account but keeps therein sub-accounts that may be attributable to each trustor, principal, or beneficial owner, the covered person shall, at the minimum, obtain the true and full name, place and date of birth or date of registration, as the case may be, present address, nature of work or business and source of funds as if the account was opened by them separately. Where the covered person is required to report a CT or circumstances warrant the filing of an ST, it shall obtain such information on every trustor, principal, beneficial owner, or person on whose behalf the account is being opened in order that a complete and accurate report may be filed with the AMLC.

In case a covered person entertains doubts as to whether the trustee, nominee, agent, or intermediary is being used as a dummy in circumvention of existing laws, it shall apply enhanced due diligence in accordance with this Section on *Customer acceptance and identification policy* and file an ST report, if warranted.

- h. *Prohibited accounts.* A covered person shall maintain accounts only in the true and full name of the account owner. The provisions of existing law to the contrary notwithstanding, anonymous accounts, accounts under fictitious names, numbered checking accounts and all other similar accounts shall be absolutely prohibited.

***On-going monitoring of customers, accounts and transactions.***

- a. Covered persons 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. The covered person shall document the actions taken in connection with updating of customer's records/information, and accordingly update customer's risk profile.

Covered persons shall establish a system that will enable them to understand the normal and reasonable account or business activity of customers to ensure that the customers' accounts and transactions are consistent with their knowledge of the customers, and the latter's commercial activities, risk profile, and source of funds and detect unusual or suspicious patterns of account activity. Thus, a risk-and-materiality-based on-going monitoring of customer's accounts and transactions, including periodic sanction screening, should be part of a covered person's customer due diligence.

b. Enhanced due diligence. Covered persons shall examine the background and purpose of all complex, unusually large transactions, all unusual patterns of transactions, which have no apparent economic or lawful purpose, and other transactions that may be considered suspicious. Covered persons shall apply enhanced due diligence on the customer in accordance with this Section on *Customer acceptance and identification policy* if they acquire information in the course of customer account or transaction monitoring that:

- (1) Raises doubt as to the accuracy of any information or document provided or the ownership of the entity;
- (2) Justifies reclassification of the customer from low or normal risk to high risk pursuant to this Part or by their own criteria; or
- (3) Indicates that any of the circumstances for the filing of an ST report exists such as, but not limited to, the following:
  - (a) Transacting without any underlying legal or trade obligation, purpose or economic justification;
  - (b) Transacting an amount that is not commensurate with the business or financial capacity of the customer or deviates from his profile;
  - (c) Structuring of transactions in order to avoid being the subject of covered transaction reporting; or
  - (d) Knowing that a customer was or is engaged in any unlawful activity as herein defined.

If the covered person:

- (1) fails to satisfactorily complete the enhanced due diligence procedures; or
- (2) reasonably believes that performing the enhanced due diligence process will tip-off the customer,

it shall file a ST report, and closely monitor the account and review the business relationship.

***Non-discrimination against certain types of customers.*** The provisions of this Part shall not be construed or implemented in a manner that will discriminate against certain customer types, such as PEPs, as well as their relatives, or against a certain religion, race or ethnic origin, or such other attributes or profiles when used as the only basis to deny these persons access to the covered person's services. In this regard, covered persons shall have appropriate policies and procedures to ensure non-discrimination against certain customer types when implementing AML/CFT regulations. Covered persons who will commit said discriminatory act shall be subject to appropriate sanctions provided under existing laws and regulations.