MONEY LAUNDERING AND TERRORIST FINANCING PREVENTION PROGRAM (MTPP)

(REVISED AS OF 27 AUGUST 2025)

Version 7.0

Version History

Version #	Date	Author/Editor	Version/Revision Comments
7.0	August 27, 2025	Jemelyn N. Duhilag Francis G. Yap	Amendments/additions include: 1. Part VI. Customer On-Boarding Due Diligence (CODD) • Added provision on the use of multi-pronged approach to determine Ultimate Beneficial Owner (UBO). • Added elements of beneficial ownership due diligence 2. Part VII. On-Going Monitoring of Customers • Updated TEDD Approval Matrix. Included the authority of the BOD Division Head even if not a Senior Officer to approve Transaction Enhanced Due Diligence (TEDD). • Added Real-time Transaction Monitoring Through Fraud Management System (FMS). • Updated Transaction Monitoring Function of Base60 and participants in the Alerts Management. 3. Part IX. Customer Risk Assessment • Included repeat subjects of STRs in the coverage of Deposit Account/ Client Account AML Exit Policy. • Included accounts with KYC deficiencies and failure to meet the commitment date in the coverage of Deposit Account/ Client Account AML Exit Policy. 4. Part XII. Handling of Freeze Order, Bank Inquiry and Other Orders • Incorporated policy on the Anti-Financial Account Scamming Act

6.0	October 17, 2024	Jemelyn N. Duhilag Francis G. Yap	Amendments/additions include: 1. Part II. Definition of Terms • Included Transactors. • Updated definition of terms under 2.2 Targeted Financial Sanctions. 2. Part V. General Provisions • Updated the members of the AML Committee. 3. Part VI. Customer On-boarding Due Diligence • Added Transactor as a customer and subject of risk profiling. • Added mandatory information for Transactors. • Added Policy on Deferment of Documentary Submission • Added Transactor as subject of watchlist screening. • Added definition of "business" for Designated Non-Financial Business and Professions (DNFBPs) • Added Due Diligence Questionnaire (DDQ), Sworn Statement of Non-Engagement requirement for DNFBPs • Added provision to tag DNFBPs as such in the system. • Added indicators to determine if a customer qualifies as DNFBP. • Added Annex W Framework for Gaming and Gaming-related Clients • Added provision on validation of names via source link of the news prior to uploading/updating. 4. Part VII. On-going Monitoring of Customers

			• Added pre-transaction monitoring controls for Transactors. • Revised approving authority for Cross-border remittances. • Added approving authority for Transaction Enhanced Diligence for non-crossborder transactions. • Revised TEDD thresholds for Cross-border Remittances. • Revised Annexes AC and AD Revised Alerts Management Guidelines for Compliance Investigators and Approvers; for Branches and Business Units 5. Part VIII. Sanctions Program and Targeted Financial Sanctions • Added provisions to align with BSP Circular No. 1182, Series of 2023. 6. Part X. Institutional Risk Assessment (IRA) • Added Annex AJ – Parameters/Criteria in Evaluating the Strength of Controls. • Added Risk Operations Department Head as the assigned officer to review the IRA independent from the makers. • Added Internal Audit Division to also review the IRA report during their regular audit examination. • Revised low risk assessment in the IRA to be conducted every 2 years. 7. Part XI. Covered and Suspicious Transaction Reporting • Added provision that RISA Form is no longer required if the suspicious transaction or activity is discovered by AML Compliance Department.

			• The endorser of RISA is changed from AML Compliance Department Head to AMLCOM Secretariat • Revised STR process flow to not require RISA Form if the RISA is initiated by AML Compliance Department. • Added information sharing for suspicious transaction reporting between and among Customer Experience Management Department, Governance and Regulatory Compliance Department and AML Compliance Department. 8. Part XII. Handling of Freeze Order, Bank Inquiry and Other Orders • Incorporate provision on the review of the status of accounts with freeze order to be conducted semi-annually.
5.0	August 17, 2023	Jemelyn N. Duhilag Francis G. Yap	Amendments/additions include: 1. Part II. Definition of Terms • Included Electronic Know Your Customer (e-KYC) 2. Part VI. Customer On- Boarding Due Diligence • Revised Minimum Mandatory Information for individuals to include PhilSys Number as mandatory and changed the requirement on TIN and SSS/GSIS No. to TIN or SSS/GSIS No. • Added various formats of the Philippine National ID as acceptable ID. • Added provision for customer scrubbing under Negative Watchlist Verification Guidelines.

			• Added Ultimate Beneficial Owners (UBOs) as mandatory subjects of watchlist screening and scrubbing. • Revised provision under UBO policy. UBO Determination from: "The use of the UBO Determination Form applies only to partnership and corporation (including special types of corporations)." to: "The use of the UBO Determination Form does not apply to individuals and sole proprietorships". • Added provision and process on scrubbing of UBOs under UBO policy. • Added Electronic Know Your Customer (e-KYC) policy. • Revised OGB and MSB Guidelines to include documentary requirements checklist and list of deferrable documents and require Group Head approval for account opening/maintenance regardless of the purpose of the account. • Added provision for annual review of MSB clients under MSB Guidelines. • Added Documentary Requirements Checklist under Cash-Intensive Business Guidelines. • Revised automatic TEDD requirement for transactions involving high risk Philippine Areas to only remittance transactions bound for any high risk Philippine area. 3. Part VII. Ongoing Monitoring of Customers • Added provision to require watchlist screening for payees of manager's

			checks who are non-accountholders of the Bank. • Added thresholds for automatic TEDD requirements for MC transactions and foreign exchange transactions. • Added provision for Whitelisting of Alert 4. Part IX. Customer Risk Assessment • Revised policy on co-mingling of accounts to not allow co-mingling regardless of whether the business is a covered institution or not. • Added Deposit Account / Client Account AML Exit Policy. • Revised Determination and Filing of Suspicious Transaction Report to align with the 2021 AMLC Registration and Reporting Guidelines (ARRG). • Amended requirement of Money Laundering Suspicion Evaluation Sheet (MLSES) for ratification of STR approvals in the Minutes of the Meeting. 5. Part XII. Handling of Freeze Order, Bank Inquiry and Other Orders • Revised policy on handling of bank inquiry to utilize the DIGICUR system. 6. Part XV. Sanctions and Penalties • Added Inter-Agency Council Against Trafficking or IACAT (for trafficking-in-persons cases) as one of the possible

			regulating agencies to impose administrative sanctions on the Bank. 7. Part XVI: AML Training and Information Dissemination • 2022 Revised Implementing Guidelines in the AMLA e-Learning Course 8. Annexes • Updated list of acceptable valid IDs • Added Diplomatic Visa under Guidelines on Acceptable IDs of Foreign Nationals • Added MSB, OGB, and CIB Documents Checklist • Added Standard Template on Annual Analysis of MSB Clients • Revised Enhanced Due Diligence Form for Gaming and Gaming-related Clients • Revised Ultimate Beneficial Ownership (UBO) Determination Form • Added Guidelines on Whitelisting of Clients from Alerts Generation • Added Revised Implementing Guidelines for the AMLA e-Learning Course • Results of 2022 Institutional Risk Assessment
4.0	June 7, 2022	Jemelyn N. Duhilag Francis G. Yap Christine Michelle N. Morales	Amendments/additions include: 1. Part II. Definition of Terms • Included Offshore Gaming Operators (OGOs) and Real Estate Developers and

			Brokers in Designated Non-Financial Businesses and Professions (DNFBPs) per R.A. 11521 • Added CTR threshold of P7,500,000.00 cash for Real Estate Developers and P7,500,000.00 cash for Brokers, respectively, per 2021 ARRG • Added 2 new predicate crimes, Violation of Strategic Trade Management Act and Violation of the National Internal Revenue Code, in the list of unlawful activities per R.A. 11521 • Included all related definitions pertaining to Targeted Financial Sanctions 2. Part V. General Provisions • Removed AML Compliance Department Head as regular member of the AMLCOM • Removed AML Advisory in the category of AML Issuances and merged it with AML Bulletin 3. Part VI. Customer On- Boarding Due Diligence • Added PhilID as one of the Acceptable Official Identification Documents • Harmonized Policy on ID Validation by way of Certification - Official Identification Documents & Average Due Diligence • Added Guidelines on Negative Watchlist Verification

			• Added Time Limits of PEP Status & PEP Declassification • On-Boarding Policy for DNFBPs • Revised Guidelines on Accepting Clients Engaged in Gaming or Gaming-Related Activities • Guidelines on Accepting Clients Engaged in Cash-Intensive Business • Guidelines in Handling Clients and Transactions from High Risk Philippine Areas 4. Part VII. Ongoing Monitoring of Customers • Policy on the TAT of TEDD for Inter-Branch Outward Remittance • Guidelines on Negative News Reporting - Bottom-Up Approach 5. Added Part VIII. Sanctions Program and Targeted Financial Sanctions 6. Part IX. Customer Risk Assessment • Average Due Diligence • Risk Re-Assessment • Prevalence of Unusually Large Transaction Alerts 7. Part XI. Covered & Suspicious Transaction Reporting • Repeated Filing of STR to a Particular Customer

			• Updated List of Low Risk Transactions per 2021 ARRG 8. Part XII. Handling of Freeze Order, Bank Inquiry and other Orders • Handling of Customers Subject of Freeze Order 9. Part XIII. Customer Records Updating and Record Keeping • Guidelines on Digitization of Customer Records.
3.0	June 25, 2020	Rechie W. Lastimoso	Amendments/revisions include: 1. Part II. Definition of Terms • Moved from 1.3 of Part I. Introduction 2. Part III. Money Laundering and Terrorism Financing • Expanded 1.4 – Basic Principles and Policies of Anti-Money Laundering and Combating of Financing of Terrorism 3. Part IV. Monitoring, Enforcement, and Supervision • Moved from 1.5 and 1.6 of Part I. Introduction 4. Part V. General Provisions • Expanded from Part II. Compliance General Provisions

			5. Part VI. Customer On-boarding Due Diligence (CODD) • Moved and expanded from Part III. Know-Your-Customer (KYC) Policy 6. Part VIII. Customer Risk Assessment • Moved from Part V. Customer Risk Assessment Methodology and Part VI. Customer Due Diligence (CDD) 7. Part XI. Handling of Freeze Order, Bank Inquiry, and Other Orders • Moved from Part IX. Handling of Freeze Order and Part X. AMLC and BSP Authority to Examine Deposits and Investments 8. Part XII. AML Training and Information Dissemination • Renamed from "Record Keeping and Retention" 9. Part XV. AML Training and Information Dissemination • Expanded from Part XII. Training Program
2.0	April 25, 2019	Rechie W. Lastimoso	Amendments/revisions include: 1. Introduction • Declaration of Policy - Cited provision on BSP Circular No. 706, as amended by Circular No. 950 and 1022 or the Anti-

			Money Laundering Rules and Regulations • Definition of Terms - Added definitions for matters related to the following: a. Alerts Management b. AMLC Transaction Reporting c. Terrorism Financing d. Ultimate Beneficial Owner (UBO) • Monitoring, Enforcement and Supervision - A new provision with contents defining the regulatory agencies covering the Bank 2. Compliance General Provisions • The AML Committee (AMLCOM) Charter a. Strengthened the scope of authority of the AMLCOM b. Itemized the responsibility of the AMLCOM Secretary c. Added provisions on email confirmation/approval in lieu of physical meetings on AML related issues d. Included provision on voting requirements and amendments • Know-Your-Customer Responsibility - A new provision reinforcing the Bank's ultimate responsibility to KYC 3. Know-Your-Customer (KYC) Policy • Who is the Customer - A new provision defining who are the customers/clients

			• Customer Acceptance and Identification Policy - A new provision defining the criteria on customer acceptance and identification that shall be strictly observed prior to on-boarding • Customer On-boarding Policy - A new provision discussing the following customer due diligence procedures upon on-boarding: a. Conduct Face-to-face Contact b. Gathering of Information and Identification Documents c. Watchlist and PEP List Screening d. Customer Risk Profiling e. Conduct of the Required Due Diligence • Denial of Business Relationship - A new provision wherein the Bank has the option to deny banking relationship if the client is unable to comply with the CDD measures • Private Banking/Wealth Management Account - A new provision on Guidelines for CBC PBG referred accounts • Ultimate Beneficial Ownership (UBO) - A new provision defining the ultimate beneficial ownership pursuant to BSP Circular No. 1022 • Politically Exposed Person (PEP) a. Added provision itemizing the persons considered to be politically exposed by position b. Revised the coverage on relatives of PEP from 1st degree to 2nd degree of consanguinity

			or affinity pursuant to BSP Circular No. 1022 • Default High Risk Customers - Added provision enumerating customers considered as High Risk by default in details regardless of the total risk rating score in ECRAF 4. On-going Monitoring of Customers - A new provision demonstrating the stages of the on-going monitoring process of customers with whom the bank has a business relationship pursuant to BSP Circular No. 1022, to wit: • Pre-transaction Monitoring Controls • Post-transaction Monitoring Controls • Monitoring of Negative News Report • Internal Watchlist Monitoring • Sanctions List Monitoring • Updating of Customer Records Base60 AML System - Indicated/discussed the different transaction alert scenarios, the participants in Alerts Management, and alerts disposition 5. Bank-wide ML/TF Risk Assessment - A new provision on the assessment methodology of the Bank in assessing the ML/TF Risk arising from customers, countries or geographic areas of operations and customers, products, services, transactions or delivery

			Risk assessment process is divided into the following: a. Understanding the Business b. Determination and Impact of Inherent ML/TF Risk c. Measurement and Evaluation of ML/TF Controls d. Evaluation of Residual ML/TF Risk e. Propose Action Plans on ML/TF Control Gaps 6. Record Keeping and Retention • Digitization of Customer Records - The Bank shall implement the digitization of customer records using the Electronic Document Management System (EDMS) 7. Sanctions and Penalties • Imposition of Administrative Sanctions - Added a provision on the non-compliance on digitization of customer records pursuant to BSP Circular Letter No. CL-2019-002 8. Annexes - Added the following annexes: • R.A. 10168 (Terrorism Financing Prevention and Suppression Act) • Enhanced Customer Risk Assessment Form V.2.0 • ECRAF Implementing Guidelines

			• Suspicious Transaction Incident Report (STIR) Form – Individual and Corporate • Money Laundering Suspicion Evaluation Sheet (MLSES) • Ultimate Beneficial Owner (UBO) Disclosure Form

Table of Contents

PART I
INTRODUCTION

PART I: INTRODUCTION

1.1 DECLARATION OF POLICY

The China Bank Savings Inc. adopts the AML Manual that shall be officially called the Money Laundering and Terrorist Financing Prevention Program (MTPP) in compliance with Section 911 of the Manual of Regulations for Banks and Circular Number 706 or the Anti-Money Laundering Rules and Regulations as amended by Circulars 950 and 1022. This is also in adherence with the policy of the State to (a) protect the integrity and confidentiality of bank accounts and to ensure that the Bank shall not be used as a money laundering site and conduit for the proceeds of an unlawful activity as hereto defined; and (b) to protect life, liberty and property from acts of terrorism and to condemn terrorism and those who support and finance it. This shall serve as guide for all units of China Bank Savings, Inc. (CBSI) when dealing with clients in processing their transactions to ensure compliance with R.A. 9160 or Anti-Money Laundering Act (AMLA) of 2001, as amended by R.A. 9194, R.A. 10167, R.A. 10365, R.A. 10927, RA 11521 and its Revised Implementing Rules and Regulations. The contents of this MTPP also ensure compliance with R.A. 10168 or The Terrorism Financing Prevention and Suppression Act of 2012 and R.A. No. 11479 or the Anti-Terrorism Act of 2020. In the same manner, this MTPP includes operational policies and procedures adopted by the Bank to counter the threat of money laundering and terrorist financing from its operations. It also provides the tools for proper risk management on Money Laundering and Terrorist Financing.

1.2 SCOPE OF APPLICATION

This Manual shall apply to all branches and business units of China Bank Savings, Inc.

PART II
DEFINITION OF TERMS

PART II: DEFINITION OF TERMS

2.1 GENERAL DEFINITION OF TERMS

1. **Anti-Money Laundering** – is a term mainly used in the financial and legal industries to describe the legal controls that require financial institutions and other regulated entities to prevent or report money laundering activities.

2. **Alert** – transaction or group of transactions flagged by the AML system that meet the established KYC or Transaction alert scenarios or parameters instituted to detect potential money laundering activities.

3. **Beneficiary Institution** – refers to the entity that will pay out the money to the beneficiary and can either be: (a) a covered institution as specifically defined by the AMLA, as amended, and its IRR and BSP/AMLC regulations, or (b) a financial institution operating outside the Philippines that is other than the covered institutions referred to in (a) but conducts business operations and activities similar to them.

4. **Beneficial Owner** – or Ultimate Beneficial Owner (UBO) refers to a natural person(s) who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being conducted. It also includes persons who exercise ultimate effective control over a legal person or arrangement.

5. **Board of Directors** – refer to directors duly elected by the stockholders or elected to fill vacancies in the board of directors which exercises corporate powers, conducts the business and controls all the resources of the institution.

6. **Designated Non-Financial Businesses and Professions (DNFBP)** – refers to businesses and professions, which are not under the supervision or regulation of the BSP, SEC and IC, that are designated as covered persons under the AMLA, as amended.

7. **Correspondent Banking** – refers to a relationship involving one bank (the correspondent bank) providing banking services to another bank (respondent bank), where the banks carry on activities or business at or through permanent establishments in different countries.

8. **Cross Border Transfer** – refers to any wire transfer where the originating and beneficiary institutions are located in different countries. It shall also refer to any chain of wire transfers in which, at least, one of the financial institutions is located in a different country.

9. **Covered Institution** – refers to banks, off-shore banking units, quasi-banks, trust entities, non-stock savings and loan associations, pawnshops, foreign exchange dealers, money changers, remittance agents, electronic money issuers, and other financial institutions, which under special laws are subject to BSP supervision and/or regulation, including their subsidiaries and affiliates.

10. **Covered Person** – the following are the covered persons under AMLA:

    a) The following financial institutions:

I. Persons supervised and/or regulated by BSP, including their subsidiaries and affiliates, which are also covered persons, supervised and/or 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.

II. 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.

III. 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:

I. Jewelry dealers.

II. Dealers in precious metals and dealers in precious stones.

III. 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.

IV. 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.

V. Casinos, including internet-based casinos and ship-based casinos, with respect to their casino cash transactions related to their gaming operations.

The "Casino Implementing Rules and Regulations of Republic Act No. 10927" shall govern the implementation of the AMLA with regard to casinos, unless, otherwise indicated therein by the AMLC and the AGAs.

VI. Offshore Gaming Operators, as well as their service providers, supervised, accredited or regulated by the Philippine Amusement and Gaming Corporation (PAGCOR) or any Appropriate Government Agency (AGA).

VII. Real Estate Brokers and Developers.

11. **Covered Transaction** – refers to:

a. A transaction in cash or other equivalent monetary instrument involving a total amount in excess of Five Hundred Thousand Pesos (P500,000.00) within one (1) banking day.

b. A transaction with or involving jewelry dealers, dealers in precious metals and dealers in precious stones in cash or other equivalent monetary instrument exceeding One Million pesos (Php1,000,000.00) within one (1) banking day.

c. A casino cash transaction exceeding Five Million Pesos (PHP5,000,000.00) or its equivalent in other currency within one (1) banking day.

d. A cash transaction with or involving real estate developers or brokers exceeding Seven Million Five Hundred Thousand Pesos (P7,500,000.00) or its equivalent in any other currency within one (1) banking day.

12. **CSV File** - is a file in comma-separated value (CSV) format created using the AMLA Reporting System containing covered/suspicious transaction of the Bank and submitted five (5) banking days after the occurrence for CTRs and within the next working day from the date of determination of the suspicious nature of the transaction for STRs.

13. **Customer/Client** – refers to any person or entity that keeps an account, or otherwise transacts business with the Bank. It includes the following: a) beneficial owner, or any natural person who ultimately owns or controls a customer and/or on whose behalf an account is maintained or a transaction is conducted; b) transactors, agents and other authorized representatives of beneficial owners; c) beneficiaries of trusts, investment and pension funds, insurance policies, and remittance transactions; d) persons whose assets are managed by an asset manager; e) trustors/grantors/settlors of a trust; f)any insurance policy holder whether actual or prospective; and juridical person.

14. **Domestic Transfer** – refers to any wire transfer where the originating and beneficiary institutions are located in the same country. It shall also refer to any chain of wire transfers that takes place entirely within the borders of a single country, even though the system used to effect the fund/wire transfer may be located in another country.

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

16. **Freeze Order** – an Order issued by the Court of Appeals upon verified ex parte petition by the AMLC and after determination that probable cause exists that any monetary instrument or property is in any way related to any unlawful activity as defined in the AMLA and its RIRR or to a money laundering offense, directing the concerned covered person or government agency to desist from allowing any transaction, withdrawal, transfer, removal, conversion, concealment, or other disposition of the subject monetary instrument or property which shall be effective immediately. The freeze order shall be effective for six (6) months.

17. **Foreign PEPs** are individuals who are or have been entrusted with prominent public functions by foreign country, such as:

    a. Presidents or Heads of State or Government;
    b. Senior Politicians;
    c. Judicial or Military Officials;
    d. Senior Executives of state owned corporations; and
    e. Important political party officials.

18. **Fund/Wire Transfer** – refers to any transaction carried out on behalf of an originator (both natural and juridical) through a financial institution (originating institution) by electronic means with a view to making an amount of money available to a beneficiary at another financial institution (beneficiary institution). The originator person and beneficiary person maybe the same person.

19. **Intermediary Institution** – refers the entity utilized by the originating and beneficiary institutions where both have no correspondent banking relationship with each other but have established relationship with the intermediary institution. It can either be: (a) a covered institution as specifically defined by the regulations and generally defined by AMLA, as amended and its RIRR or (b) a financial institution operating outside the Philippines that is other than the covered institutions referred to in (a) but conducts business operations and activities similar to them.

20. **KYC Alert** – alert generated by Base60 AML System due to the possible match of the details of the customer with that of the watchlist individual or entity.

21. **Materially linked accounts** – an account or monetary instrument:

    a. All accounts or monetary instruments under the name of the person whose accounts, monetary instruments or properties are subject of the freeze order or an order of inquiry.
    b. All accounts or monetary instruments held, owned or controlled by the owner or holder of the accounts, monetary instruments or properties subject of a freeze order or order of inquiry, whether such accounts are held, owned or controlled singly or jointly with another person.
    c. All "In trust for" (ITF) accounts where either the trustee or trustor pertains to a person whose accounts, monetary instruments or properties are the subject of the freeze order or order of inquiry.
    d. All accounts held for the benefit or in the interest of the person whose accounts, monetary instruments or properties are the subject of the freeze order or order of inquiry.
    e. All accounts under the name of the immediate family or household members of the person, if the amount value involved is not commensurate with the business or financial capacity of the said family or household member.
    f. All accounts of c juridical persons or legal arrangements that are owned or ultimately effectively controlled by the natural person whose accounts, monetary instruments or properties are subject of the freeze order or order of inquiry, or where the latter has ultimate effective control.
    g. All shares or units in any investment accounts and/or pooled funds of the person whose account are subject of the freeze order or order of inquiry.
    h. All other accounts, share, units or monetary instruments that is similar, analogous or identical to any of the foregoing.

22. **Monetary Instrument** – refers to, but is not limited to, the following:

    a. Coins or currency of legal tender of the Philippines, or of any other country;
    b. Credit instruments, including bank deposits, financial interest, royalties, commissions, and other intangible property;
    c. Drafts, checks, and notes;

d. Stocks or shares, participation or interest in a corporation or in a commercial enterprise or profit-making venture and evidenced by a certificate, contract, instrument, whether written or electronic in character, including those enumerated in Section 3 of the Securities Regulation Code;
e. A participation or interest in any non-stock, non-profit corporation;
f. Securities or negotiable instruments, bonds, commercial papers, deposit certificates, trust certificates, custodial receipts, or deposit substitute instruments, trading orders, transaction tickets, and confirmations of sale or investments and money market instruments;
g. Contracts or policies of insurance, life or non-life, contracts of suretyship, pre-need plans, and member certificates issued by mutual benefit association; and
h. Other similar instruments where title thereto passes to another by endorsement, assignment, or delivery.

23. **Originating Institution** – refers to the financial institution, which initiates the wire transfer and transfers the funds upon receiving the request for a wire transfer on behalf of the originator.

24. **Originator** – refers to the account holder who allows the wire transfer from that account or where there is no account, the person that places an order with the originating/ordering financial institution to perform a wire transfer

25. **Politically Exposed Person (PEP)** – refers to an individual who is or has been entrusted with prominent public positions in the Philippines or in a foreign state, including the following:

    a. President
    b. Vice President
    c. Senators
    d. Cabinet members
    e. Justices of the Supreme Court, Court of Appeals, Sandiganbayan, Court of Tax Appeals
    f. Congressmen
    g. Heads of Military and Generals
    h. Mayors
    i. Governors
    j. President of Major Political Parties as certified by the COMELEC
    k. President of Government Owned and Controlled Corporation (GOCC)

        a. Immediate family shall include parents, siblings, spouse, children and in-laws and all relatives within the 2nd degree of consanguinity or affinity.
        b. Close associates – a person widely and publicly known to maintain an unusually close relationship with the senior foreign political figure and includes a person who is in a position to conduct substantial domestic and international financial transactions on behalf of the senior foreign political figure.

26. **Proliferation Financing** – refers to the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, transshipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery

and related materials (including both technologies and dual use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations.

27. **Real Estate** – refers to the land and all those items which are attached to the land. It is the physical, tangible entity, together with all the additions or improvements on, above or below the ground.

28. **Real Estate Broker** – refers to a duly registered and licensed natural person who, for a professional fee, commission or other valuable consideration, acts as an agent of a party in a real estate transaction to offer, advertise, solicit, list, promote, mediate, negotiate or effect the meeting of the minds on the sale, purchase, exchange, mortgage, lease or joint venture, or other similar transactions on real estate or any interest therein.

29. **Real Estate Developer** – refers to any natural or juridical person engaged in the business of developing real estate development project for his/her or its own account and offering them for sale or lease.

30. **Related Web of Accounts pertaining to the Monetary Instrument or Property Subject of the Freeze Order** – shall refer to those accounts, the funds and sources of which originated from and/or materially linked to the monetary instrument(s) or property(ies) subject of the freeze order(s) or an order of inquiry, regardless of the layer of accounts that the funds had passed through or transactions that they had undergone.

31. **Senior Management** – shall refer to the senior officers to include the CEO or President, Head of respective groups, divisions or departments. For BBG, it includes Region Heads and District Heads with a rank of at least Assistant Vice President.

32. **Shell Company** – refers to a legal entity which has no business substance in its own right but through which financial transactions may be conducted.

33. **Shell Bank** – refers to a shell company incorporated as a bank or made to appear to be incorporated as a bank but has no physical presence and no affiliation with a regulated financial group. It can be a bank that: (a) does not conduct business at a fixed address in the jurisdiction in which the shell bank is authorized to engage; (b) does not employ one or more individuals on a full time basis at this fixed address, (c) does not maintain operating records at this address, and (d) is not subject to inspection by the authority that licensed it to conduct banking activities.

34. **Supervising Authority** – refers to the appropriate supervisory or regulatory agency, department or office designated by law to supervise or regulate the covered institutions, such as the Bangko Sentral ng Pilipinas (BSP), the Insurance Commission (IC), or the Securities and Exchange Commission (SEC).

35. **Suspicious Transaction** – is a transaction regardless of the amount involved, where any of the following suspicious circumstances exist:

    a. There is no underlying legal or trade obligation, purpose or economic justification;
    b. The client is not properly identified;
    c. The amount involved is not commensurate with the business or financial capacity of the client;

d. Taking into account all known circumstances, it may be perceived that the client's transaction is structures in order to avoid being the subject of reporting requirements under the AMLA, as amended;
e. Any circumstance relating to the transaction which is observed to deviate from the profile of the client and/or the client's past transactions;
f. The transaction is in any way related to an unlawful activity or offense under the AMLA, as amended, that is about to be, is being or has been committed;
g. Any transaction that is similar or analogous or identical to any of the foregoing, such as the relevant transactions in related and materially-linked accounts, as herein defined; or
h. Any unsuccessful attempt to transact with a covered person, the denial of which is based on any of the foregoing circumstances.

36. **Trafficking in Persons (TIP)** – refers to any of the acts as enumerated in Sections 4 and 5 of the Expanded Anti Trafficking in Persons Act of 2022.

37. **Transaction** – refers to any act establishing any right or obligation or giving rise to any contractual or legal relationship between the covered person and its customer. It also includes any movement of funds, by any means, in the ordinary course of business of a covered person.

38. **Transaction Alert** – shall refer to an Alert generated by the Bank's AML system pertaining to a transaction or series of transactions that met the scenario requirements/parameters of the Base60 AML System. These are transactions flagged by the system as worth investigating.

39. **Transactor** – is a person who does not have an account with the Bank, but is transacting with the Bank. A transactor is the not the same as an authorized agent/representative, as they are acting on behalf of oneself, rather than for an account holder.

40. **Terrorism Financing** – is the provision of financial sustenance or service to terrorist and its activities. It may involve funds raised from legitimate sources, such as personal donations and profits from businesses and charitable organizations, as well as funds from criminal sources, such as the drug trade, the smuggling of weapons and other goods, fraud, kidnapping and extortion, and the like.

41. **Money Laundering** is a crime whereby the proceeds of an unlawful activity are transacted thereby making them appear to have originated from legitimate sources. It is committed by any person who, knowing that any monetary instrument or property represents, involves, or relates to the proceeds of any unlawful activity:

    a. Transacts said monetary instrument or property;
    b. Converts, transfers, disposes of, moves, acquires, possesses or uses said monetary instrument or property;
    c. Conceals or disguises the true nature, source, location, disposition, movement or ownership of or rights with respect to said monetary instrument or property;
    d. Attempts or conspires to commit money laundering offenses referred to in paragraph (a), (b) or (c);
    e. Aids, abets, assists in or counsels the commission of the money laundering offenses referred to in paragraphs (a), (b) or (c) above; and

f. Performs or fails to perform any act as a result of which he facilitates the offense of money laundering referred to in paragraphs (a), (b) or (c) above.

Money laundering is also committed by any person knowing that any monetary instrument or property is required under this Act to be disclosed and filed with the Anti-Money Laundering Council (AMLC), fails to do so.

Money laundering is likewise committed by any covered person who, knowing that a covered or suspicious transaction is required under this Act to be reported to the Anti-Money Laundering Council (AMLC), fails to do so.

42. **Weapons of Mass Destruction (WMD)** – refers to chemical, biological, radiological, or nuclear weapons which are capable of a high order of destruction or of causing mass casualties. It excludes the means of transporting or propelling the weapon where such means is a separable and divisible part from the weapon.

43. **Unlawful Activity** – refers to any act or omission or series or combination thereof involving or having direct relation to the following:

1) Kidnapping for ransom under Article 267 of Act No. 3815, otherwise known as the Revised Penal Code, as amended;
2) Sections 4, 5, 6, 8, 9, 10, 11, 12, 13, 14, 15 and 16 of Republic Act No. 9165, otherwise known as the Comprehensive Dangerous Drugs Act of 2002;
3) Section 3 paragraphs B, C, E, G, H and I of Republic Act No. 3019, as amended, otherwise known as the Graft and Corrupt Practices Act;
4) Plunder under Republic Act No. 7080, as amended;
5) Robbery and extortion under Articles 294, 295, 296, 299, 300, 301 and 302 of the Revised Penal Code, as amended;
6) Jueteng and Masiao punished as illegal gambling under Presidential Decree No. 1602;
7) Piracy on the high seas under the Revised Penal Code, as amended and Presidential Decree No. 532;
8) Qualified theft under Article 310 of the Revised Penal Code, as amended;
9) Swindling under Article 315 and Other Forms of Swindling under Article 316 of the Revised Penal Code, as amended;
10) Smuggling under Republic Act Nos. 455 and 1937;
11) Violations of Republic Act No. 8792, otherwise known as the Electronic Commerce Act of 2000;
12) Hijacking and other violations under Republic Act No. 6235; destructive arson and murder, as defined under the Revised Penal Code, as amended;
13) Terrorism and conspiracy to commit terrorism as defined and penalized under Sections 3 and 4 of Republic Act No. 9372;
14) Financing of terrorism under Section 4 and offenses punishable under Sections 5, 6, 7 and 8 of Republic Act No. 10168, otherwise known as the Terrorism Financing Prevention and Suppression Act of 2012;
15) Bribery under Articles 210, 211 and 211-A of the Revised Penal Code, as amended, and Corruption of Public Officers under Article 212 of the Revised Penal Code, as amended;
16) Frauds and Illegal Exactions and Transactions under Articles 213, 214, 215 and 216 of the Revised Penal Code, as amended;

17) Malversation of Public Funds and Property under Articles 217 and 222 of the Revised Penal Code, as amended;
18) Forgeries and Counterfeiting under Articles 163, 166, 167, 168, 169 and 176 of the Revised Penal Code, as amended;
19) Violations of Sections 4 to 6 of Republic Act No. 9208, otherwise known as the Anti-Trafficking in Persons Act of 2003;
20) Violations of Sections 78 to 79 of Chapter IV, of Presidential Decree No. 705, otherwise known as the Revised Forestry Code of the Philippines, as amended;
21) Violations of Sections 86 to 106 of Chapter VI, of Republic Act No. 8550, otherwise known as the Philippine Fisheries Code of 1998;
22) Violations of Sections 101 to 107, and 110 of Republic Act No. 7942, otherwise known as the Philippine Mining Act of 1995;
23) Violations of Section 27(c), (e), (f), (g) and (i), of Republic Act No. 9147, otherwise known as the Wildlife Resources Conservation and Protection Act;
24) Violation of Section 7(b) of Republic Act No. 9072, otherwise known as the National Caves and Cave Resources Management Protection Act;
25) Violation of Republic Act No. 6539, otherwise known as the Anti-Carnapping Act of 2002, as amended;
26) Violations of Sections 1, 3 and 5 of Presidential Decree No. 1866, as amended, otherwise known as the decree Codifying the Laws on Illegal/Unlawful Possession, Manufacture, Dealing In, Acquisition or Disposition of Firearms, Ammunition or Explosives;
27) Violation of Presidential Decree No. 1612, otherwise known as the Anti-Fencing Law;
28) Violation of Section 6 of Republic Act No. 8042, otherwise known as the Migrant Workers and Overseas Filipinos Act of 1995, as amended by Republic Act No. 10022;
29) Violation of Republic Act No. 8293, otherwise known as the Intellectual Property Code of the Philippines;
30) Violation of Section 4 of Republic Act No. 9995, otherwise known as the Anti-Photo and Video Voyeurism Act of 2009;
31) Violation of Section 4 of Republic Act No. 9775, otherwise known as the Anti-Child Pornography Act of 2009;
32) Violation of Sections 5, 7, 8, 9, 10(c), (d) and (e), 11, 12 and 14 of Republic Act No. 7610, otherwise known as the Special Protection of Children Against Abuse, Exploitation and Discrimination;
33) Fraudulent practices and other violations under Republic Act No. 8799, otherwise known as the Securities Regulation Code of 2000;
34) Violation of Section 9 (a)(3) of Republic Act No. 10697, otherwise known as the "Strategic Trade Management Act", in relation to the proliferation of weapons of mass destruction and its financing pursuant to United Nations Security Council Resolution Numbers 1718 of 2006 and 2231 of 2015";
35) Violation of Section 254 of Chapter II, Title X of the National Internal Revenue Code of 1997, as amended, where the deficiency basic tax due in the final assessment is in excess of Twenty-five million pesos (P25,000,000.00) per taxable year, for each tax type covered and there has been a finding of probable cause by the competent authority: Provided, further, that there must be a finding of fraud, willful misrepresenting or malicious intent on the part of the taxpayer: Provided, finally, That in no case shall the AMLC institute forfeiture proceedings to recover monetary instruments, property or proceeds representing, involving, or relating to a tax crime, if the same has already been recovered or collected by the Bureau of Internal Revenue (BIR) in a separate proceeding and
36) Felonies or offenses of a similar nature that are punishable under the penal laws of other countries.

Note: The above lists of unlawful activities or predicate crimes were adopted from Republic Act 11521 as the latest amendatory law of AMLA.

2.2 TARGETED FINANCIAL SANCTIONS

1. **Targeted Financial Sanctions** – refers to (1) For TFS related to terrorism and TF: both asset freezing and prohibitions to prevent funds or other assets from being made available, directly or indirectly, for the benefit of designated persons and those proscribed by the Court of Appeals under Section 26 of the ATA. (2) For TFS related to PF. both asset freezing and prohibition to prevent funds or other assets from being made available, directly or indirectly, for the benefit of any individual, natural or legal persons or entity designated pursuant to UNSCR and its designation process.

2. **Name Match** – refers to an individual or entity whose name matches with a name in the UNSC Consolidated List, any list of designations made by the Anti-Terrorism Council (ATC) under Paragraph 3, Section 25 of the ATA, or those proscribed by the Court of Appeals under Section 26 of the ATA.

3. **Potential Target Match** – refers to an individual or entity whose identity matches most, but not all, of the identifier information provided in the UNSC Consolidated List, any list of designations made by the Anti-Terrorism Council (ATC) under Paragraph 3, Section 25 of the ATA, or those proscribed by the Court of Appeals under Section 26 of the ATA.

4. **Target Match** – refers to an individual or entity whose identity matches all the identifier information and is identified to be the designated person in the UNSC Consolidated List, any list of designations made by the Anti-Terrorism Council (ATC) under Paragraph 3, Section 25 of the ATA, or those proscribed by the Court of Appeals under Section 26 of the ATA.

5. **UNSC Consolidated List** – refers to the integrated list of individuals and entities subject to measures imposed by the UNSC, as relevant to the Philippines sanctions regime. This includes those designated under U NSCR Nos. 1267/1989/2253 (Al Qaeda/ISIL Da'esh), 1988 (Taliban), 17/8 (2006) (DPRK) and 2231 (2015) (Iran) and their successor resolutions.

6. **Proliferation of Weapons of Mass Destruction** – refers to the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of WMD, in contravention of national laws or, where applicable, international obligations.

7. **Designated Persons** – shall refer to: (1) Any person or entity designated as a terrorist, one who finances terrorism, or a terrorist organization or group under the applicable United Nations (UN) Security Council (UNSC) Resolutions (UNSCR) and their successor resolutions; or (2) Any person, organization, association, or group of persons designated under Paragraph 3, Section 25 of the Anti-Terrorism Act of 2020 (ATA); and (3) Any person or entity designated under UNSCR Nos. 1718 (2006) and 2231 (2015) and their successor resolutions.

8. **Sanctioned Parties** – any Person that is the target of Sanctions, including, without limitation, (a) any Person identified in any Sanctions-related list of sanctioned persons administered by OFAC, UN, EU and UK HMT; (b) any person located, organized or resident in a sanctioned jurisdiction; or (c) any juridical person or arrangement owned, directly or indirectly, or controlled by any such person described in (a) and (b).

9. **Sanctions Screening** – it is a control used in the detection, prevention and disruption of financial crime and, in particular, sanctions risk thru watchlist screening to determine if there is a possible match and conducting appropriate actions, including freezing of the account as well as filing of STR depending on the type of match found.

10. **Sectoral Sanctions** – is the US OFAC and the EU Ukraine and Russia-related sanctions programmes prohibiting certain types of transactions with targeted entities in the finance, energy and defense sectors, as well as entities owned by 50% or more by the targets in traduced in July 2014. OFAC refers to these sanctions as Sectoral Sanctions Identification List.

11. **Specially Designated Nationals and Blocked Persons** – individuals and entities which are owned or controlled by, or acting for or on behalf of, the government of target countries or are associated with international narcotics trafficking or terrorism. These individuals and entities are listed on the Treasury Department's Specially Designated Nationals and Blocked Persons list so that persons subject to the jurisdiction of the U.S. will know that they are prohibited from dealing with the listed entities and must block all property within their possession or control in which these individuals and entities have an interest.

12. **Specific License** – a permit issued by OFAC on a case-by-case basis to a specific individual or company allowing an activity that would otherwise be prohibited by the embargo or sanctions program.

13. **Transaction Screening** – is the process of screening a movement of value within the FI's records, including funds, goods, or assets, between parties or accounts. In order to mitigate risk associated with trade finance transactions and international wire transfers, FIs conduct real-time screening of cross border transactions against Sanctions Lists, where any of the Sending Bank, Originating Bank, Receiving Bank, Intermediary Bank or Beneficiary Bank are located in different countries.

14. **Anti-Terrorism Act of 2020 (ATA)** – also known as Republic Act No. 11479, it is an act to prevent, prohibit and penalize terrorism. It supersedes Republic Act No. 9372, otherwise known as the "Human Security Act of 2007"

15. **Anti-Terrorism Council (ATC)** – implements the ATA and assume the responsibility for the proper and effective implementation of the policies of the country against terrorism. It is chaired by the Executive Secretary with the National Security Adviser as the Vice Chairman. Its other members are the Secretary of Foreign Affairs, Secretary of National Defense, Secretary of Interior and Local Government, Secretary of Finance, Secretary of Justice, Secretary of Information and Communications Technology, the Executive Director of the Anti-Money Laundering Council Secretariat.

16. **Sanctions Freeze Order** – refers to a freeze order on the assets of a sanctioned individual or entity.

17. **Strategic Trade Management Act (STMA)** – also known as Republic Act No. 10697, is an act preventing the proliferation of weapons of mass destruction by managing the trade in strategic goods, the provision of related services, and for other purposes.

18. **Property or Fund** – refers to financial assets, property of every kind, whether tangible or intangible, movable or immovable, however acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such funds or other assets, including, but not limited to, bank credits, traveler's cheques, bank cheques, money orders, shares, securities, bonds, drafts, or letters of credit, and any interest, dividends, or other income on or value accruing from or generated by such funds or other assets.

19. **Proliferation of Weapons of Mass Destruction (WMD) Financing / Proliferation Financing (PF)** – refers to an action or circumstances when a person makes available an asset; or provides a financial service; or conducts a financial transaction; and the person knows that, or is reckless as to whether, the asset, financial service or transaction is intended to, in whole or in part, facilitate proliferation of WMD in relation to UNSCR Nos. 17/8 (2006) (Democratic People's Republic of Korea or DPRK) and 2231 (2015) (Islamic Republic of Iran or Iran) and their successor resolutions.

20. **Sanctions risk** – refers to the risk of losses arising from failure to implement relevant sanctions requirements, including TFS. This includes risks of potential breach, non-compliance/non-implementation or evasion of TFS obligations.

21. **Targeted asset freeze** – applies to named individuals, entities and bodies, restricting access to funds and economic resources. Someone subject to an asset freeze will be listed on the Consolidated List, designated or proscribed and posted under the Anti-Money Laundering Council (AMLC) or ATC websites.

PART III
MONEY LAUNDERING AND TERRORISM FINANCING

PART III: MONEY LAUNDERING AND TERRORISM FINANCING

3.1 MONEY LAUNDERING

What is Money Laundering? It is a crime whereby proceeds from unlawful activity (or simply "dirty money or property") are transacted, thereby making it appear to have originated from legitimate source.

Commission of Money Laundering. Per Section 4 of R.A. No. 9160, as amended (also Section 904 of the MORB), Money laundering is committed by any person who, knowing that any monetary instrument or property represents, involves, or relates to the proceeds of any unlawful activity:

a) Transacts said monetary instrument or property;
b) Converts, transfers, disposes of, moves, acquires, possesses or uses said monetary instrument or property
c) Conceals or disguises the true nature, source, location, disposition, movement or ownership of or rights with respect to said monetary instrument or property;
d) Attempts or conspires to commit money laundering offenses referred to in Items "(a)",'(b)' or "(c)" above;
e) Aids, abets, assists in or counsels the commission of the money laundering offenses referred to in items "(a)", "(b)" or "(c)"above; and
f) Performs or fails to perform any act as a result of which he facilitates the offense of money laundering referred to in Items "(a)", "(b)" or "(c)" above.

Money laundering is also committed by any person knowing that any monetary instrument or property is required under this Act to be disclosed and filed with the Anti-Money Laundering Council (AMLC), fails to do so.

Money laundering is likewise committed by any covered person who, knowing that a covered or suspicious transaction is required to be reported to the Anti-Money Laundering Council (AMLC) under any of the provisions of the AMLA, as amended, its RIRR, or this Part, fails to do so.

Unlawful Activity refers to any act or omission or series or combination thereof involving or having direct relation to the following – *refer to number 34, Part II Definition of Terms* for the complete list.

Stages of Money Laundering. Money Laundering involves three stages, namely:

1. **Placement** – the physical disposal of cash proceeds derived from illegal activity. At this stage, the launderer inserts the dirty money into a legitimate financial institution. This is often in the form of cash deposits. This is the riskiest stage of the laundering process because large amounts of cash are pretty conspicuous, and banks are required to report high-value transactions. Common examples are the following:

    a. Dirty money deposited or invested to the bank;
    b. Dirty money co-mingled to legitimate funds and transacted to the bank;
    c. Structured transacting (just below the reporting threshold) of dirty money to avoid detection of regulators;
    d. Dirty money being exchanged/converted to another currency;
    e. Dirty money being used to purchase cashier/manager's check, drafts or other cash equivalent, instead of conveniently debiting the client's deposit account';
    f. Dirty money being exported from one country to another;

g. Dirty money being used to purchase high value goods, property, business or assets

2. **Layering** – separating illicit proceeds from their source by creating complex layers of financial transactions designed to disguise audit trail and provide anonymity. Layering involves sending the money through various financial transactions to change its form and make it difficult to follow. It may consist of several bank-to-bank transfers, wire transfers between different accounts in different names in different countries, making deposits and withdrawals to continually vary the amount of money in the accounts, changing the money's currency, and purchasing high-value items (boats, houses, cars, precious metals, etc.) to change the form of the money. This is the most complex step in any laundering scheme, and it's all about making the original dirty money as hard to trace as possible. The following are some of the common activities involved:

    a. Use of multiple bank and/or bank accounts (both local and foreign);
    b. Engaging professionals act as intermediaries and transacting through corporations and trusts;
    c. Performing series of transactions after possession or deposit of funds such as wire transfer, conversion to money orders or drafts, acquisition of property, or purchase of insurance policy;
    d. Selling of investments or cash equivalents acquired using the dirty money
    e. Investing in legitimate business, whether by creating a new one or buying an existing business;
    f. Using the deposited dirty money as collateral to loan availed by the client-launderer (one-to-one loan)

3. **Integration** – the final step to legitimize criminally derived wealth. If the layering process has succeeded, integration schemes place the laundered proceeds back into the economy in such a way that they re-enter the financial system appearing to be normal business funds. Integration may be illustrated in the following:

    a. Using the laundered funds to pay-off bank loans;
    b. Using the laundered funds to purchase luxury goods;
    c. Gaining profit/income from investments/properties acquired using the laundered funds

3.2 TERRORISM FINANCING

What is Terrorism Financing? Terrorism financing is the provision of financial sustenance to terrorists and its activities. It may involve funds raised from legitimate sources, such as personal donations and profits from businesses and charitable organizations, as well as funds from criminal sources, such as the drug trade, the smuggling of weapons and other goods, fraud, kidnapping and extortion, and the like.

Commission of Financing of Terrorism. Section 4 of the Philippine R.A. 10168 (*The Terrorism Financing Prevention and Suppression Act of 2012*) defined Financing of terrorism as a crime committed by a person who, directly or indirectly, willfully and without lawful excuse, possesses, provides, collects or uses property or funds or makes available property, funds or financial service or other related services, by any means, with the unlawful and willful intention that they should be used or with the knowledge that they are to be used, in full or in part: (1) to carry out or facilitate the commission of any terrorist act; (2) by a terrorist organization, association or group; or (3) by an individual terrorist. Commission of financing of terrorism shall include:

1. Organizing or directing others to commit financing of terrorism under the immediately preceding paragraph shall likewise be guilty of an offense and shall suffer the same penalty as herein prescribed (2nd par. Section 4 of R.A. 10168)

2. Attempt or Conspiracy to Commit the Crimes of Financing of Terrorism and Dealing with Property or Funds of Designated Persons (Section 5 of R.A. 10168)

3. Accomplice or any person who, not being a principal under Article 17 of the Revised Penal Code or a conspirator as defined in Section 5 hereof, cooperates in the execution of either the crime of financing of terrorism or conspiracy to commit the crime of financing of terrorism (Section 6 of R.A. 10168)

4. Accessory or any person who, having knowledge of the commission of the crime of financing of terrorism but without having participated therein as a principal, takes part subsequent to its commission, by profiting from it or by assisting the principal or principals to profit by the effects of the crime, or by concealing or destroying the effects of the crime in order to prevent its discovery, or by harboring, concealing or assisting in the escape of a principal of the crime shall be guilty as an accessory to the crime of financing of terrorism and shall be imposed a penalty two degrees lower than that prescribed for principals in the crime of financing terrorism (Section 6 of R.A. 10168)

5. Prohibition Against Dealing with Property or Funds of Designated Persons – Any person who, not being an accomplice under Section 6 or accessory under Section 7 in relation to any property or fund: (i) deals directly or indirectly, in any way and by any means, with any property or fund that he knows or has reasonable ground to believe is owned or controlled by a designated person, organization, association or group of persons, including funds derived or generated from property or funds owned or controlled, directly or indirectly, by a designated person, organization, association or group of persons; or (ii) makes available any property or funds, or financial services or other related services to a designated and/or identified person, organization, association, or group of persons, shall suffer the penalty of reclusion temporal in its maximum period to reclusion perpetua and a fine of not less than Five hundred thousand pesos (Php500,000.00) nor more than One million pesos (Php1,000,000.00)

6. Offense by a Juridical Person, Corporate Body or Alien. – If the offender is a corporation, association, partnership or any juridical person, the penalty shall be imposed upon the responsible officers, as the case may be, who participated in, or allowed by their gross negligence, the commission of the crime or who shall have knowingly permitted or failed to prevent its commission. If the offender is a juridical person, the court may suspend or revoke its license. If the offender is an alien, the alien shall, in addition to the penalties herein prescribed, be deported without further proceedings after serving the penalties herein prescribed.

Why Terrorism Financing is More Difficult to Detect? Terrorists or their sympathizers use techniques like those of money launderers to divert the authorities' and the financial institution’s attention to protect the true identity of the funds, the contributor and the ultimate beneficiary. Financial transactions relative to terrorism financing usually involves customary amounts, and may came from legitimate sources such as those contributions from sympathizers who are people with legitimate sources of income. Thus, unlike money laundering, terrorism financing is more difficult to detect.

As it is not uncommon for a terrorist group to receive support from sympathizers located in other countries, the financial system of any country is vulnerable to the threat of terrorism financing.

3.3 BASIC PRINCIPLES AND POLICIES OF ANTI-MONEY LAUNDERING AND COMBATING OF FINANCING OF TERRORISM

The Bank, in performing its roles as a vehicle of the State in fighting money laundering and terrorist financing in the Philippines, shall be guided by the following principles:

1. To conduct business in conformity with the high ethical standards in order to protect its safety and soundness as well as integrity of the national banking and financial system;

2. To know sufficiently its customers at all times and 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 or maintaining an account or transacting with the Bank;

3. To adopt and effectively implement a sound AML and terrorist financing risk management system that identifies, assesses, monitors and controls risk associated with money laundering and terrorist financing;

4. To comply fully with these rules and existing laws aimed at combating money laundering and terrorist financing by making sure that its officers and employees are aware of their respective responsibilities and carry them out in accordance with superior and principled culture of compliance; and

5. To fully cooperate with the AMLC for the effective implementation and enforcement of the AMLA, as amended, and its RIRR.

3.4 A TYPICAL MONEY LAUNDERING SCHEME

Process of Money Laundering

SOURCES OF INCOME	PLACEMENT	LAYERNG	INTEGRATION
	GOAL Deposit Criminal Proceeds Into Financial System	GOAL Conceal the Criminal Origin of Proceeds	GOAL Create an Apparent Legal Origin for Criminal Proceeds
• Tax Crimes • Fraud • Embezzlement • Drugs • Theft • Bribery Corruption	• Change of Currency • Change of Denominations • Transportation of Cash • Cash Deposits	• Wire Transfers • Withdrawals in Cash • Cash Deposits in Other Bank Accounts • Split and Merge Between Bank Accounts	• Creating Fictitious Loans, Turnover/Sales, Capital Gains, Deeds, Contracts, Financial Statements • Disguise Ownership of Assets • Criminal Funds Used In Third Party Transactions

PART IV
MONITORING, ENFORCEMENT AND SUPERVISION

PART IV: MONITORING, ENFORCEMENT AND SUPERVISION

4.1 THE ANTI-MONEY LAUNDERING COUNCIL (AMLC)

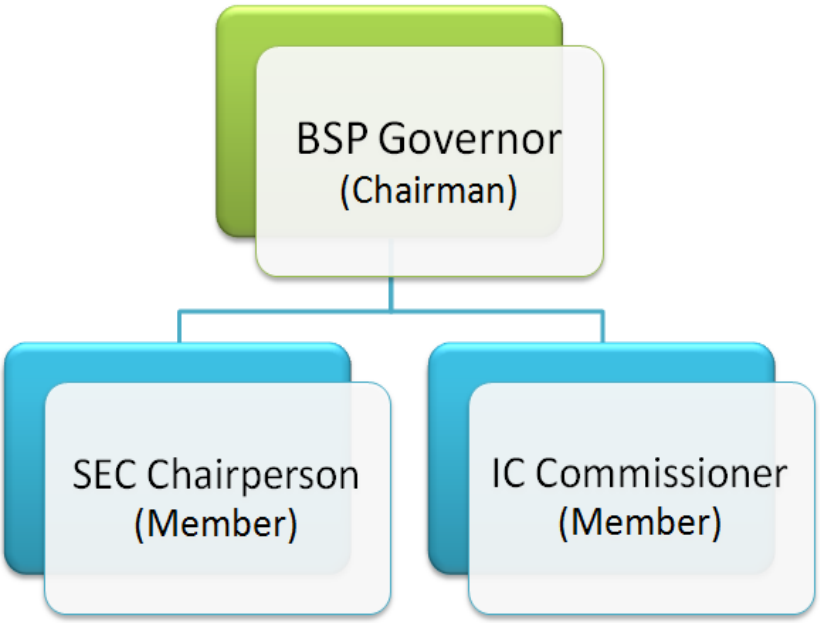
Composition

The AMLC that was created under Republic Act (RA) No. 9160, as amended by RA No. 9194, is composed of the following members:

1. Governor of the Bangko Sentral ng Pilipinas (BSP) as Chairman
2. Commissioner of the Insurance Commission (IC) as member
3. Chairman of the Securities and Exchange Commission (SEC), as member

Decision

The AMLC shall act unanimously in discharging its functions as defined in RA No. 9160, as amended. However, in the case of the incapacity, absence or disability of any member to discharge his functions, the officer duly designated or authorized to discharge the functions of the Governor of the BSP, the Chairman of the SEC or the Insurance Commissioner, as the case may be, shall act in his stead in the AMLC.



4.2 ENFORCEMENT ACTIONS BY THE AMLC

The AMLC shall, where the circumstances warrant, impose administrative sanctions and warnings upon the Bank for the violation of the AMLA and its IRR, or for failure or refusal to comply with the orders, resolutions and other issuances of the AMLC.

The following are the violations and their corresponding sanctions based pursuant to the Rules of Procedure in Administrative Cases (RPAC):

Classification	Minimum	Medium	Maximum
Grave	P250K per violation but not to exceed P10M	P375K per violation but not to exceed P15M	P500K per violation but not to exceed P20M
Major	P150K per violation but not to exceed P5M	P225K per violation but not to exceed P7.5M	P300K per violation but not to exceed P10M
Serious	P100K per violation but not to exceed P1M	P150K per violation but not to exceed P2.5M	P200K per violation but not to exceed P5M
Less Serious	P50K per violation but not to exceed P500K	P75K per violation but not to exceed P750K	P100K per violation but not to exceed P1M
Light	P25K per violation but not to exceed P250K	P37.5K per violation but not to exceed P375K	P50K per violation but not to exceed P500K

The AMLC may impose against the Bank warnings or non-monetary sanctions that may include, but are not limited to, any, or a combination of, the following:

a) Warning that future infractions or other acts of a similar nature shall be dealt with more sternly;
b) Reprimand of the Bank, with directive to correct the deficiencies within a reasonable period of time;
c) Submission of a Compliance Commitment signed by the Bank's Board of Directors, indicating the specific timelines of concrete measures to correct the deficiencies, and of regular reporting of updates on said corrective measures;
d) Revocation of the certificate of registration issued by the AMLC;
e) Referral of the administrative Resolution to the appropriate Supervising Authority or Appropriate Government Agency for appropriate action; and
f) Publication of the administrative Resolution involving (assessment) grave or major violations or repeat significant non-compliance.

4.3 THE AMLC SECRETARIAT

Composition

The Secretariat that was created under RA No. 9160, as amended by RA No. 9194, is composed of the following members:

1. Executive Director who is appointed by the AMLC for a term of five (5) years
2. Members chosen by AMLC from those who have served continuously or cumulatively, for at least five (5) years in the BSP, the SEC or the IC.

Detail and Secondment

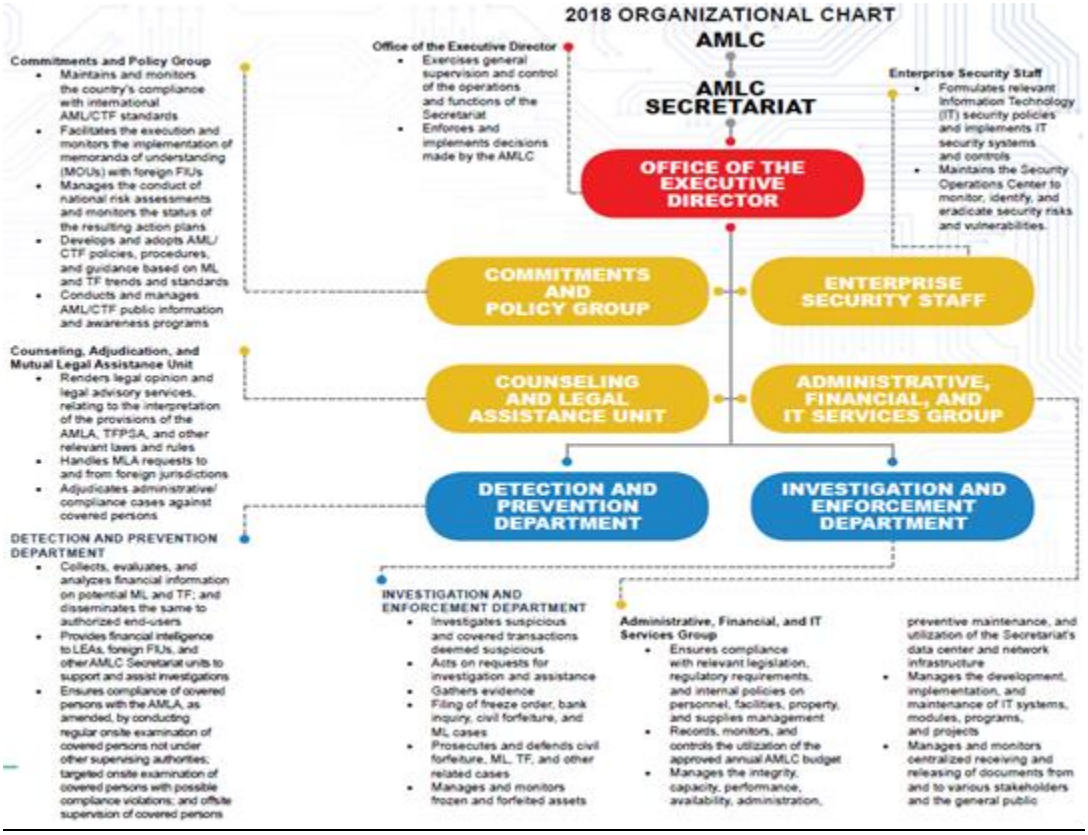
The AMLC is authorized to enlist the assistance of the BSP, the SEC or the IC, or any other branch, bureau, office, agency or instrumentality of the government in undertaking any and all anti-money laundering operations. This includes the use of any member of their personnel who may be detailed or seconded to the AMLC.

Composition

Any member of the BSP, the SEC or the IC, or any other branch, bureau, office, agency or instrumentality of the government.

Function

The detailed and seconded personnel shall assist the AMLC in undertaking any and all anti-money laundering operations.



4.4 DEPARTMENT OF JUSTICE

Functions

The AMLC, upon determining after investigation that there is probable cause to charge any person with money laundering offense shall cause a complaint to be filed before the Department of Justice. The Department of Justice shall conduct the preliminary investigation of the case. If after due notice and hearing in the preliminary investigation proceedings, and it should find probable cause of a money laundering offense, it shall file the necessary information before the Regional Trial Courts.

4.5 OMBUDSMAN

Functions

The AMLC, upon determining after investigation that there is probable cause to charge public officers and private persons who are in conspiracy with public officers, with money laundering offense shall cause a complaint to be filed before the Ombudsman. The Ombudsman shall conduct the preliminary investigation of the case. If after due notice and hearing in the preliminary investigation proceedings and it should find probable cause of a money laundering offense, it shall file the necessary information before the Sandiganbayan.

4.6 REGIONAL TRIAL COURTS (RTCs)

Function

The RTCs shall have the jurisdiction to try all cases on money laundering.

4.7 SANDIGANBAYAN

Function

The Sandiganbayan shall have the jurisdiction to try all cases on money laundering of public officers and private persons who are in conspiracy with public officers.

4.8 CONGRESSIONAL OVERSIGHT COMMITTEE (COC)

Composition

The COC that was created under RA No. 9160, as amended, is composed of the following members:

1. Seven (7) members from the Senate appointed by the Senate President
2. Seven (7) members from the House of Representatives appointed by the Speaker of the House of Representatives

Functions

The COC shall have the following functions:

1. promulgate its own rules
2. oversee the implementation of RA No. 9160, as amended
3. review and revise the implementing rules issued by the AMLC

4.9 BANGKO SENTRAL NG PILIPNAS (BSP)

Authority and Enforcement Actions

The supervising authorities, the BSP, SEC and the IC shall, under their own respective charters and regulatory authority, issue their Guidelines and Circulars on anti-money laundering to effectively implement the provisions of RA 9160, as amended.

BSP Authority to examine deposits and investments; additional exception to the Bank Secrecy Act and annual testing of numbered accounts.

To ensure compliance with the AMLA, as amended, its RIRR, and these Rules, the BSP may inquire into or examine any deposit or investment with any banking institution or non-bank financial institution and their subsidiaries and affiliates when the examination is made in the course of a periodic or special examination, in accordance with the Rules of Examination of the BSP.

The BSP may likewise conduct annual testing solely limited to the determination of the existence and true identity of the owners of numbered and similar accounts.

In the course of the periodic and special examination for purposes of complying with the provisions of the AMLA, as amended, its RIRR, and these Rules, the covered institutions, their officers and employees and the BSP shall not be deemed to have violated the provisions of Republic Act No. 1405, as amended, Republic Act No. 6426, as amended, Republic Act No. 8791 and other similar laws and BSP Circular No. 706 or the Updated Anti-Money Laundering Rules and Regulations when disclosing information to BSP relative to covered and suspicious transaction reports filed with the AMLC.

Sanctions and Penalties

In line with the objective of ensuring that the Bank maintain high anti-money laundering standards in order to protect its safety and soundness as well as protecting the integrity of the national banking and financial system, violation of these Rules shall constitute a major violation subject to the following enforcement actions by the BSP against the Board of Directors, Senior Management and line officers, not necessarily according to priority:

1. Written reprimand;
2. Suspension or removal from the office they are currently holding; and/or
3. Disqualification from holding any position in any covered institution.

In addition to the non-monetary sanctions stated above, BSP may also impose monetary penalties computed in accordance with existing regulations and in coordination with the Anti-Money Laundering Council.

Enforcement actions shall be imposed on the basis of the over-all assessment of the covered institution's AML risk management system. Whenever the Bank's AML compliance system is found to be grossly inadequate, this may be considered as unsafe and unsound banking practice that may warrant initiation of prompt corrective action.

4.10 SUMMARY OF DUTIES AND RESPONSIBILITIES

Unit	Person Responsible	Responsibilities
HO Units and Branches	• All Officers and Employees	• Attend and participate in the AMLA trainings conducted regularly by the Bank Compliance Division
	• Soliciting Officers (SOs) - Business Managers (BMs) - Marketing Officers (MOs) - Relationship Managers (RMs) - Account Officers (AOs) - Other Marketing Account Officers	• Conduct initial client risk assessment/ profiling and the corresponding due diligence to assess and identify the client's true identity prior to account opening or establishing business relationship. • Ensure, being accountable officers, submission of required documents within committed timelines, including completeness and correctness of the documents submitted.
		• Monitor, validate and report if deemed suspicious unusual movements and activities of accounts to AML Compliance Department particularly if said account is subject of: - STR - Authority/resolution to inquire into Bank Deposits
	• Service Associates of Branches or its equivalent for HO Units	• Determine the positive identification of the client upon account opening and shall assess at all times based on factors such as, but not limited to, the nature of the service or product to be availed of by the client and the purpose of the account or transaction; country or origin or residence of operations, public or high profile position of the client, PEP relatives within the second degree of consanguinity and affinity, watchlist of individuals and entities engaged in illegal activities as circularized by BSP, AMLC and other international entities or organizations such as, among others, Office of Foreign Assets Control (OFAC), Al Qaeda List and Interpol List based on available data; client's name appearing in other watchlist categories such as caution list and negative list; existence of suspicious transaction indicators; and such other factors necessary to consider in assessing the risk of a customer to ML/TF. • Perform customer risk profiling and requires from depositor additional identification document when warranted • Secure appropriate approval of the opening of the account
		• Investigate alerts from the date of alert generation or date of re-assignment in case of re-assigned alerts
	• Branch Service Heads or its equivalent for HO units	• Approve opening of new accounts based on MTPP Manual and Branch Operations Manual which covers customer identification and verification guidelines/measures

Unit	Person Responsible	Responsibilities
		• Update, review and re-evaluate existing client records and accounts every 2 years or as often as necessary whenever material information has become available and assess need to re-classify based on risk • Review client transactions and identify suspicious transactions, if any, based on available source/information such as, but not limited to: - Reports via Finnacle Core Banking System, i.e., CA/SA Significant Movement Report, CA/SA with increase/decrease of P500,000 or more - Base60 AML System Alerts - Public Information • Submit Suspicious Transaction Report (STR) and other reports and documents to CD as required/necessary and safe keep reports and pertinent documents accordingly
		• Execute order or instruction received as to: - Notice of Freeze Order (NFO) - Lifting of freeze status of accounts - Authority/resolution to inquire into Bank Deposits
		• Review and approve Enhanced Customer Risk Assessment Form (ECRAF)
		• Review and approve alerts
		• Monitor, validate and report if deemed suspicious unusual movements and activities of accounts to AML Compliance Department particularly if said account is subject of: - STR - Authority/resolution to inquire into Bank Deposits
		• Dispose alerts in Base60 AML System within their limits • Promptly attend to AML alerts
	• Reserve Team Lead, Quality Assurance Officers and Assistant Quality Assurance Officers or its equivalent for HO Units	• Review AMLA CTR/STR reports, if accurately and timely reported
		• Ensure Officers and Employees strictly comply with the guidelines on: - Customer assessment - Opening of account - Record keeping
		• Ensure their respective Branches/HO Units' compliance with the MTPP of the Bank
	• Business Managers or Branch Service Heads and Senior Management *(refer to Part II*	• Approve account opening of high risk accounts as determined by SOs

Unit	Person Responsible	Responsibilities
	no. 25 for the complete definition of Senior Management) or its equivalent for HO units	
Compliance Division (CD)	• AML Compliance Officers	• Design and implement an effective training program in money laundering and terrorist financing prevention
		• Ensure compliance of concerned HO Units/ Branches to the: - Notice of Freeze Order (NFO) - Lifting of freeze status • Authority/resolution to inquire into Bank Deposits
		• Circulate to HO Units/Branches the list of individual and business entities involved in money laundering per mandate and issuance of BSP or AMLC
		• Confirm with or through a letter or written communication with AMLC the following: - Notice of Freeze Order (NFO) - Authority/Resolution to Inquire into Bank Deposits received by the Bank - Lifting of freeze status on affected accounts before the expiration date of freeze order • The letter should be reviewed by the designated AML lawyer of LSG for any legal implications
		• Prepare and submit the duly approved STR to AMLC Secretariat • Submit/Upload the Suspicious Transaction Report (STR) to the AMLC portal
		• Submit/Upload the Covered Transaction Report (CTR) to the AMLC portal
		• Prepare memoranda and correspondences for submission to the AMLC and other regulatory agencies
		• Sign reports as may be delegated by the Chief Compliance Officer
		• Monitor the Base60 AML System - Send monthly reminder to all Branches / HO Units to dispose alerts within five (5) banking days - Refer non-compliance to prescribed alert disposal period to the BBG Head / CLG Head / HO Group Heads for appropriate action - Dispose alerts requiring CD approval within five (5) banking days, for STR
		• Act as Secretariat to AML Committee

Unit	Person Responsible	Responsibilities
		• Assist the Branches/HO Units in the preparation of STR and other required reports
		• Ensure reports and pertinent documents related to AMLA are safe kept accordingly • Review and analyze large transactions of branches • Keep AML Base60 system up-to-date • Verify newspaper reports allegedly related to AML • Maintain and regularly update watchlist database in AML System • Monitor high risk accounts based on newspaper reports • Perform all other functions and responsibilities as specified under the Job Description
	• Chief Compliance Officer / AML Compliance Department Head	• Conduct the required AML Education and Training Program
		• Recommend approval of STR and other required reports to AML Committee for submission to AMLC and other Government offices and agencies
		• Report AML issues to AML Committee, Corporate Governance Committee and the Board of Directors (BOD)
Legal Services Division (LSD)	• Designated Legal Officer	• Confirm authenticity of the following orders with the issuing Court: - Notice of Freeze Order (NFO) - Lifting of Freeze Order - Authority to Inquire into Bank Deposits
		• Submit the detailed "Written Return" report to the issuing Court and AMLC
		• Provide legal assistance as to: - Review of Court notices, replies and reports received or submitted to the AMLC or other concerned government agencies - Preparation of pleadings, references, briefs and evidences - Representation of the Bank in any Philippine Courts
AML Committee	• Chairman and Members	• Approve STR for submission to AMLC
		• Determine the safety and protection assistance to be provided to Bank employees in relation to compliance to AMLA
		• Determine issues and reports to BOD regarding AMLA implementation, sanctions as deemed necessary and other matters requiring BOD attention

PART V
GENERAL PROVISIONS

PART V: GENERAL PROVISIONS

The General Provisions shall provide guidance to the Authorized Personnel of Compliance Division and/or branch/unit/subsidiary/affiliate in the administration, implementation, updating, dissemination, and ensuring compliance with relevant laws and regulations of this Money Laundering and Terrorist Financing Prevention Program (MTPP).

5.1 THE BOARD OF DIRECTORS (BOD) AND SENIOR MANAGEMENT

a. It shall be the ultimate responsibility of the BOD to fully comply with the provisions of the AMLA including its Revised Implementing Rules and Regulations (RIRR)

b. The BOD, thru its Corporate Governance Committee, shall be apprised as the need arises during meetings by the Bank Compliance Division (CD) on matters relating to Anti-Money Laundering (AML)

5.2 THE AML COMMITTEE (AMLCOM)

The AML Committee shall be a BOD-approved committee, duly constituted to assist in the implementation of the Bank's compliance with AMLA and all related external policies and guidelines.

It shall take the lead in carrying out the Bank's policies and procedures to ensure that the requirements of the law are fully complied with and the covered and suspicious transactions are accurately reported in a timely manner.

a. Membership

The AML Committee shall be composed of the following regular members:

1. Chief Compliance Officer (Chairman)
2. Head, Risk Management Division (Vice Chairman)
3. Head, Legal Services Division (Member)
4. Head, Centralized Operations Group (Member)
5. Deputy Head, Consumer Lending Group (Member)

Except for the Chief Compliance Officer, the regular members may appoint in writing an alternate member who shall be attending the AML Committee meetings, with full power and authority to decide and/or vote on issues brought before the Committee.

In the event a regular member abstains in a case by reason of conflict of interest, the remaining regular members shall appoint an interim member to ensure the case at hand is expeditiously resolved in compliance with the AML laws and regulations. For purposes of this Charter, "conflict of interest" shall refer to a situation whereby a member is involved in the case pending before the Committee which could possibly affect the decision of the said member.

b. Meeting

The AML Committee of the Bank shall meet and convene at least every month or as often as may be necessary. Other resource speakers such as Branch Officers and staff may be invited to the meeting, particularly when there are specific AML issues to be addressed.

In lieu of physical meetings, issues or items for confirmation or approval may be communicated through email using the Office365 email of the AML Committee Secretary or its duly appointed Assistant AML Committee Secretary and members of the Committee.

c. Quorum

Majority of the members present shall constitute a quorum.

d. Responsibilities of the Committee

The AML Committee shall be vested with the following responsibilities and authority:

1. Conduct or authorize an inquiry into any matter within the scope of its responsibilities.

2. Oversee the Bank's compliance strategy with respect to the AML Law by:
   - Recommending new policies and procedures to ensure sustained compliance by the bank to AML/CFT laws, regulations and implementing guidelines.
   - Ensuring that an adequate training program is provided to all officers and staff concerned.

3. Call any unit of the Bank for assistance in carrying out its duties and facilitate the continuing adoption of a risk-based approach to AML and terrorist financing, documenting its strategy as follows:
   - Risk Identification
   - Bank's system to assess the identified risk
   - Controls to mitigate risks are effectively implemented
   - Monitor adequate reporting system if in place

4. Upon the endorsement of and based on the RISA submitted by the branch/unit and facts presented by the AML Compliance Officer, the AML Committee shall review and confirm whether or not to file suspicious transaction report, as well as recommend other appropriate actions on the following:
   I. Transactions of a client who is a subject of a negative news report by mainstream media, publication or outlet;
   II. Alert due to a possible match in any of the watchlist on sanctioned individuals or entities provided by the Philippine or foreign government or institutions (i.e. OFAC, UN, EU, HMT);
   III. Alert pertaining to cross-border inward or outward remittance transaction wherein the sending party is a non-banking institution, amounting to at least Php100,000,000.00 or its foreign currency equivalent;
   IV. Transaction, action or alert originally determined as not suspicious by the branch or business unit but is subsequently recommended as suspicious transaction by Compliance Division upon further review.

V. The decision on filing of STR shall be based on the majority vote of the members present constituting a quorum.

5. Recommend directives for the close monitoring and conduct of review/assessment of the business relationship of the customers/accounts subjected to enhanced due diligence regardless of the decision whether to file STR or not. The recommendation may include the issuance of a resolution on whether to retain as active customers, close the account or reject the business relationship, among others, as appropriately determined by the Committee.

6. Refer to appropriate unit(s) of the Bank the fact-finding or investigation of Bank employees for any violation of the Bank Code of Ethics other than AMLA Laws.

7. Address and resolve significant AML issues and concerns from operating and business units of the Bank.

8. Oversee and regularly monitor the status and action plans resolved in relation to AML Compliance.

9. Review, discuss and take appropriate action on any request from the BSP and/or AMLC, subject to existing laws and regulations.

10. Provide policy direction in the implementation of the AMLA and other applicable laws, rules and regulations.

11. Monitors compliance to AMLC reporting of covered and suspicious transactions.

12. Check adequacy of preparations made for the annual BSP Examination.

e. The AML Committee Secretary

The AML Compliance Department Head shall be the Secretary of the Committee and shall be responsible for the following:

1. Keeping of records and documents of the Committee;
2. Administration and documentation of all Committee activities and actions;
3. Communicating, coordinating, and/or liaising with other units or branches of the Bank, government and other regulatory agencies on the activities, directives, and resolutions of the Committee;
4. Preparation of the minutes of Committee meetings;
5. Preparation of presentation materials, reports or other documents for, or on occasion of, Board or management meetings;
6. Such other responsibilities as may be determined by the Committee necessary to achieve the objectives under this Charter; and
7. Appoint an AML Committee Assistant Secretary who will be responsible for assisting the AML Committee Secretary in performing the preceding functions. The assistant secretary shall be an officer within the AML Compliance Department with a rank of at least supervisor.

f. Reporting Line

The Committee through the Compliance Division shall submit report to the Corporate Governance Committee (CGCOM) every other month. The report should include CTR statistics, summary of STRs submitted to AMLC, new regulations relevant to AML, status of AML trainings for employees, status of deliverables under the BSP Report of Examination, and such other relevant matters.

Minutes of the meetings and any other resolutions/decisions made by the AML Committee shall be presented to the Corporate Governance Committee for notation and information during the regular Corporate Governance Committee meeting. Any directives from the Corporate Governance Committee shall likewise be presented and communicated to the AML Committee through the Compliance Division.

g. Voting Requirements

Decision on the disposition of an incident of money laundering concern shall require majority vote (50%+1) of ALL members of the Committee in the meeting called for that purpose. The voting process shall not take more than two (2) banking days from the date of endorsement of the AMLCOM Secretariat. The date of final decision of the Committee shall as well be based on the time of occurrence. Shall the body reach a final decision later than 3PM, the decision shall be taken as occurred the next working day.

For incidents requiring urgent disposition, voting for the decision may be done via Office365 Email, provided that physical or electronic copy of the report has been provided to the Members of the Committee prior to the voting. Results of the voting via Office365 Email shall be ratified by the quorum of the attending members of the Committee on the immediately succeeding meeting.

Members of the Committee who are directly or indirectly involved in the decision of a subject matter of money laundering concern, shall inhibit from voting on a decision affecting such.

In case majority vote cannot be established within the AML Committee, the case in point shall be elevated to the Corporate Governance Committee for final disposition.

h. Relationship with Other Units

The AML Committee is to coordinate its efforts with other units of the Bank in order to effectively carry out its mandate.

i. Amendments

Review of the AML Committee Charter shall be made continuously and amendments shall be proposed as and when necessary to ensure compliance with the requirements of AML laws and regulations.

5.3 THE COMPLIANCE DIVISION

Management and implementation of the Money Laundering and Terrorist Financing Prevention Program (MTPP) shall be the primary task of Compliance Division. To ensure its independence, it shall have a direct reporting line to

the Board of Directors or a Board Level Committee on all matters related to AML/TF compliance and risk management. The Compliance Division shall be principally responsible for the following functions under this MTPP:

1. Ensure compliance by all responsible officers and employees with Anti-Money Laundering Laws, implementing rules and regulations, and the Bank's MTPP. It shall conduct periodic compliance testing which covers, among others, evaluation of existing processes, policies and procedures including monitoring of performance by staff and officers involved in Money Laundering or Terrorist Financing, reporting channels, effectiveness of AML Transaction Monitoring System, and record keeping through sample testing and review of audit or examination reports. The results shall be reported to the Anti-Money Laundering Committee, and to the Corporate Governance Committee or to the Board;

2. Ensure that infractions discovered by either by Internal Audit or by Special or Regular Examination of the BSP and other applicable regulator are immediately corrected;

3. Inform all responsible officers and employees of all resolutions, circulars and other issuances by the BSP and AMLC in relation to matters aimed at preventing Money Laundering or Terrorist Financing;

4. Alert Senior Management, the Board of Directors or Corporate Governance Committee, and AML Committee if it believes that the Bank is failing to appropriately address anti-money laundering and terrorist financing issues; and

5. Organize the timing and content of AML Training of officers and employees including regular refresher trainings in coordination with HRD CBS Academy.

5.4 THE CHIEF COMPLIANCE OFFICER (CCO)

a. The Chief Compliance Officer (CCO) shall be primarily responsible for the management of the day-to-day operations of the Compliance Division. In the absence of an official designation, the CCO shall act as the de facto AML Compliance Officer who will be the lead implementer of the Bank's Money Laundering and Terrorist Financing Prevention Program (MTPP) and will serve as the primary liaison between the BSP and AMLC in matters relating to the Bank's AML/CFT compliance.

b. It shall report to the BOD, through the BOD-designated Corporate Governance Committee and AML Committee, on matters related to AML, Terrorist Financing, compliance and risk management in order to ensure the independence of the office, such as:

    a. STR submitted for the period
    b. Results of its monitoring activities
    c. Notices of Freeze Order (NFO), Inquiry Order and other related Orders issued by the Courts
    d. Completeness of documents related to NFO and Inquiry Order
    e. Status and update on AML ratings
    f. AML-related news articles
    g. CD investigation repots related to AML
    h. Other AML-related issues

c. Principal Functions

1. Ensure compliance by all responsible officers and employees with the AMLA, as amended, the RIRR, applicable BSP regulations and its own MTPP.

    a) It shall conduct periodic compliance checking.
    b) It shall also report compliance findings to the BOD, Corporate Governance Committee and AML Committee.

2. Ensure that infractions discovered either by internally-initiated audits or by special or regular examination conducted by the BSP, are immediately corrected;

3. Inform all responsible officers and employees of all resolutions, circulars and other issuances by the BSP and the AMLC in relation to matters aimed at preventing money laundering and terrorist financing;

4. Alert Senior Management, the BOD, Corporate Governance Committee and AML Committee if it believes that the Bank is failing to sensibly address anti-money laundering and terrorist financing issues; and

5. Organize the timing and content of AML training of officers and employees including regular refresher trainings.

5.5 THE UNIT COMPLIANCE COORDINATORS (UCC)

The Branch Service Head for branches, and the designated/appointed officer for head office units, shall act as Unit Compliance Coordinators and shall perform the following functions:

1. Assist the Compliance Division in the implementation of the applicable provisions of this MTPP.

2. Serve as liaison between the Branch/Unit and Compliance Division on issues pertaining to AML/CFT compliance, AML Testing, regulatory examination or the implementation of the applicable provisions of this MTPP.

3. Review and assess the business unit's compliance to laws, regulations and the applicable provisions of this MTPP.

4. Ensure that policy memorandums issued by the Compliance Division pertaining to AML/CFT compliance are timely disseminated and discussed to the branch/unit.

5. Ensure that all personnel of the branch/unit have updated AML/CFT training as required in this MTPP.

6. Report all audit or testing findings to the Compliance Division relating to infractions of the applicable provisions of this MTPP or violations of the AML/CFT laws and regulations.

7. Develop relationship with Unit Compliance Coordinators of other business units and close coordination with Compliance Division.

8. Promote compliance guidelines, procedures, policies and practices that retain or enhance compliance with the applicable provisions of this MTPP.

5.6 DUE DILIGENCE RESPONSIBILITY

It is the responsibility of the Bank (its branches/business units), through its authorized personnel responsible of conducting due diligence and its approval, to know the customer. The due diligence process does not stop at account opening, but is a continuous process from the application of business relationship up to its ultimate termination. Thus, due diligence is the process embedded to CBS's on-boarding, on-going monitoring and updating policies and procedures, for the sole purpose of continuously knowing the clients, including their affairs that may affect our business relationship with them.

5.7 REVIEW AND UPDATING OF THE MTPP

This MTPP shall be reviewed / updated every two (2) years by the Compliance Division. The revised manual must incorporate changes in AML policies and procedures, latest trends in money laundering and terrorist financing typologies and latest pertinent BSP issuances. Any revision or update in the MTPP shall likewise be approved by Corporate Governance Committee and the Board of Directors.

The Branch Operations Manual and other internal policies and procedures relevant and consistent to the provisions of this MTPP such as training, KYC, transaction monitoring, shall form part of this MTPP.

5.8 DISSEMINATION POLICIES AND PROCEDURES

AML Compliance Department will issue AML Bulletins or Advisories for immediate adoption into Bank's Policy and implementation of newly issued BSP Circulars, updates on Banking Laws, Rules and Regulation. The following issuances will also be used to issue clarification on the significant provisions of BSP Circulars, banking Laws, Rules and Regulations. These issuances shall be implemented on the dissemination of this MTPP or any portions or interpretations thereof.

5.8.1 Issuances from AML Compliance Department shall be categorized into the following:

a. AML Bulletin – this will cover AML policy issuances and amendments, implementing guidelines or procedures of the policies, regulations or directives, and official interpretations/clarifications thereof. This may be communicated bank-wide or to specific applicable units of the Bank.

b. AML EyeWatch – this will cover warning communications to restrain and caution branches and business units regarding individuals and entities subject of regulatory investigation and/or sanction.

c. AML Reminder – this will cover reminders of any of the above, existing policies, an event, and existing regulation or law relevant to the AML subject.

5.8.2 Issuances of the AML Compliance Department shall be subject to the following lines of approval:

AML Issuances	AML Compliance Department Head	Chief Compliance Officer
AML Bulletin	Required	Not Required, except in Advisories specifically stated by the CCO
AML EyeWatch	Required	Not Required
AML Reminder	Required	Not Required

5.9 RISK MANAGEMENT

As part of sound risk management, China Bank Savings Inc. developed policies and practices to ensure that risk associated with money-laundering such as counterparty, reputational, operational, and compliance risks are identified, assessed, monitored, mitigated and controlled, as well as to ensure effective implementation of the regulations, to the end that China Bank Savings, Inc. shall not be used as a vehicle to legitimize proceeds of unlawful activity or to facilitate or finance terrorism.

5.10 INTERNAL AUDIT

The internal audit function associated with money laundering and terrorist financing shall be conducted by qualified personnel who are independent of the office being audited. It must have the support of the Board of Directors and Senior Management and have direct reporting line to the Board or Audit Committee. The Internal Audit shall have the following functions under this Manual:

1. To conduct periodic and independent evaluation of the: (a) efficiency of the electronic monitoring and reporting system, (b) risk management, (c) degree of adherence to internal control mechanisms related to the customer identification process, e.g., determination of the existence of customers and completeness of the minimum information and/or documents establishing the true and full identity of, and the extent and standard of due diligence applied to, customers, (d) covered transaction and suspicious transaction reporting, (e) alerts dispositions (f) record keeping and retention, and (g) adequacy and effectiveness of other existing internal controls associated with money laundering and terrorist financing; and

2. To communicate on a timely manner, the results of the internal audit to the Board of Directors and the Compliance Division. The Compliance Division shall regularly submit reports to the Board to inform them of management's action to address deficiencies noted in the audit.

The AML Compliance Department shall also extend support to the internal audit in its audit of branches/business units' compliance with this MTPP and AML/CFT laws and regulations.

5.11 HUMAN RESOURCES DIVISION

1. The Human Resources Division shall institute adequate screening and recruitment procedures to ensure high standards when hiring employees;

2. It shall coordinate with the Compliance Division on the schedule of the training and ensure that all concerned officers and staff, including new employees are given appropriate training on money laundering and terrorist financing prevention;

3. It shall ensure that logistical support is provided to the AML training program of the Bank.

5.12 KNOW-YOUR-CUSTOMER (KYC) RESPONSIBILITY

It is the responsibility of the Bank (its covered person subsidiaries/ affiliate/ branch/ units), through its authorized personnel responsible of conducting due diligence and its approval, to know the customer. The KYC process does not stop at account opening, but is a continuous process from the application of business relationship up to its ultimate termination. Thus, KYC is the process embedded to CBS's on-boarding, on-going monitoring and updating policies and procedures, for the sole purpose of continuously knowing the clients, including their affairs that may affect our business relationship with them.

5.13 KNOW-YOUR-EMPLOYEE (KYE) RESPONSIBILITY

Based on submitted documents and information, credit and court checking conducted by the Bank, conduct due diligence to ascertain if an employee-applicant qualifies based not only on his/her professional and career background but also has on passing the requirements under AMLA.

1. Family/Personal Background

   Determine based on the Background Investigation report, if employee-applicant has family members/associates who are engaged in activities prone to ML/TF or other criminal acts. Check if candidate falls under the high-risk category as defined for customers, such as PEP or closely related to one.

2. Credit Background

   Determine if employee-applicant has outstanding overdue loans with any bank or financial institution or past records show default in credit obligations.

3. Criminal Background

   If with same name in NBI or court checking, require the candidate to secure court clearance

4. Watchlist

   Determine if employee-applicant is not in the watchlist of the BSP for Bank employees, nor is in the watchlist of the AMLC for M/L and T/F offenses and other reliable sources.

5.14 INTERPRETATION OF THE MTPP PROVISIONS

The Compliance Division shall have the sole authority to issue interpretations and specific implementing guidelines pertaining to the provisions of this MTPP.

The provision in this section does not include statement of facts/provisions/plain meaning of the provisions, which are provided in regular inquiries.

5.15 MTPP AS MINIMUM STANDARDS

The provisions of this MTPP shall serve as minimum standards in terms of compliance with the AML laws, rules and regulations. The existing operational manuals of applicable units/departments/divisions shall be amended to comply with the minimum standards provided herein. However, no operational manual or any parts thereof shall be amended pursuant to this MTPP, if such operational manual or any parts thereof provides higher standards of compliance with AML/CFT laws, rules or regulations than the equivalent portions or provisions of the MTPP.

Such amendment to the operational manuals to comply with the minimum provisions of this MTPP may be in the form of providing reference to this MTPP if such provision is impractical to copy in the operational manuals.

5.16 REPEALING PROVISION

Any guidelines, policies, procedures and policies pertaining to money laundering and terrorist financing, including previously issued AML bulletins and compliance related communications, that is contrary to the foregoing provisions of this MTPP are deemed amended and repealed.

PART VI
CUSTOMER ON-BOARDING DUE DILIGENCE (CODD)

PART VI: CUSTOMER ON-BOARDING DUE DILIGENCE (CODD)

The objective of the KYC policy is to prevent China Bank Savings, Inc. from being used, intentionally or otherwise by criminal elements for money laundering and terrorist financing activities. The policy shall also ensure that the financially or socially disadvantaged are not denied access to financial services without sacrificing the requirements of AMLA and the applicable provisions of this Manual.

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. The customer due diligence system of the Bank includes the following:

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;

2. Identifying the beneficial owner and taking reasonable measures to verify the identity of the beneficial owner;

3. Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship; and

4. Conducting on-going 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 Bank's knowledge of the customer, their business and risk profile.

The Bank shall be required to conduct customer due diligence:

1. Prior to establishment of business relationship with the customer;

2. Upon scheduled updating of customer records, per policy;

3. It undertakes any occasional but relevant business transaction for any customer who has not otherwise established relations with the covered person.

   Relevant business transaction shall refer to (a) a transaction exceeding Php100,000 (except money changing/remittance transactions), (b) two or more transactions believed to be linked with an aggregate value exceeding Php100,000; or in relation to remittance and money changing transactions, any transaction or two or more transactions believed to be linked, with an aggregate value exceeding Php5,000.

4. There is a suspicion of money laundering or terrorism financing;

5. There is doubt about the veracity or adequacy of previously obtained customer identification data.

6. Recent material information that warrants immediate updating of customer records.

6.1 WHO IS THE CUSTOMER

Client/customer refers to any of the following:

1. Any person or entity who keeps an account, or otherwise transacts business with the Bank;
2. Any person or entity on whose behalf an account is maintained or a transaction is conducted, as well as the beneficiary of said transactions;
3. Beneficiary of a trust, an investment fund or a pension fund;
4. A company or person whose assets are managed by an asset manager;
5. A grantor of a trust; and
6. Any insurance policy holder, whether actual or prospective (for insurance company)
7. Transactor

6.2 CUSTOMER ACCEPTANCE AND IDENTIFICATION POLICY

The following Customer Acceptance Policy indicating the criteria for acceptance of customers shall be followed in the Bank. The New Accounts, Branch Service Head or Business Manager of all branches or business units (collectively referred as Authorized Personnel) shall strictly observe the following prior to customer on-boarding:

1. Numbered Accounts – No peso or foreign currency non-checking numbered accounts shall be allowed without establishing the true and full identity and existence of customers and applying enhanced due diligence.

   Peso and foreign currency non-checking numbered accounts existing prior to 17 October 2001 shall continue to exist but the Authorized Personnel shall establish the true and full identity and existence of the beneficial owners of such accounts and applying enhanced due diligence.

2. Prohibited Accounts – Accounts shall only be maintained in the true and full name of the account owner or holder. The provisions of existing law to the contrary notwithstanding, (i) anonymous accounts, (ii) accounts under fictitious names, (iii) accounts under alias/A.K.A. names, (iv) numbered checking accounts, (v) accounts for shell banks, (vi) bearer share companies, and (vii) other similar accounts shall be absolutely prohibited.

3. Doing Business Under (DBU) Accounts – Customers using their personal account to facilitate transactions of their business shall bear the naming convention in their Account Name or Statement of Account (SOA), i.e. “Proprietor’s Name_Doing Business Under (DBU)_Business Name”. The necessary documents for Sole Proprietorship shall be required.

4. The Authorized Personnel shall collect documents and other information from the customer depending on perceived risk and keeping in mind the requirements of Republic Act No. 9160 as amended, otherwise known as the Anti-Money Laundering Act of 2001, its revised implementing rules and regulations and Bangko Sentral ng Pilipinas (BSP) Circular No. 706 or the Updated Anti-Money Laundering Rules and Regulations (*as amended by BSP Circulars 950 and 1022*).

5. The Authorized Personnel shall close an existing account or shall not open a new account where it is unable to apply appropriate customer due diligence measures i.e., the Authorized Personnel is unable to

verify the identity and/or obtain documents required as per the risk categorization due to non-cooperation of the customer or non-reliability of data/information furnished to the Authorized Personnel. The Authorized Personnel may also consider filing a suspicious transaction report (STR) in relation to the customer, if the circumstances warrant such filing.

6. The Authorized Personnel shall exert all efforts, not contrary to any of the provisions of the MTPP and the Bank's policy, to ensure that these measures do not lead to the inconvenience of the customer. When closure of the account is appropriate, the client shall be notified of such closure in writing, documenting the general reasons for the closure of the account. Such notice will be done at least fifteen (15) days prior to the closure of the account, except when such prior notice will deem to "tip-off" the client. Compliance Division or Legal may recommend immediate closure depending on the circumstances, in consideration of the "tipping-off" prohibition and other applicable provisions of this MTPP.

7. The Authorized Personnel shall ensure that the following customer due diligence procedures upon on-boarding of the customer is being observed consistently:

    a. Conduct Face-to-Face contact
    b. Gathering of Information, Identification and Other Documents
    c. Watchlist and PEP List Screening
    d. Customer Risk Profiling
    e. Conduct of the Required Due Diligence

    The Bank shall begin business relationship only to those new customers passing the foregoing Customer On-boarding Policy.

6.3 CUSTOMER ON-BOARDING POLICY

The following are the Customer On-boarding Procedures which discuss the processes to be followed by the Bank before acceptance or continuance of the business relationship with a customer. Such procedures shall apply in full to applicable individual or corporate clients.

The New Accounts, Branch Service Head or Business Manager of all branches or business units (collectively referred as Authorized Personnel) shall accept a customer after passing the on-boarding processes enumerated below.

For an authorized signatory of a corporate customer, who has no account with the Bank and who is not transacting with the branch or unit as an authorized signatory, the minimum mandatory information shall be required for gathering. Screening against watchlist shall still be performed. The rest of the due diligence procedure shall be optional depending on the assessment of the branch/unit authorized officer and approver. However, if such authorized signatory subsequently decides to transact with the branch or unit, the full applicable requirements of this MTPP shall be complied with prior to such transaction.

Transactors shall also be risk profiled.

6.3.1 Face-to-Face contact

6.3.1.1 No new account shall be opened and created without face-to-face contact and personal interview between the Bank's Authorized Personnel and the prospective customer. However, the responsibility to conduct face-to-face contact and certain parts of the due diligence may be transferred/assigned in the following instances:

a. Account opened through a trustee, agent, nominee or intermediary
b. Outsourcing of the gathering of minimum information and/or documents and face-to-face contact
c. Third Party Reliance

6.3.1.2 At a minimum, the Authorized Personnel shall perform the following face-to-face contact activities:

a. Pre-screening of the client, which includes:

- Briefing the prospective client on the requirements and features of the account being opened and/or transaction being conducted.
- Requesting the client to accomplish the Account Opening Documents and submit valid photo-bearing ID enumerated in section 6.3.2.2 of this Manual.
- Carefully examining the identification documents presented and look for any sign of forgery or alterations.
- Checking if the Account Opening Documents are duly filled-out.

b. Interview with the client – New Accounts / Account Officer of Acquired Asset / Consumer Lending / SME Lending / APD Lending Groups and other applicable Head Office Units:

- Conduct an interview with the client. Using the Enhanced Customer Risk Assessment Form (ECRAF), perform exploratory questioning to fully establish the client's identity and determine the risk classification of the client.
- During the interview, the Authorized bank personnel should observe any suspicious or unusual behavior of the client that may require Enhanced Due Diligence on the client's identity.

c. The Authorized Personnel should carefully examine the information provided by the client through the application/disclosure forms and interviews, and look for the following indicators/red flags that may lead to further probing of the client:

- Minimal, vague or fictitious information provided. An individual provides minimal, vague or fictitious information that the bank cannot readily verify.

- Lack of references or identification. An individual attempts to open an account without references or identification, gives sketchy information, or refuses to provide the information needed by the bank.
- Non-local address. The individual does not have a residential or business address in the bank vicinity or jurisdiction, and there is no apparent legitimate reason for opening an account with the bank.
- Customers with multiple accounts. A customer maintains multiple accounts for no apparent legitimate reason. The accounts may be in the same names or in different names with different signature authorities.
- Accounts used as temporary repository for funds. The customer appears to use an account as a temporary repository for funds that ultimately will be transferred to other bank or withdrawn.

6.3.1.3 The use of Information and Communication Technology in the conduct of face-to-face contact may be allowed and shall be limited to opening of Peso Savings Account of the following individual clients:

a. Clients who are opening for purposes of payroll account.
b. Clients classified as Low Risk.

The face-to-face contact through the use of Communication Technology shall be subject of the following:

a. It shall be subject to minimum mandatory information/document for individual client.
b. Branch/unit is in possession of and has verified the identification documents submitted by the prospective client prior to the interview.
c. The entire procedure is documented.
d. The proof of face-to-face contact through the use of technology such as the screen shot during interview shall form part of the KYC documents on file.

The conduct of face-to-face contact through the use of Communication Technology shall be in accordance with the approved manual and procedure of concerned unit and shall form part of the MTPP.

6.3.1.4 On-boarding indicators warranting further action. The following indicators are sourced from the Amended Registration and Reporting Guidelines (ARRG) of the AMLC, and recommendations of the Compliance Division. The listing below is not exhaustive. Indicators of similar type or nature, or an entirely new indicator may warrant further action.

The indicators below shall serve as a trigger to the Authorized Personnel conducting the due diligence, to gather more information so that further appropriate action can be taken (*i.e. classify as High Risk or deny business relationship and/or File an STR*). The presence of any of the indicators below does not necessarily require outright High Risk classification,

denial of business relationship or filing of STR. The Authorized Personnel must satisfy him/herself that presence of any of the indicators below are reasonably justified and such justification be documented in the Enhanced Customer Risk Assessment Form (ECRAF) or any other form recommended by Compliance Division.

However, if the customer has two (2) or more indicators coming from either items "a", "b", "c", "d" or "e" below, regardless of justification, such will be treated as "Suspicious Indicator" per section 6.8(n) below and the ECRAF policy at the very least. Thus, if denial of business relationship is not warranted in this instance, the client will be classified as High Risk and enhanced due diligence will be applied.

Absence/lacking of acceptable justification on any of the identified indicators shall warrant tagging of Suspicious Indicator in the ECRAF (making the customer High Risk), or denial/termination of business relationship and/or filing of suspicious transaction report (STR), whichever is deemed appropriate.

a. Corruption Related:

- Client is unable or reluctant to provide details or credible explanations for establishing a business relationship or opening an account with the branch/bank
- Type of business is commonly identified to have dealings with the government or any of its subdivision (e.g. Construction), and one of the owners, beneficiary or beneficial owner, senior officer or signatory is a PEP

b. Cross-border investment fraud:

- Accountholders or clients are individuals or very recently registered entities (e.g. with SEC or DTI). There may be common signatories for the accounts opened. Normally, the signatory is not an incorporator. In some instances, the individuals opening the account present themselves as owners of a domestic company, branch head or consultant of a foreign entity
- An individual or consultancy firm sets-up two or more companies, mainly engaged in trading, retail and call center business
- Multiple companies are linked by common addresses and signatories. These companies maintain accounts at different banks to conceal their business activities
- Sole proprietorship set-up as consultancy providing technical services (e.g. IT) with expected regular remittance from abroad

c. Drug related transactions:

- Persons using other names/alias/A.K.A.

- Persons using different IDs with inconsistent information such as: name, birth date, address
- Sole proprietorship business under the name of a Filipino, substantially managed by an authorized representative who is not a relative, specially a foreigner representative
- Agent insisting to open an account for the principal without personal appearance of the latter
- Prospective customer tries to deposit large amount of cash without visible source of funds and supporting official documents

d. Unverified banking accounts:

- Return of customer "Thank You" letter

e. Terrorist financing:

- Entities, not a positive match, but with certain details match in the sanctions lists
- Entity is a small broker/intermediary but disclosed/actual activity does not match the business profile
- A commercial entity acts as money-remittance business

f. General Areas of Suspicion:

- Customer admits to or makes statements about involvement in criminal activities
- The Authorized Personnel processing or approving the business relationship is aware that the customer is the subject of a criminal investigation
- Customer does not want correspondence sent to residential address, without acceptable/valid justification
- Customer appears to have accounts with several financial institutions in one area for no apparent valid reason
- Customer repeatedly uses an address but frequently changes the names involved
- Customer is accompanied and watched, seemingly the customer is not related to the accompanying person
- The money deposited is in unusual condition (e.g. damp, odorous, or coated with substance without appropriate reason
- Nervous or uncooperative behavior exhibited by employees and/or customers
- Customer shows uncommon curiosity about internal systems, controls and policies
- Customer has only vague knowledge of the amount of deposit or remittance expected to the account
- Customer presents confusing details about the incoming transaction or knows few details about its purpose
- Customer over-justifies or over-explains the incoming transaction

- Customer is secretive or reluctant to visit the branch
- Customer's home or business telephone number has been disconnected, or there is no such number when an attempt is made to contact the customer shortly after the opening of the account
- Normal attempts to verify the background of a new or prospective customer are very difficult
- Customer appears to be acting on behalf of a third party but does not inform the branch about it
- Customer is involved in activity(ies) out of keeping for an individual or business
- Customer appears to have recently established a series of new relationships with different financial entities
- Customer attempts to develop close rapport with the branch personnel, especially those involved in processing or approving account opening and transactions
- Customer uses aliases and a variety of addresses
- Customer spells his/her name differently from one transaction to another (e.g. account opening to deposit)
- Customer uses a post office box or general delivery address, or other type of mail drop address, instead of a street address
- Customer provides false information or information that the personnel of the bank reasonably believe is unreliable
- Customer offers money, gratuities, or unusual favors to the bank personnel for the account opening or provision of service that may appear unusual or suspicious
- Customer pays for service/open an account via financial instruments, such as money orders or traveler's checks, without relevant entries on the instrument or with unusual symbols, stamps or notes
- The branch/unit is aware that a customer is the subject of money laundering or terrorist financing investigation
- The branch/unit is aware, or becomes aware, from a reliable source (e.g. media or government agencies) that the customer is suspected of being involved in illegal activity/ies
- A new or prospective customer is known as having a questionable legal reputation or criminal background

g. Knowledge of requirements:

- Customer attempts to convince the authorized bank personnel not to complete any documentation required to complete the account opening
- Customer makes inquiries that would indicate a desire to avoid reporting
- Customer has unusual knowledge of the law in relation to suspicious transaction reporting

- Customer seems very conversant with money laundering or terrorist activity financing issues
- Customer is quick to volunteer that funds are "clean" or are "not being laundered"
- Customer appears to be collaborating with others to avoid record-keeping, customer identification, or reporting thresholds

h. Identity documents:

- Customer provides doubtful or vague information
- Customer produces seemingly false identification or identification that appears to be counterfeited, altered or inaccurate
- Customer refuses to produce personal identification documents
- Customer insist to present copies of the IDs rather than the originals
- Customer insist on using only foreign-issued IDs or unverifiable identity documents
- Customer wants to establish identity using something other than his or her personal identification documents
- Customer's supporting documentation lacks important details, such as a telephone number
- Customer inordinately delays presenting corporate documents
- All identification presented pertains to foreign countries or cannot be checked for some reason
- All identification documents presented appear new or have recent issue dates
- Customer presents different identification documents at different times
- Customer alters the transaction after being asked for identity documents
- Customer presents different identification documents each time a transaction is conducted

i. Transaction Involving accounts:

- Opening accounts when customer's address is outside the local service area
- Opening accounts in other people's names
- Opening accounts with names very close to other established business entities
- Attempting to open or operate accounts under a false name
- Account that was reactivated from inactive or dormant status suddenly sees significant activity
- Reactivated dormant account containing a minimal amount suddenly receives a deposit or series of deposits followed by frequent cash withdrawals until the transferred sum has been removed

j. Transactions involving areas outside the country:

- Customer and other parties to the planned transaction have no apparent ties to the country
- Use of credit card issued by a foreign bank that does not operate domestically by a customer who does not live and work in the country of issue

k. Personal transactions:

- Customer wishes to have credit and debit cards sent to international or domestic destinations other than his/her address
- Customer gives power of attorney to a non-relative to conduct the large transactions

l. Corporate and business transactions:

- The corporate/business client does not want to provide complete information regarding its activities
- Financial statements of the business differ noticeably from those of similar businesses
- Representative of the business avoid contact with the branch as much as possible, even if it would be more convenient for them

m. Transactions for non-profit organizations

- Absence of contributors from donors located in the country where the NPO operates/registered
- NPO's directors are outside the country, particularly if large outgoing transactions are made to the country of origin of the directors, and especially if that country is a high risk jurisdiction
- Non-profit organization with unexplained links to other non-profit organizations
- Non-profit organization appears to have little or no staff, no suitable officers, or no telephone number, which is incompatible with their stated purpose and financial flows
- Non-profit organization has operations in, or conducts transactions to or from, high risk jurisdictions

n. Suspicious indicator related to lending:

- Source of down payment is inconsistent with the borrower's background and income
- Customer shows income from "foreign sources" on loan application without providing any details when asked to provide
- Customer's employment documentation lacks important details that would make it difficult for the Bank to locate or contact the employer

- Customer's documentation to ascertain identification, support income, or verify employment is provided by an intermediary who has no apparent reason to be involved
- Customer has loans with offshore institutions or companies that are outside the ordinary course of business of the customer
- Customer offers the Bank large deposits or some other form of incentive in return for favorable treatment of loan request
- Customer asks to borrow against assets held by another financial institution or a third party, when the origin of the assets is not known
- Loan transaction does not make economic sense (e.g., the customer has significant assets, and there appears to be no sound business reason for the transaction)
- Customer seems unconcerned with terms of credit or costs associated with the completion of the loan transaction
- Customer applies for loans on the strength of a financial statement reflecting major investments in or income from businesses incorporated in countries known for highly secretive banking and corporate laws, and application is outside the ordinary course of the business of the customer
- Down payment or other loan payments will be made by a party who is not a relative of the customer
- Reluctance to use favorable facilities, for example, avoiding high interest rate facilities for large balances

6.3.2 Gathering of Information and Documents

Initially, the Authorized Personnel shall collect both the: (1) minimum mandatory information; and (2) identification documents applicable to the prospective customer (individual or corporate).

6.3.2.1 Minimum Mandatory Information

Customer Information and other related forms to be filled-out by the client prior to establishing of business relationship shall contain at least the following minimum information:

For individual/Authorized Signatories/Representative	For Corporation
1. Name of customer and/or PhilSys Number	1. Name of Entity
2. Date of birth	2. Official address
3. Place of Birth	3. Contact numbers or information
4. Address	4. Nature of business
5. Contact number or information	5. Specimen signatures or biometrics of the authorized signatory

6. Citizenship or Nationality	6. Name, address, citizenship or nationality of beneficial owner or beneficiary, if applicable
7. Specimen signature or biometrics of the customer	**For Legal Arrangement**
8. Nature of work, name of employer or nature of self-employment/business	1. Name of legal arrangement and proof of existence
	2. Address and country of establishment
9. Source of funds	3. Nature, purpose and objects of the legal arrangement
10. Tax Identification Number (TIN), Social Security System (SSS) number, or Government Service Insurance System number, as may be applicable	4. Description of the purpose/activities of the legal arrangement
	5. Expected use of the account
	6. Amount, number, type, purpose and frequency of the transaction expected
11. Name, address, date and place of birth, contact number of information and citizenship or nationality of beneficial owner, whenever applicable	7. The names of the settler, the trustee, the trustor, the protector, if any, the beneficiary and any other natural person exercising ultimate effective control over the legal arrangement

Minimum mandatory information for Individual shall also apply to signatories of a Corporate/Entity account. For non-corporate accounts (i.e. partnership, sole-proprietorship, cooperatives) minimum mandatory information for Corporation shall apply.

Identification of the beneficial owner is required under the UBO policy provided in this MTPP. The Authorized Personnel responsible for the conduct of due diligence shall identify natural person(s) passing the UBO criteria and shall record the basic information of identified beneficial owners in the UBO Determination Form (for entity/corporation).

For local banks opening or with deposit accounts, AML Due Diligence Questionnaire shall be accomplished by the client. Refer to **Annex F** for *AML Due Diligence Questionnaire for Counterparty Financial Institutions*.

For transactors, unless classified as low risk, the following information are mandatory:

1. Name of Customer and/or PhilSys Number
2. Date of Birth
3. Place of Birth
4. Address
5. Contact number or information
6. Citizenship or Nationality
7. Specimen signature or biometrics of the customer

If the transactor is considered as low risk, the following information shall suffice:

1. Full Name
2. Address
3. Date of Birth

6.3.2.2 Official Identification Documents

An official identification document refers to the following:

General Customer Type	Acceptable Official Identification Documents (IDs)
Identification Requirements for Individual Accounts	
1. Individual – Filipino Citizens	Those issued by any of the following official authorities: • Government of the Republic of the Philippines, including its political subdivision, agencies, and instrumentalities • Government-owned or Controlled Corporations (GOCCs) • Covered persons registered with and supervised or regulated by the BSP, SEC or IC
2. Individual – Resident Foreign Nationals	• PhilID and its various formats, for resident aliens • Alien Certificate of Registration (ACR) as permanent resident or Special Retiree's Resident Visa (SRRV); **and** any of • Passport or IDs issued by official authorities of the Philippines • See **Annex G** for the Amended Guidelines on Acceptable IDs of Foreign Nationals
3. Individual – Non-resident Foreign Nationals	• Passport; **and** any of • Alien Certificate of Registration (ACR) except tourist; or Special Investor's Residence Visa (SIRV); or • Other IDs issued to the non-resident foreign national, as approved by the Compliance Division

General Customer Type	Acceptable Official Identification Documents (IDs)
	• See **Annex G** for the Amended Guidelines on Acceptable IDs of Foreign Nationals
4. Individual – Filipino Students	• PhilID and its various formats; or • School ID signed by the school principal or head of the educational institution • IDs issued by the official authorities of the Philippines
Identification Requirements for Business/Entity Accounts	
5. Sole Proprietorship	a. Certificate of Registration issued by the Department of Trade and Industry (DTI) b. Special Power of Attorney (SPA), if appointed by the owner/principal c. Identification documents of the owner/principal d. Identification documents of the agent/attorney-in-fact (if appointed) e. Special licenses/certificate of registration issued by the official authorities of the Philippines *(e.g. certificate of registration for MSBs issued by Bangko Sentral ng Pilipinas)*, if applicable
6. Corporation/ Partnership/ Cooperative/ Other Entity	a. Certificates of Registration issued by the Authorized Government Agencies; b. Secondary license or certificate of authority issued by the supervising authority or other government agency, if applicable c. Articles of Incorporation/ Partnership/ Cooperation or similar official document applicable to the entity; d. Latest General Information Sheet (GIS) or similar official document *(in case GIS is not applicable)* which lists the names of directors/ trustees/ partners/ principal stockholders (or contributors) owning at least twenty percent (20%) of the outstanding capital stock (or contributions) and primary officers such as the President and Treasurer;

General Customer Type	Acceptable Official Identification Documents (IDs)
	e. Board or Partners' Resolution duly certified by the corporate/Partners' secretary, or other equivalent official document, authorizing the signatory to sign on behalf of the entity; f. Official identification documents of authorized signatories; g. For entities registered outside the Philippines, similar documents above (items "a" to "f") and/or information shall be obtained duly authenticated by the Philippine Consulate, company register or notary public, where said foreign entity is registered. This requirement shall also apply to a parent foreign entity/corporation of our corporate customer who is a branch/ office/ subsidiary affiliate registered and operating here in the Philippines. *(Note: The effects of R.A. 11232 – Revised Corporation Code of the Philippines to the above requirement shall be considered whenever a new corporation registered under the new law is applying to open an account.)*
7. For Legal Arrangement	a. Identification requirements of individuals/ signatories and/or corporation, as applicable

Students who are beneficiaries of remittances/fund transfers, who are not yet of voting age and unemployed, may be allowed to present the original and submit a clear copy of one (1) current photo-bearing school ID duly signed by the principal or head of the school.

The Authorized Personnel shall require their customers or authorized signatory to submit a clear copy of at least one (1) valid ID on a one-time basis only at the commencement of business relationship. The Authorized Personnel shall require their clients to submit an updated photo, documents and other information as provided in this policy.

In case the identification documents mentioned above or other identification documents acceptable to the Bank do 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, the Authorized Personnel may utilize some other technology to take the photo of the customer or authorized signatory.

Valid IDs include the following:

- Passport including those issued by foreign governments;
- PhilID and its various formats
- Driver's License;
- PRC ID;
- NBI Clearance;
- Police Clearance;
- Postal ID;
- Voter's ID;
- Philhealth (PHIC);
- Tax Identification Number (TIN);
- Barangay Certification;
- GSIS e-Card;
- SSS card;
- Unified Multi-Purpose ID;
- Senior Citizen card;
- OWWA ID;
- OFW ID;
- Seaman's Book;
- Alien Certification of Registration/Immigrant Certificate of Registration;
- Government Office and GOCC ID (e.g., LGU, AFP, HDMF IDs);
- Certification from the NCWDP;
- DSWD Certification;
- IBP ID;
- ID issued by the National Council on Disability Affairs (NCDA); and
- Company IDs issued by covered persons registered with and supervised or regulated either by the BSP, SEC or IC.

Identification documents, depending on the risk classification of the customer, will be subject to the following layers of review:

1. Basic Information Review – simply involves checking of information on the ID and matching it with the information provided by the customer:

    a. Matching the ID photograph with the presenter and with other ID presented. Extreme caution is required if a photo in any ID (where photo is embedded) is an exact match with another ID (for individual).
    b. Verifying the basic information with other documents presented such as name, date of birth, address (for some IDs) against CIF and other documents (for both individual/and entity/corp)
    c. Matching signature on the ID with the other documents (e.g. specimen signature)
    d. Noting the signatory of the Official Authority and the date of issuance of the ID to check if the signatory is the incumbent authority on the date of issuance

(applicable only to IDs of individual or entity/corp without security features or cannot be validated through the issuing authority)

This layer of validation is applicable to all individual customers (Low, Normal, and High).

2. Feature Inspection – involves examining the physical features of the ID, including the security features. Applicable to all individual customers (Low, Normal, High).

3. Validation with the Issuing Authority – this requires seeking certification from the issuing authority as to the authenticity of the ID presented by the client. This also includes other means of verification such as those available thru the official website of the issuing authority or thru text, if such are applicable.

   This type of validation is applicable only to High Risk clients or when authorized personnel reviewing or approving such IDs noted inconsistencies, deformity or any other signs of falsification/tampering (regardless of the customer's risk classification).

   When the photocopy of the identification documents is stamped "verified", the signing authorized personnel guarantees that the (1) Basic Information Review and (2) Feature Inspection (if applicable) have been performed. Validation with the issuing authority shall be recorded by printing the screenshot of the result of validation or through other documentation means acceptable by the court.

6.3.2.3 Deferment on Documentary Submission

In extreme cases wherein the client requires more time to submit necessary documents prior to onboarding or updating, deferment may be allowed no longer than 30 calendar days from the date of onboarding or supposed date of updating.

Requests for deferment shall be done by an officer of the branch/unit and shall have Senior Management Approval. The next table refers to the approval matrix for deferment on documentary submission:

Stage	Branch	Business Unit
Request for deferment	Branch Service Head	Officer of the Unit
Endorsement of deferment	Team Leader / Department Head	Department Head
Approval of deferment	Division Head / Group Head (must be member of Senior Management)	Division Head / Group Head (must be member of Senior Management)

Each branch or unit must have its own monitoring system for deferments. The monitoring system must be in spreadsheet/workbook form manageable via programs such as

Microsoft Excel. There shall likewise be at least one designated officer to monitor the status of the deferments.

Failure to address the deferment within the requested period shall result in account closure through this MTPP's Deposit Account/ Client Account AML Exit Policy.

Deferment on documentary submission shall not be treated as the norm. It shall only be applied if the branch or business unit has fully exhausted all efforts for the client to comply with the documentary submission. Abuse of the deferment policy is considered as an AML infraction and shall be reported to the AML Committee.

6.3.3 Watchlist and PEP List Screening

Screening for this purpose is simply searching for the name of the client if such name is included in the sanctions list and other watchlist database maintained by the Bank. Screening of prospective clients with the established watchlist database is required for the following reasons:

a. To ensure that newly accepted clients are not among those individuals or entities sanctioned due to their involvement in crimes and are included in the sanctions list of a country or group of countries;

b. To ensure that enhanced due diligence will be performed on individuals or entities with "suspicious indicator" and senior management approval will be obtained prior to the start of business relationship.

c. To provide reasonable assurance that domestic principal politically exposed persons (PEPs) are detected at the opening stage of the account, and that senior management approval will be obtained prior to the start of business relationship.

Screening shall be conducted on the following:

a. Prospective customer
b. Authorized Representative or Signatories
c. Ultimate Beneficial Owner (UBO)
d. Principal Officers (President/CEO, Treasurer), if the entity client is High Risk
e. Directors
f. Transactors

6.3.4 Negative Watchlist Verification Guidelines

6.3.4.1 What Is Negative Watchlist Verification

Negative Watchlist Verification is the process of checking the identity of a client (and ultimate beneficial owners for corporate clients) or an applicant against the watchlist

database of the bank. This is a significant part of strengthening the Know Your Client (KYC) procedure, in compliance with BSP Circular No. 706, Series of 2011.

The aforementioned process involves using the bank's AML system as the primary tool in searching for possible matches with the individuals or entities present in the bank's watchlist.

6.3.4.2 Types of Positive Match

In compliance with the 2021 Sanctions Guidelines, CBS has three (3) types of positive match, to wit:

1. Name Match – wherein the name of the client or applicant matches with one or more entries in the watchlists
2. Potential Target Match – wherein two (2) or more identifiers match with at least one entry in the watchlists
3. Target Match – wherein all identifiers match with at least one entry in the watchlists

6.3.4.3 Sources of Watchlists

The bank's consolidated watchlist is composed of two general types of watchlists: Sanctions Lists and Internal Watchlist.

1. Sanctions Lists

   Collectively, Sanctions Lists are a Database of names of personalities who are subject to different sanctions by a country or group of countries due to involvement on sanctioned activities (i.e. terrorism, drug trafficking) – OFAC, UN, EU, HMT

2. Internal Watchlist
   On the other hand, the bank's Internal Watchlist is its own database of names and other identifiers that are based from the following:

   - Subject of Negative News
   - Subject of Freeze Order
   - Subject of Suspicion of STR
   - Subject of AMLC Inquiry
   - SEC Advisories
   - PEP (Politically Exposed Persons) List
   - Anti-Terrorism Council (ATC) Designations

6.3.4.4 Screening and Scrubbing

Base60 AML System can do screening either by manual searching done by a user or by automated screening. For manual search, the results are shown on the screen, as will be discussed further in this policy. For automated screening, the system does a daily check between the customer database and the bank's watchlists. KYC Screening alerts are then generated for potential and target matches which Compliance Division shall investigate to validate the results, and file an STR if warranted.

Scrubbing refers to checking of whether a person, either natural or juridical, has a match against the bank's customer database. Similar to the methods of screening, scrubbing can be done either manually on Base60 AML System or automatically by the said system. Manual scrubbing can also be done on the bank's core banking system, but it is highly suggested to use the AML system due to its fuzzy logic.

On the day AML Compliance Department disseminates an **AML EyeWatch**, the branches/units shall **likewise check** if the names in the on-boarded customers, updated customer information, and payees of manager's checks done on that day have any match with the names in the advisory. The transaction document (deposit slip, withdrawal slip, application for MC purchase, etc.) shall have the words "no match with EyeWatch" or simply "no match", signed by the reviewing/approving officer.

Branches/units shall ensure that all clients and ultimate beneficial owners (UBOs) are included in the screening and scrubbing against the watchlist in the bank's AML System.

6.3.4.5 Effects of Verification Results on Customer On-Boarding

a. Name Match

If a Name Match occurs, the branch or business unit shall perform Enhanced Due Diligence. Should the client deemed to be of no relation to the ones in the watchlists, the on-boarding shall continue.

b. Potential Target Match

Potential Target Match may arise from initial watchlist verification or from Enhanced Due Diligence. If further probing leads to a positive match, additional actions shall be done by the branch or business unit.

IWL Code	Source	Required Action if "Potential Target Match"
ATC	Anti-Terrorism Council Declarations	• Deny business relationship • File RISA and STR

NN	Subject of Negative News	• Perform EDD to assess whether or not to accept • If accept, classify as High Risk • If deny, file a RISA and STR
FO	Subject of Freeze Order	• Deny business relationship • File RISA and STR
STR	Subject of Suspicion of STR	• Perform EDD to assess whether or not to accept • If accept, classify as High Risk
AMLCI	Subject of AMLC Inquiry	• Perform EDD to assess whether or not to accept • If accept, classify as High Risk
SEC	SEC Advisories	• Perform EDD to assess whether or not to accept • If accept, classify as High Risk • If deny, file a RISA and STR

SL Code	Source	Required Action if "Potential Target Match"
OFAC	Office of Foreign Assets Control	• Deny business relationship • File RISA and STR
UNSC	United Nations Security Council	• Deny business relationship • File RISA and STR
EU	European Union	• Deny business relationship • File RISA and STR
HMT	Her Majesty's Treasury	• Deny business relationship • File RISA and STR

c. Target Match

For Target Matches with the Sanctions Lists and the ATC Declarations, the bank shall **deny business relationship and file RISA and STR with no delay**. For other Target Matches, the process for Potential Target Match shall follow.

6.3.4.6 Effects of Verification Results on Maintenance of Customer Records

a. Name Match

If a Name Match occurs, the branch or business unit shall perform Enhanced Due Diligence. Should the client deemed to be of no relation to the ones in the watchlists, the on-boarding shall continue.

b. Potential Target Match

Potential Target Match may arise from initial watchlist verification or from Enhanced Due Diligence. If further probing leads to a positive match, additional actions shall be done by the branch or business unit.

IWL Code	Source	Required Action if "Potential Target Match"
ATC	Anti-Terrorism Council Declarations	• FREEZE the existing account/s • File FO Return, RISA, and STR
NN	Subject of Negative News	• Perform EDD and TEDD to assess to whether or not retain • If retain, update ECRAF and re-classify as High Risk • If deny, file a RISA and STR
FO	Subject of Freeze Order	• Comply with FO • Update ECRAF and re-classify as High Risk • File a RISA and STR
STR	Subject of Suspicion of STR	• Perform EDD and TEDD to assess whether or not to retain • If retain, update ECRAF and re-classify as High Risk • Assess filing of RISA and STR
AMLCI	Subject of AMLC Inquiry	• Perform EDD and TEDD to assess whether or not to retain • If retain, update ECRAF and re-classify as High Risk • Assess filing of RISA and STR
SEC	SEC Advisories	• Perform EDD and TEDD to assess whether or not to retain • If retain, update ECRAF and re-classify as High Risk • If deny, file a RISA and STR

SL Code	Source	Required Action if "Potential Target Match"
OFAC	Office of Foreign Assets Control	• Terminate existing business relationship • File RISA and STR
UNSC	United Nations Security Council	• FREEZE the existing account/s • File FO Return, RISA, and STR
EU	European Union	• Terminate existing business relationship • File RISA and STR

HMT	Her Majesty's Treasury	• Terminate existing business relationship • File RISA and STR

c. Target Match

For Target Matches with the Sanctions Lists and the ATC Declarations, the bank shall **FREEZE the existing account/s and file FO Return, RISA, and STR with no delay**. For other Target Matches, the process for Potential Target Match shall follow.

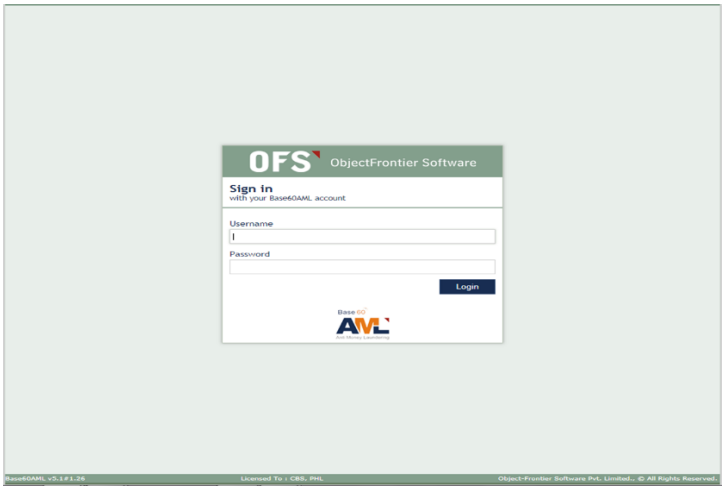
6.3.4.7 Effect of Verification Results of Scrubbing

The effect of verification results of screening shall likewise be applied to verification results of scrubbing.

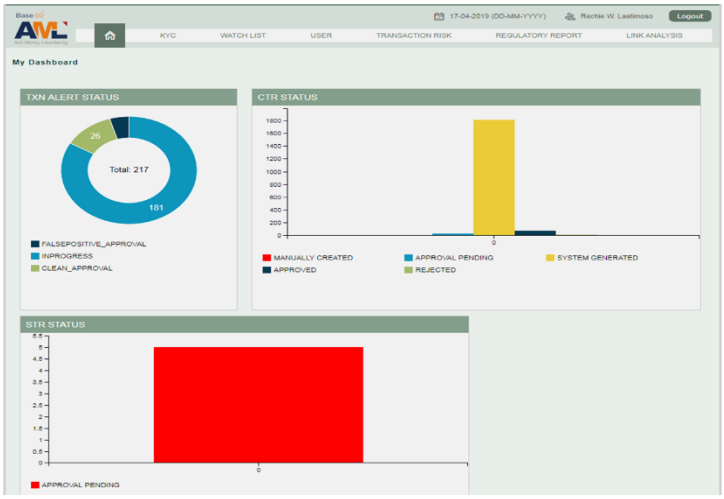
6.3.4.8 Verification Through Base60 AML System

As the bank's AML System, Base60 has a function for users to search names and other details in the bank's watchlists.

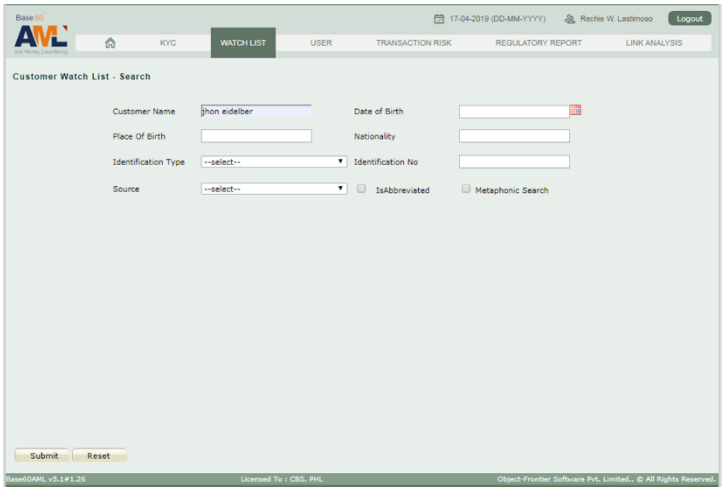
1. Go to Base60 AML System (https://cbcamlaapp:8443/aml/) and log in with your credentials.



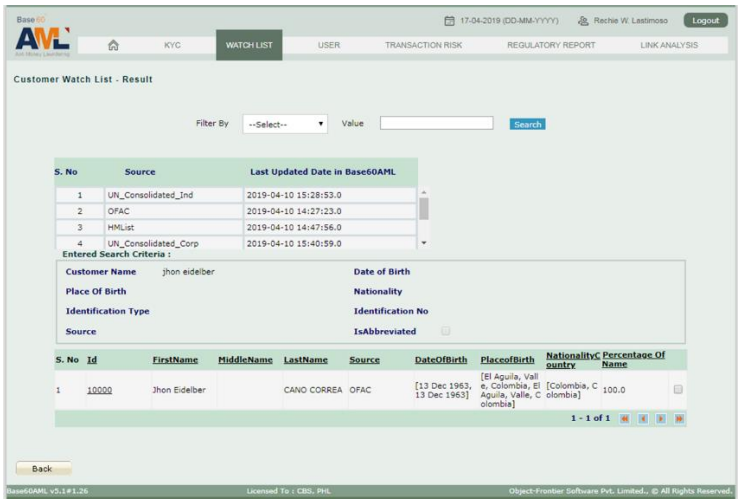
2. Proceed to Watch List→Watch List→Customer.



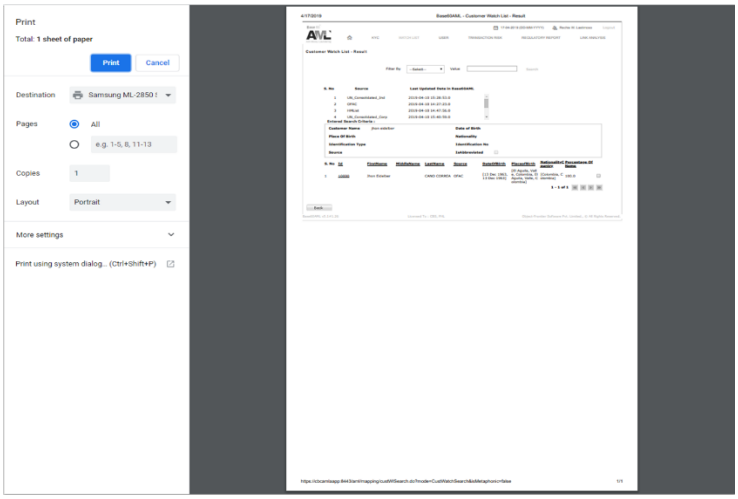
3. Type the name of the customer in the Customer Name Field and click Submit.



4. Watchlist screening results will be displayed. In this example, the customer is a positive match with the OFAC Sanctions List. Thus, the bank shall deny banking relationship.



5. Print the watchlist screening results and have it form part of the KYC folder. To print, press CTRL+P in your keyboard as displayed below.



6.3.4.9 Maintenance of Internal Watchlist

The Internal Watchlist must be updated by Compliance Division on a weekly basis or as needed. Compliance Division shall consolidate with the various lists, to wit:

- Customers with filed Suspicious Transaction Report (STR) which are the subject of suspicion.
- Customers with filed Reports on Crimes and Losses (RCL) which are the perpetrators.
- Employees of the Bank with filed Reports on Crimes and Losses (RCL) which are the perpetrators.
- Persons captured in the negative news monitoring of the AML Compliance Department and the branches.
- Persons reported in the news and/or news articles to have been identified with involvement in any of the thirty-six (36) predicate crimes of AMLA as determined and approved by the Chief Compliance Officer or its designated alternate.

The designated AML officer in-charge of uploading or updating the Internal Watchlist into the AML System shall validate the names to be added/updated via the URL of the source, prior to uploading or updating the names in the said system.

As for the Sanctions Lists, Anti-Terrorism Council Designations, and PEP List, the designated Compliance Officer shall coordinate with the Parent Bank's IT Compliance Department.

Watchlist (Sanctions and Internal), PEP List and List of Suspicious Indicators are maintained by the Bank for the purpose of screening customers. In addition, for foreign clients, internet search is required to determine the PEP status or relationship with a PEP.

Category	Description	Disposition

Suspicious Indicator (which includes Internal Watchlists)	Includes client who is a positive match with the Internal Watchlist, and other suspicious indicators (per ECRAF policy)	If POSITIVE match with the Internal Watchlist or with presence of other suspicious indicators, conduct enhanced due diligence Seek Senior Management Approval
PEP List	Database of names of Philippine Primary Politically Exposed Persons (for domestic clients) Internet search relating to the PEP status or relationship with a PEP (for foreign clients)	If POSITIVE match, tag as PEP in the source system Seek Senior Management Approval
Sanctions List (OFAC, EU, HMT)	Database of names of personalities who are subject to different sanctions by a country or group of countries due to involvement on sanctioned activities (i.e. terrorism, drug trafficking) – OFAC, UN, EU, HMT	If POSITIVE match, DENY business relationship Report to Compliance Division for filing of Suspicious Transaction Report (STR)
Sanctions List (UNSC and ATC)	Database of names of personalities who are subject to different sanctions by a country or group of countries due to involvement on sanctioned activities (i.e. terrorism, drug trafficking) – UN	If POSITIVE match, FREEZE any funds/properties/account. Report to Legal Division and Compliance Office for filing of FO Return and Suspicious Transaction Report (STR), respectively

Note: There is POSITIVE match when there is either a name match, potential target match, or target match.

Results of the screening process shall be recorded in the Bank's Enhanced Customer Risk Assessment Form (ECRAF).

The result of the screening shall be treated as the Bank's property and shall not be disclosed to the client.

6.3.5 Customer Risk Profiling

As required by BSP Circular 706, as amended by BSP Circulars 950 and 1022, the Bank shall conduct risk profiling of all customers. Risk profiling shall consider the following customer information:

a. PEP Classification
b. Residency and Citizenship
c. Geographical Location
d. Occupation/ Nature of Work
e. Source of Funds
f. Type of Ownership
g. Amount of Initial Deposit and/or Estimated Monthly Transactions
h. Length of Relationship with the Bank
i. Products/Services Availed or to be Availed

The assessment of each customer's information above shall be documented in the Enhanced Customer Risk Assessment Form (ECRAF) – see **Annex H & I** for the ECRAF Form. For complete ECRAF Implementing Guidelines, please see **Annex J**.

At the end of the assessment, customers will be classified into LOW, NORMAL, or HIGH risk. Such classification will determine the appropriate due diligence and frequency of updating of customer records.

6.3.6 Required Due Diligence

The Bank uses three types of due diligence namely: a) Reduced Due Diligence (RDD); b) Average Due Diligence (ADD); and Enhanced Due Diligence (EDD).

The following guidelines shall be used in determining the required due diligence to be applied to a particular customer:

Customer Risk Classification	Required Due Diligence
LOW RISK	Average Due Diligence (ADD)
NORMAL RISK	Average Due Diligence (ADD)
HIGH RISK	Enhanced Due Diligence (EDD)

a. Reduced Due Diligence (RDD) – Under no circumstances shall reduced due diligence will be applied, except for those instances expressly approved by the Board of Directors *(e.g. publicly listed domestic banks)*.

b. Average Due Diligence (ADD) – includes the following:

Requirements for ADD	Individual	Entity
1. Obtain all minimum information	YES	YES
2. Confirm date of birth/registration from a duly authenticated official document	YES	YES

Requirements for ADD	Individual	Entity
3. Verify the address through recent utility bills, bank or credit card statement, authenticated official document, by sending "thank you" letters, or through on-site visitation	YES	YES
4. Contacting the customer by phone or email	YES	YES
5. Verification of Identification Documents (a. Basic Information Review; b. Feature Inspection)	YES	YES
6. Determination of Ultimate Beneficial Owners (UBO)	YES	YES

c. Enhanced Due Diligence (EDD) – on top of the requirements of average due diligence, the following additional procedures and documentation are required for all High Risk customers:

Requirements for EDD	Individual	Entity
1. Supporting documents for the nature of the intended business relationship with the Bank, intended or performed transactions	YES	YES
2. Obtain a list of entities where the client is an officer, director or stockholder	YES	NO
3. Obtain a list of banks where the client has previous or existing business relationship	YES	YES
4. Volume of assets (e.g. thru Audited FS, ITR)	YES	YES
5. 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)	NO	YES
6. Validating the source of income or wealth thru official documents (e.g. ITR, Audited FS, Deed of Sales, Deed of Donation)	YES	YES
7. Authentication of identification documents by requesting a certification from the issuing authority or by any other effective and reliable means (e.g. validation through the database of the issuing authority)	NO	YES
8. Obtain other information available through public databases or internet	YES	YES
9. Senior Management Approval	YES	YES

The result of the Enhanced Due Diligence shall be recorded in the Enhanced Due Diligence (EDD) Form (see **Annex K** for the EDD Form). Additional documents required in the enhanced due diligence above shall be attached to the EDD Form.

For new High Risk clients, require the initial deposit/payment to be in the form of check or MC or domestic inward remittance from another domestic bank (*except rural/cooperative bank per Circular 950*). In lieu of this requirement, bank statement/ statement of account/ proof of deposit/investment from another domestic bank where the high risk client has existing business relationship will suffice. Non-compliance with this requirement alone will not warrant denial of business relationship, however, the reason for non-compliance shall be documented in the EDD Form.

6.4 DENIAL OF BUSINESS RELATIONSHIP

Where the Bank is unable to comply with the relevant customer due diligence (CDD) measures, it shall:

a. Refuse to open an account or commence business relationship, or terminate business relationship, or refuse to perform the transaction; and

b. Assess the appropriateness of filing a suspicious transactions reports (STR) in relation to the customer.

6.5 ULTIMATE BENEFICIAL OWNER (UBO)

Beneficial Owner refers to any natural person(s) who ultimately owns or controls a customer and/or on whose behalf a transaction is being conducted; or those who have ultimate effective control over the juridical person or legal arrangement. (*BSP Cir. 1022*)
Ultimate Effective Control refers to the situation in which ownership/control is exercised through actual or a chain of ownership or by means other than direct control. (*BSP Circ. 1022*).

For corporation, the Beneficial Owner shall be determined using the following:

a. Natural person who ultimately have direct or indirect controlling ownership interest in a juridical person (*Ownership Prong*). Direct ownership is manifested when a natural person directly owns a shareholding ownership interest of at least 20% of the juridical entity client. Indirect ownership is manifested when at least 20% of the shareholding or ownership interest of a corporate client is held by another corporate entity which is under the control of a natural person(s), or by multiple corporate entities, which are under the control of the same natural person(s). Please see illustrations in **Annex M** for direct and indirect ownership.

b. Natural person who has control through other means (*Effective Control Prong*). This will apply in case no beneficial owner was identified or there is doubt on the beneficial owner(s) identified under item "a" above. Control through other means (CTOM) includes control exerted by means of trusts, agreements, arrangements, understandings, or practices, or when an individual can exercise control through making decisions about financial and operating policies. Control also includes (i) power to govern the financial and operating policies of the enterprise under statute or an agreement; (ii) power to appoint or remove majority of the members of the board of directors or equivalent governing body; (iii) power to cast the majority votes at a meeting of the board of directors or equivalent governing body; (iv) any other arrangement similar to any of the above.

c. Natural person(s) who hold the position of senior managing official(s) or equivalent ranks (*Effective Control Prong*), where no natural person under items "a" and "b" above is identified, or if there is any doubt that the person(s) identified are the beneficial owners. This shall include the following:

   - Chief Executive Officer (CEO) or equivalent position (i.e. President)
   - Chief Finance Officer (CFO)or equivalent position or Treasurer
   - Chief Operating Officer or equivalent position
   - Managing Member
   - General Partnership (for partnership)

- Any corporate officer who is solely designated as signatory to manage the affairs of the corporation or its business relationship with the Bank.

To reinforce the BO identification process, the Bank should take a multi-pronged approach in obtaining BO information and implement risk-based verification process from other independent, reliable sources, apart from client representation, such as annual report, third-party tools, and publicly available information using open source/internet searches. Additional validation procedures for identified high-risk customers and/or BOs may include conducting onsite visits, and interviews with competent company officers or personnel.

Due Diligence Required:

Gathering of minimum mandatory information. Minimum mandatory information for beneficial owners will be obtained prior to account opening. For beneficial owner or beneficiary of an individual account, see discussion of *Minimum mandatory Information* for Individuals above. For juridical persons (e.g. corporate clients), the Authorized Personnel responsible for the conduct of due diligence shall gather the minimum information of the identified UBO:

a. Name
b. Address
c. Citizenship or Nationality

For High Risk clients, any two (2) of the additional information on the UBO shall be required:

a. volume of assets
b. occupation/business
c. nature of the business relationship
d. source of funds or wealth

In addition to the individual information of the UBOs, the corporate information of the parent entities owned by the UBOs shall be gathered. For the list of documents to be presented, see discussion of *Official Identification Documents*.

Verification of Information and Screening. The identity of the UBOs shall be verified against any of the following sources:

a. Government-issued identification documents
b. Official documents issued by the government
c. Official documents submitted to and officially received by the government
d. Other covered persons, including designated non-financial businesses and professions (DNFBP)
e. Credit Bureaus
f. Company Registers (e.g. Securities & Exchange Commission – SEC, Cooperative Development Authority – CDA)

g. Competent Authorities, where disclosure requirements ensure adequate transparency of beneficial ownership
h. Other verification sources using the internet such as, but not limited to, website of the corporate client or other organization where the UBO is connected.

The identified UBO, including the entity where he/she directly holds interest, shall be subject to screening against the Bank's PEP list and watchlists. In addition, a negative news search of the UBO and the entity will be conducted via internet in any of the following instances:

a. When the customer, where the UBO is related, is classified as High Risk
b. When the customer, where the UBO is related, is a PEP (*per PEP policy*)
c. When the UBO or the entity where he/she holds interest or exercise effective control, is a positive match in the Internal Watchlist.

Any negative news pertaining to the UBO or to the entity where he/she has direct interest shall be assessed by the authorized officer approving the account opening. The likelihood of impact on the future/existing business relationship and possible effect to the Bank's reputation shall be considered.

Be it noted that if any UBO or entity related to the UBO is a positive match with any of the Sanctions List (*i.e. OFAC, UN, EU, HMT*), the business relationship with the customer where such UBO is related shall be denied or shall be immediately terminated (*if already existing*), and a suspicious transaction report (STR) will be filed as appropriate.

Verification and Screening. Without prejudice to the requirements on customer on-boarding pertaining to the Bank Customer and the authorized representatives, the verification of UBOs identified shall be conducted upon customer onboarding. For existing customers, verification shall be done upon the client's updating of customer records.

When to Conduct Verification and Screening. Without prejudice to the requirements on customer on-boarding pertaining to the Bank Customer and the authorized representatives, the verification of other UBOs identified (if any) shall be conducted within thirty (30) days from the date of account opening/business relationship, so as not to interrupt with the normal conduct of business of the branch/business unit.

Screening of the UBO and the entity, where he/she holds direct interest, against watchlist and PEP list shall be conducted prior to opening of account/business relationship.

Documentation, Record-keeping and Updating. The UBO information including the result of the screening and verification shall be recorded in the UBO Determination Form as prescribed by Compliance Division (– see **Annex N** for the UBO Determination Form and **Annex O** for the UBO Determination Form Implementing Guidelines). The use of the UBO Determination Form does not apply to individuals and sole proprietorships.

The UBO Determination Form shall form part of the customer's (partnership/corporation/cooperative/etc.) KYC documents, to be attached to the ECRAF, and shall be retained co-terminus to the basic KYC documents of the customer.

Scrubbing of UBOs. For existing customers, Base60 AML System can do automated scrubbing,

through KYC alert. Since the UBOs have their own information in the core banking system, they shall be included in the automated scrubbing of customer's database versus the names in the bank's watchlist. KYC Screening alerts are then generated and reviewed for any name match.

AML Compliance Officer

1. Receive from the assigned officer the consolidated list of names gathered from Negative News Reporting (NNR) on a daily basis;

2. The consolidated names from the NNR will then be uploaded in the Internal Watchlist on the same day;

3. On the next day, the assigned AML officer checks the KYC alert in the Base60. If there is a generated alert, the review and investigation of the alert must be prioritized to determine if our customer is the same as against the name in the watchlist. If the name is the same in the internal watchlist, file STR.

4. On the other hand, in identifying potential or target matches for TFS-related name match, consider the following information provided for designated persons:

    - First and Last Name
    - Aliases
    - Date of Birth
    - Passport Details
    - Nationality
    - Last Known Address
    - Employment and Government Role
    - Other Information Provided

5. If potential target match or a target match is identified, the account must be frozen immediately, file STR and inform the Legal Services Division to file a detailed return to the AMLC within 24 hours upon determination or confirmation that they are one and the same person.

6. Branches ad business units shall ensure that all required information in the UBO Determination Form and in the UBO information in FCBS are complete so that UBOs are included in the screening and scrubbing process in the bank's AML system.

BSP Memo No. M-2024-021, Guidance Paper on Beneficial Ownership Due Diligence provides the elements of beneficial ownership due diligence and some of the good practices already applied by BSFIs.

Board of Directors (BOD) and Senior Management (SM) Oversight. The BOD has the ultimate responsibility to comply with the AML/CTPF laws, rules and regulations, including the requirements on beneficial ownership due diligence. It shall ensure that ML/TF/PF risks are effectively managed, and the identified risks are appropriately mitigated by the bank's enterprise risk management system. The bank's institutional risk assessment (IRA) should encompass ML/TF/PF risks arising from the respective operations, including the use of ambiguous ownership and

corporate structure, as relevant. Anchored on the results of the IRA, the bank should take appropriate measures to manage and mitigate ML/TF/PF risks and take enhanced measures on identified high risks areas or customers, which should be articulated in the MTPP. Below are some noted good practices by the BSP:

- The BOD and SM have regular discussions, covering risk management policies and practices on UBO, including:
    1) Due diligence requirements;
    2) Instances of non-identification and non-verification of UBOs;
    3) Results of compliance testing and internal audits;
    4) Suspicious transaction reports (STR) involving UBOs;
    5) Compliance with freeze order/asset preservation order and bank inquiry order (FO/APO/BI); and
    6) Record keeping.
- The IRA covers key areas, such as
    1) Identification of threats associated with legal persons and legal arrangements, generally under the customer profile and geographic location; and
    2) Assessment of UBO-related internal controls in mitigating ML/TF/PF risks.
- Other noteworthy actions to improve BOD and SM oversight include:
    1) Enhancing of reporting package to the BOD and SM to include, as applicable, root causes of non-identification and non-validation of UBOs, remediation strategies, as well as relationship management policies and procedures.
    2) Expanding the IRA to cover identification of the ML/TF/PF risks exposure and typologies associated with UBOs, jurisdiction of incorporation, types of products and services availed, volume and value of customer transactions, and nature of abuse, as applicable.

Beneficial Ownership Identification and Verification. The bank is expected to identify the UBO and take reasonable measures to verify his/her identity based on official documents or other relevant, reliable source of information or data. The bank should have a system to understand the nature of the customer's business, including its ownership and control structure, particularly that of juridical persons or legal arrangements. Further, the bank is required to conduct sanctions screening procedures for customers and their transactions, including UBOs or any persons purporting to act on behalf of the customer, and their authorized signatories. Below are some noted good practices by the BSP:

- Implementing a framework to identify the UBO of legal persons and business entities, which includes obtaining the required information and documents of BOs, and actions to be taken (e.g., denial of business relationship) if the BO was not properly identified or yields possible match during sanctions/targeted financial sanctions (TFS) screening.
- Utilizing a UBO form, either embedded in the account opening form or as a separate document, during onboarding, and requires submission of the GIS to validate the UBO information.
- Performing negative and watchlist screening on UBOs and considers the beneficial ownership information in assessing the overall ML risk profile of the corporate customer.
- Requiring corporate customer to inform the bank of any changes in ownership or control structure throughout the life of the relationship.
- Assigning designated unit or point person responsible for ensuring that beneficial ownership information and documentation are adequate, complete and updated on a regular basis.
- Other noteworthy actions to improve beneficial ownership identification and verification include:
    - On a risk-based approach, adopt a multi-pronged approach in collecting and verifying UBO information from other independent, reliable sources, apart from client representation, such as

annual report, third-party tools, and publicly available information using open source/internet searches. Additional validation procedures for identified high-risk customers and/or UBOs may include conducting onsite visits, and interviews with competent company officers or personnel.
- Obtain and verify the means and mechanisms through which the natural person(s) exercises control17 as UBO, as applicable.
- Identify juridical entities with common UBOs, for better understanding of the profile and transactions of the customers.
- Highlight policies and procedures in identifying and verifying UBOs in the AML/CTPF training, including sample cases/schemes on use of dummy/front/shell companies and customers with complex or ambiguous corporate structure.

Ongoing Monitoring of Customers, Accounts and Transactions. The bank shall, based on materiality and risk, ensure that pertinent identification information and documents collected during the CDD process, including beneficial ownership information, are kept up-to-date and relevant. This ensures that the customer's risk profile is updated and the bank's understanding of its customers are current. This informs the establishment and/or maintenance of a system that will enable the bank to understand the normal and reasonable account or business activities (e.g.,
commercial activities, risk profile, source of funds, expected transactions) of customers, and detect unusual or suspicious patterns of account activity. The bank is encouraged to disclose beneficial ownership information in filing suspicious transactions involving its corporate customers. Below are some noted good practices by the BSP:

- Updating UBO information based on existing company policy.
- Conducting periodic scrubbing of UBOs, whether customer or non-customer, against sanctions and watchlist databases, and for this purpose, assigns a unique identification number to UBOs or maintains a separate UBO database.
- Investigating and reporting, as appropriate, suspicious accounts and/or transactions of juridical customers whose UBOs were subject of adverse/negative news, STRs, and FO/APO, and vice versa.
- In the presence of suspicious indicators on UBOs, conducting EDD procedures on the UBOs, files STR, and closely monitors their transactions.

Targeted Financial Sanctions

- Adopting policies and procedures to freeze the UBO account and/or report STR when a match is found.
- Maintaining UBO database, either through assigning a separate customer information file (CIF) or manual build-up, and scrubbing UBOs of corporate customers, as part of the process to implement TFS requirements.

Bank Inquiry / Freeze Order Handling

- Conducts EDD, considers ST reporting, and includes UBOs of corporate customers in the watchlist/blacklist database based on defined trigger events, such as being subject of bank inquiry or FO, negative news or previous STR; Performs similar procedures for corporate customers when their BOs are the subject of certain suspicious triggers.
- Reporting the UBOs of juridical customer subject of FO/APO or corporations whose BOs are the subjects of FO/APO, as materially-linked accounts.
- Scrubs the UBO names included in the bank inquiry / FO against the customer database, including those not identified as accountholder of the bank.
- Discloses BO information, e.g., business, address, citizenship, in the STR narratives.
- Other noteworthy actions to improve ongoing monitoring of customers, accounts and transactions:

- Use a trigger-based approach to update beneficial ownership information, e.g., discovery of suspicious indicators and other risk factors on customers or their UBO. Triggers for review may also include open-source investigative media reports (e.g., Panama and Pandora papers).
- Update the UBO's current status in terms of ownership, control or company position periodically.
- Adopt written policies, including red flag indicators on UBOs for consistent implementation and proper guidance.
- Review the accounts of corporate customer subject of previous STRs to check UBO information and file STR on the UBO, as warranted.
- Adopt proportionate policies and procedures to ensure that
- UBOs of corporate customer subject of STRs are included in the watchlist database; and
- UBO information is indicated in the STR narrative.

Record-keeping and Information Sharing. The bank is expected to adopt policies and procedures for the proper safekeeping of beneficial ownership information of customers and allow competent authorities to have access thereto as permitted by relevant laws and regulations. In general, the bank has existing record-keeping policies and practices, covering documentation of beneficial ownership information, as well as sharing to supervising authorities, the AMLC and law enforcement authorities (LEAs), to the extent allowed by existing relevant laws and regulations. In addition, the SEC and the AMLC promoted partnerships and implemented procedures for sharing beneficial ownership information with domestic and foreign competent authorities to strengthen the LEAs' access to accurate and up-to-date UBO information. The bank is encouraged to subscribe to the AMLC's PPPP for ease of information exchange.

Role of Self-assessment. The Compliance Office (CO) promotes the adoption and implementation of bespoke policies on beneficial ownership due diligence through the conduct compliance testing. The Internal Audit (IA), on the other hand, performs periodic and independent evaluation of the risk management system, degree of adherence to internal control mechanisms and adequacy and effectiveness of existing internal controls on beneficial ownership due diligence. Below are some noted good practices by the BSP:

- Covers UBO identification and verification procedures in the risk-based compliance testing and internal audit, encompassing the following, among others:
  - Controls for gathering required information and documents to identify UBO and documenting ownership structure;
  - Process for watchlist screening and periodic scrubbing of UBOs and implementing prescribed actions in case of matches; and
  - Assessing the risk profile of juridical entities, taking into account the BO information and profile.
- Other noteworthy actions to improve beneficial ownership identification and verification include:
  - Consider the following in developing risk-based audit and compliance testing for
  - beneficial ownership due diligence:
    1) Risk-based verification procedures on UBOs;
    2) Compliance with FO/APO on corporate customers and their BOs; and
    3) Transaction monitoring and ST reporting of corporate customers and UBOs.
  - Improve root cause analysis of nonidentification and non-validation of BOs during onboarding and updating, for better remediation process.

Non-compliance with Beneficial Ownership Due Diligence. The bank shall deny the onboarding of client should they be non-compliant with this policy. Existing clients not compliant with this policy shall likewise be subjected to the bank's *Deposit Account/ Client Account AML Exit Policy*.

6.6 RESTRICTED ACCOUNT

In line with the BSP's advocacy to promote financial inclusion and to ensure that micro-business owners and low-income households are able to manage their finances through the financial system, customers who may not be able to provide all the required mandatory information or any valid identification document, as provided herein, may be allowed to open a Restricted Account. However, the Bank shall not venture in to this type of product until the following pre-requisites are met:

a. This will be treated as a separate product
b. The system is capable of monitoring the credits to the account and prevent subsequent credits whenever the total credits in one (1) year amounts or will amount to Php100,000
c. Preventive controls are in place to ensure that the account will not be used to send out or receive foreign remittance
d. Whenever the client wishes to remove the above restrictions to the account, controls will be implemented to ensure that the applicable full customer due diligence required are implemented before the account is converted to a regular deposit account.

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 Bank a proof of application for a valid ID.

6.7 POLITICALLY EXPOSED PERSON (PEP)

6.7.1 Politically Exposed Person (PEP) is the collective term that may refer to any or all of the following:

a. Principal PEP – shall refer to a person who is or has been entrusted with prominent public position: (1) in the Philippines with substantial authority over policy, operations or the use or allocation of government-owned resources; (2) a foreign State; or (3) an international organization.

i. For the Philippines, the following shall be included as Principal PEPs:

Executive	Judiciary	Legislative	Military/Law Enforcement	Office of the Ombudsman
President	Justices of Supreme Court	Senators	Heads and Generals of	Ombudsman

<table>
<tr><th>Executive</th><th>Judiciary</th><th>Legislative</th><th>Military/Law Enforcement</th><th>Office of the Ombudsman</th></tr>
<tr><td>Vice President</td><td>Justices of Court of Appeals</td><td>Congressmen</td><td rowspan="4">Armed Forces of the Philippines, PNP and other Law Enforcement Agencies[2]</td><td rowspan="4"></td></tr>
<tr><td>Cabinet Members[1]</td><td rowspan="2">Justices of Court of Tax Appeals</td><td rowspan="3">Heads of Political Party List</td></tr>
<tr><td>Governor</td></tr>
<tr><td>Mayor</td><td>Justices of Sandiganbayan</td></tr>
</table>

[1]Cabinet Members include the following:

- Cabinet Secretary
- Executive Secretary
- Presidential Communications Operations Office Secretary
- Presidential Spokesperson
- National Security Adviser
- Secretary of Agrarian Reform
- Secretary of Agriculture
- Secretary of Budget and Management
- Secretary of Education
- Secretary of Energy
- Secretary of Environment and Natural Resources
- Secretary of Finance
- Secretary of Foreign Affairs
- Secretary of Health
- Secretary of Information and Communications Technology
- Secretary of Interior and Local Government
- Secretary of Justice, including the Solicitor General
- Secretary of Labor and Employment
- Secretary of National Defense
- Secretary of Public Works and Highways
- Secretary of Science and Technology
- Secretary of Social Welfare and Development
- Secretary of Tourism
- Secretary of Trade and Industry
- Secretary of Transportation and Communication
- Presidential Assistant
- Special Assistant to the President

- Presidential Management Staff Chief

[2]Heads and Generals of Armed Forces of the Philippines, PNP and other Law Enforcement Agencies shall include the following:

- General - Philippine Air Force
- General – Philippine Army
- Admiral – Philippine Navy
- General – Philippine Marines
- Director General – Philippine National Police (PNP Chief)
- Executive Director – Philippine Drug Enforcement Agency (PDEA Chief)
- Director – National Bureau of Investigation (NBI Director)

ii. For Foreign State, the following shall be considered as Principal PEPs:

- President or Head of State/Government
- Senior Politicians
- Justices of High Courts
- Military or Police Officials with at least a rank of General or its equivalent

iii. For International Organization, the following shall be considered as Principal PEPs:

- Senior Officials of International Organizations (e.g. WHO, UN, EU, FATF, NATO)

b. Relatives of Principal PEPs – shall include those relatives within the 2nd degree of consanguinity or affinity:

- Husband/Wife or Partner (1st)
- Father or Mother (1st)
- Father-in-Law or Mother-in-Law (1st)
- Son or Daughter (1st)
- Son-in-Law or Daughter-in-Law (1st)
- Brother or Sister (2nd)
- Brother-in-Law or Sister-in-Law (2nd)
- Grandparents (2nd)
- Grandchild (2nd)

c. Close Associates – close association may be demonstrated via business/professional or personal relationship between a Principal PEP and another person that is known to the public or the Bank, including but are not limited to the following:

- Natural person having a business/professional or close personal relationship with the principal PEP that is publicly known.

- Natural person, regardless of relationship with the principal PEP, with substantial transaction with a principal PEP (or relative as defined above) within the Bank
- Natural person, regardless of relationship with the principal PEP, who is a co-owner of an account maintained within the Bank
- Business, solely or co-owned by a principal PEP. Including business partners in a partnership type of business.
- Corporation, where the principal PEP owns at least 20% of the voting stock or is identified as a beneficial owner, per existing policy.

Domestic/Local PEPs are not automatically high risk and shall be risk-classified accordingly following the policies and procedures of the Bank's Enhanced Customer Risk Assessment Form (ECRAF).

Foreign PEPs such as foreign government and international organization officials shall automatically be classified as High Risk customers. Thus, subjected to enhanced due diligence.

Compliance Division shall maintain a database of local/domestic principal PEP derived from official government and other reliable databases. This database shall be made available to the branches/units for on-boarding and subsequent screening of a customer.

Prior to the on-boarding of the customer, PEP determination shall be performed that includes: (i) Watchlist/PEP List screening (*for Filipino customers*); (ii) Internet search (*for non-Filipino customers*).

All customers qualifying as PEP shall be tagged in the bank's system (*e.g. FCBS*) as PEP and shall be regularly monitored by the branch or unit where the PEP is maintaining an account.

ALL PEPs, regardless of risk classification, shall require Senior Management approval.

6.7.2 Time Limits of PEP Status

The Financial Action Task Force (FATF) Recommendation 12 also defines a PEP as someone who has been (but may no longer be) entrusted with a prominent public function. The language of Recommendation 12 is consistent with a possible open ended approach (i.e. "once a PEP – could always remain a PEP"). The handling of a client who is no longer entrusted with a prominent public function should be based on an assessment of risk and not on prescribed time limits.

Applying the risk based approach, the Bank shall assess the ML/TF risk of a PEP who is no longer entrusted with a prominent public function, and take effective action to mitigate the risk. Possible risk factors are:

- The level of (informal) influence that the individual could still exercise; the seniority of the position that the individual held as a PEP; or

- Whether the individual's previous and current function are linked in any way (e.g. formally by appointment of the PEPs successor, or informally by the fact that the PEP continues to deal with the same substantive matters).

6.7.3 PEP Declassification

PEP declassification is based on the understanding that the money laundering risk that PEPs present will reduce progressively from the point at which they leave office. Although some high risk PEPs should retain their "once a PEP, always a PEP) status on a permanent (or at least indefinite) basis after they leave office, others may be declassified by considering the following factors:

- The level of corruption inherent in the government office which the customer is politically exposed;
- The customer's links to industries at a high risk of money laundering;
- The specific risk associated with the customer's previous political position, i.e., its susceptibility to corruption;
- How long the customer held their political position and the likelihood that they will hold office again in the future;
- The source of the customer's wealth and the source of wealth acquired while they held their political position;
- The plausibility of the customer's risk profile and net worth;
- The transparency of transactions associated with the customer's account;
- Adverse media stories involving the customer;
- The customer's ongoing connections to the political establishment.

In addition to the considerations above, PEP declassification should also require a Senior Officer review and approval and must be documented internally.

6.8 DEFAULT HIGH RISK CUSTOMERS

Regardless of risk assessment scores in ECRAF, the following customer types will be considered as High Risk by default:

a. Customers who are citizens or residents of a High Risk Country (*see **Annex P** – List of High Risk Countries/ Jurisdictions*)

b. Charitable Institutions or Foundations or similar Non-Governmental Organizations

c. Money Service Business (MSBs), to include Remittance Corporation/Agent/Sub-agent, Remittance Plat-form Provider, E-Money Issuer, Foreign Exchange Dealer/Money Changer

d. Private or Government owned/instituted Gaming Entities, including junket operators

e. Service Providers to Gaming Operations such as Gaming Software/Platform Provider, Business Process Outsourcing Provider, Data/Content Streaming Provider, Gaming Support Provider, Other Providers such as Online Payment Providers that specifically service gaming institutions.

f. Custom Brokerage (entity or sole practitioner)

g. Sole practitioner lawyer or accountant (*including sole proprietorship engaged in the practice of law or accounting*)

h. Foreign Politically Exposed Person

i. Dealers of Precious Stones or Metals or High Value Artworks, Collector's Pieces and Antiques

j. Dealer or Manufacturers of Guns or Ammunition or Military Equipment or Major Parts Thereof

k. Owner or owners (in case of family-owned or partnership) of a High Risk Business

l. Stockholder owning at least 20% of the voting stock of a High Risk Corporation

m. Numbered Non-Checking Accounts

n. Customers with any of the "Suspicious Indicator" (*as described in **Part G** of the ECRAF Implementing Guidelines V2.3 as attached in **Annex J***)

The above customer types will be automatically subject to the minimum EDD requirements as discussed in the preceding sections of this Manual.

When dealing with high risk customers, the Authorized Personnel should take extreme caution and vigilance. In no case shall reduce diligence be applied to high risk customers. On the other hand, in case the Authorized Personnel determines, based on its standards, that dealing with the high risk customer calls for, or these rules require, the application of enhanced due diligence, it shall apply the minimum requirements for enhanced due diligence in accordance with section 6.3.5(c) of this part of the MTPP.

Senior Management approval is required for all High Risk customers.

6.9 SENIOR MANAGEMENT APPROVAL (SMA)

Unless the business relationship requires higher approval than what is required in this MTPP, Senior Management Approval (SMA) shall mean approval by Senior Officers up to the District/Region/Division Heads and/or Group Heads (for Branches) and up to the Group Heads (for other Business and Head Office Units).

For the purposes of this policy, approval via official Lotus Notes email of the senior officer shall be allowed. Documents providing record of senior management approval shall be in printed form and shall be attached to the ECRAF (or EDD Form if High Risk), and shall form part of the initial KYC of the applicable customer.

6.10 ACCOUNT OPENED THROUGH A TRUSTEE, AGENT, NOMINEE OR INTERMEDIARY

Where the account is opened by, relationship established through, or any transaction is conducted by a trustee, agent, nominee or intermediary, either as an individual or through fiduciary relationship or similar arrangements, the Authorized Personnel shall establish and record the true and full identity and existence of both the (a) trustee, nominee, agent or intermediary and (b) trustor, principal, beneficial owner, or person on whose behalf the account/relationship/transaction is being opened/established/conducted. The Authorized Personnel 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, beneficial owner, or person on whose behalf the account is being opened, the Authorized Personnel 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.

In case the Authorized Personnel entertains doubts that the trustee, nominee, agent or intermediary is being used as a dummy in circumvention of existing laws, it shall apply enhanced due diligence and file a Report on Incident of Suspicious Activity (RISA – see **Annex S** & **Annex T** for the RISA Form), if warranted.

6.11 THIRD PARTY RELIANCE

The Bank may rely on the identification process or gathering of minimum information and face-to-face contact undertaken by a third party subject to the following rules:

1. Where the third party is a covered person specifically defined generally defined by AMLA, as amended, and its RIRR, the Bank 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 MTPP, 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 Bank 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 a covered persons but conducts business operations and activities similar to them - All the contents required in the sworn certification mentioned in item no. 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. 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 money laundering or terrorism investigation or regulatory action;

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.

Notwithstanding the foregoing, the ultimate responsibility for identifying the customer still lies with the Bank relying on the third party. In cases where the customer is assessed as high risk by the third party, the Bank shall conduct its separate enhanced due diligence procedure.

6.12 OUTSOURCING OF THE GATHERING OF MINIMUM INFORMATION AND/OR DOCUMENTS AND FACE-TO-FACE-CONTACT

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 gathering of the minimum information and/or documents and face-to-face contact as required under this MTPP provided, that the ultimate responsibility for knowing the customer and for keeping the identification documents shall lie with the Bank's Authorized Personnel and the following conditions are complied with:

For covered person counterparty:

a. There is a written service level agreement approved by the board of directors of both the Bank and the covered person counter-party;
b. The counter-party has a reliable and acceptable customer identification system and training program in place

For non-covered person counterparty:

a. There is a written service level agreement approved by the board of directors of both the Bank and the covered person counter-party;
b. The counter-party has a reliable and acceptable customer identification system and training program in place;
c. The Bank outsourcing the activity shall ensure that the employees/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 a covered person's (e.g. Banks) own employees undertaking similar activity; and

d. The Authorized Personnel of the Bank 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 Bank, which shall carefully review the documents or information and conduct the necessary risk assessment of the customer. The Bank 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.

6.13 ELECTRONIC KNOW YOUR CUSTOMER (E-KYC)

E-KYC refers to the process of electronically verifying the credentials of a customer. The bank 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 Bank 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, the Bank 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 Bank 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.

    - ***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.
    - ***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

- ***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.

The Bank 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 party 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 Bank 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, the Bank, as relying party, 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. Moreover, the Bank shall ensure compliance with the applicable guidelines and full implementation of the authentication procedures/methods and other related systems under the PhilSys.

In implementing e-KYC, the Bank 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.

6.14 DESIGNATED NON-FINANCIAL BUSINESS AND PROFESSIONS (DNFBPs)

DNFBPs, as covered persons, are to be regulated for anti-money laundering (AML) and countering the financing of terrorism (CFT) proportionate to the nature, scale and complexity of the DNFBPs operations in order to prevent criminals from exploiting them.
Under the AMLA, as amended, the following DNFBPs are considered covered persons

A. Jewelry dealers in precious metals, who, as a business, trade in precious metals;

B. Jewelry dealers in precious stones, who, as a business, trade in precious stones;

C. Company service providers which, as a business, provide any of the following services to third parties:

   I. Acting as a formation agent of juridical persons;
   II. Acting as (or arranging for another person to act as) a director or corporate secretary of a company, partner of a partnership, or a similar position in relation to other juridical persons;
   III. Providing a registered office, business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement; and
   IV. Acting as (or arranging for another person to act as) a nominee shareholder for another person

   For this purpose, “business” means engaging in or offering the foregoing services, whether to the public or select customers, on regular or continuing basis, whether for a fee or for free, or as means of livelihood.

D. Persons, who provide any of the following services:

   1. Managing of client money, securities or other assets;
   2. Management of bank, savings, securities or accounts;
   3. Organization of contributions for the creation, operation, or management of companies; and
   4. Creation, operation, or management of juridical persons or arrangements, and buying and selling business entities

E. Casinos, including internet and ship-based casinos, with respect to their casino cash transactions related to their gaming operations;

F. Offshore Gaming Operators, as well as their service providers, supervised, accredited or regulated by the Philippine Amusement and Gaming Corporation (PAGCOR) or any Appropriate Government Agency (AGA); and

G. Real Estate Brokers and Developers.

Juridical persons, including law firms and accounting firms, which perform any of the activities enumerated in item C and D are deemed covered persons under the AMLA.

Prospective clients falling under the list are required to accomplish the Due Diligence Questionnaire (DDQ) to fully understand the nature of the service/s they provide and to clearly determine if such client is indeed DNFBP.

In applying the risk-based approach, DNFBPs in item A, B, E & F are considered as High Risk customers by default. When dealing with high risk customers, the authorized personnel should take extreme caution and vigilance. In no case shall reduce diligence be applied.

For DNFBPs not mentioned in the preceding paragraph as automatic high risk (item C, D & G), conduct of enhanced due diligence measures and/or re-evaluation of the business relationship will only be done after failure, refusal or negligence by DNFBPs to supply the Provisional Certificate of Registration (PCOR) or Certificate of Registration (COR), as well as the other information and documents required under the 2018 IRR of AMLA.

Thus, prior to onboarding, DNFBPs must present Provisional Certificate of Registration (PCOR) and/or Certificate of Registration (COR) with AMLC. This policy shall also apply to existing DNFBPs. Failure, refusal or negligence by aforesaid DNFBPs to supply the PCOR or COR, shall be considered as grounds to conduct enhanced due diligence and/or to re-evaluate on whether to continue or terminate the existing business relationship.

Senior Management approval up to the Group Head is required.

All clients that have been identified as DNFBPs shall be tagged accordingly in the FCBS System. If the client has declared that they are not engaged in any of the abovementioned activities, they shall be required to accomplish the Sworn Statement of Non-Engagement. Thus, they will not be required to submit the COR/PCOR, and will not be tagged as DNFBPs.

Indicators to determine if a customer qualifies as DNFBP:

- Inclusion in the latest list of DNFBP from the AMLC website.
- AMLC Certificate of Registration / Provisional Certificate of Registration (COR/PCOR)
- The customer maintains their own Money Laundering and Terrorism Financing Prevention Program (MLPP/MTPP) for the business.
- Registered/licensed activities mentioned in the SEC Certificate of Registration, Articles of Incorporation, website, PRC license, etc.
- Activities undertaken by the business/professional.

- Products/services provided.
- Industry where the business/professional is employed.
- Declared source of funds.
- Name of the business.
- Analysis of the purpose declared in the Articles of Incorporation

Branches and business units processing the onboarding of customers or updating of information shall ensure that due diligence is conducted and determine whether the customer is a DNFBP or not. The Bank shall only accept DNFBP clients who are registered with the AMLC.

6.15 GUIDELINES ON ACCEPTING CLIENTS ENGAGED IN GAMING OR GAMING-RELATED ACTIVITIES

6.15.1 Risk Appetite

The Bank shall **not accept** new business relationships or accounts of clients engaged in on-line gaming and their service providers. These includes the following:

- Online Gaming Businesses (OGBs) (e.g. POGOs, other forms of internet-based casinos)
- Interactive Gaming Operators, including eSabong and e-bingo
- Service/Support Provider of Online or Interactive Gaming Operators
- Land-based Gaming with Online/Interactive Gaming Operation
- Service/Support Provider of a Land-based Gaming WITH online/interactive gaming operation
- IT Consultants on Gaming Operators and their Service Providers
- Individuals or Entities related to the above businesses

The Bank shall likewise refrain from providing banking services or products to OGB Clients, whether *directly* or *indirectly*. The term *indirect* includes MSB clients whose OGB Clients are using the remittance channels of the Bank. The Bank shall endeavor to restrict this practice.

Any existing client/s who are known to the Branch/Unit to be engaged in any of the above businesses mentioned above shall immediately be reported to the AML Compliance Department of the Compliance Division for appropriate handling. OGB Customers have begun using legitimate companies to facilitate their transactions hence, branches and business units must exercise vigilance in ensuring that banking channels are not used and abused.

However, the Bank allows acceptance of new clients engaged in purely land-based gaming business provided that:

- The client is licensed/authorized by the appropriate government entity;
- The clients undergo enhanced due diligence, including Senior Management Approval until Group Head, as provided in this guidelines; and
- Transactions shall be strictly monitored. Each transaction requires TEDD.

6.15.2 Licensing/Accrediting Authorities

The Authorized Personnel conducting the due diligence of the customer shall familiarize him/herself with the following entities and the type of license/authority/accreditation they issue/grant to gaming entities and providers of gaming-related services:

1. **Philippine Charity Sweepstakes Office (PCSO)** – have contracts with authorized agents (*e.g. for lotto, small-town-lottery*) which embody the terms of operations, among others;

2. **Philippine Amusement and Gaming Corporation (PAGCOR)** – issues license for offshore e-Casino, eSabong, eBingo, offshore gaming operator, offshore operator service provider, other online gaming and sports betting licenses (e.g. POGO), other gaming license and license for gaming service providers. Gaming licenses issued by PAGCOR enables the licensee to operate anywhere in the Philippines;

3. **Cagayan Export Economic Zone (CEZA)** – issues license for offshore e-Casino, other online gaming and sports betting licenses (e.g. POGO) operating within the jurisdiction of CEZA. Authorized licensors under CEZA are the following:

    a. First Cagayan Leisure and Resorts Corporation (FCLRC)
    b. Northern Cagayan Gaming and Amusement Corporation (NCGAC)

    Gaming entities licensed by CEZA licensors can only operate within the jurisdiction of CEZA.

4. **Aurora Pacific Economic Zone and Freeport (APECO)** – issues license for offshore e-Casino, other online gaming and sports betting licenses (e.g. POGO) operating within the jurisdiction of APECO. Master Licensor for APECO is the Pacific Seaboard Leisure and Entertainment Corporation.

    Gaming entities licensed by APECO can only operate within the jurisdiction of APECO.

5. **Authority of the Freeport Area of Bataan (AFAB)** – issues license for offshore e-Casino, other online gaming and sports betting licenses (e.g. POGO) operating within the jurisdiction of AFAB. Master Licensor for AFAB is the Grand Innovasia Concept Corporation. Gaming entities licensed by AFAB can only operate within the jurisdiction of AFAB.

6. **Games and Amusements Board (GAB)** – issues licenses, regulates and supervises professional sports and allied activities including cockfighting.

6.15.3 Licensed/Accredited Entities

Gaming entities or gaming-related entities required to be registered/accredited by PAGCOR or any appropriate licensing/accrediting authority include the following:

7. **Philippine Offshore Gaming Operator (POGO)** – which may be Philippine-based operator or an Offshore-based operator (*which will engage the services of a PAGCOR-accredited Service/Support Providers for its online gaming activity*);

8. **POGO-gaming Agent** – refers to the representative in the Philippines of Offshore-based operator;

9. **Offshore Gaming Operator (OGO)**[1] – refers to an entity engaged in offering online games of chance or sporting events via the internet using a network and software program, by themselves or through local service providers.

10. **Offshore Gaming Operator Service Provider (OGO-SP)**[2] – refers to a duly constituted business corporation which provides components of offshore gaming operations to offshore gaming operators.

11. **Service Provider** – refers to the entity which provides components of offshore online gaming operations, which may further be:

    a. **Gaming Software/Platform Provider** – for gaming systems and games, sports book, pool betting and the like;
    b. **Business Process Outsourcing (BPO) Provider** – for call centers and IT support services, excluding the service of taking actual bets; or
    c. **Data/Content Streaming Provider** – for real time streaming of casino games produced from a live dealer studio set-up, streamed via the internet to the website of the POGO/other gaming entity.

12. **Gaming Support Provider** – refers to a company that produces proprietary products and services that may or may not be found in the gaming system of the POGO/other gaming entity, but is an important part of the online gaming set-up, e.g. payment solutions, player registration, rewards and marketing modules.

13. **Casino** – is a facility which houses and accommodates certain types of gambling activities. Casinos are most commonly built near or combined with hotels, restaurants, retail shopping, cruise ships or other tourist attractions.

14. **Internet-based Casino** – refers to casinos in which persons participate by the use of remote communication facilities such as, but not limited to, internet, telephone, television, radio or any other kind of electronic or other technology for facilitating communication.

15. **Ship-based Casino** – refers to casinos, the operation of which is undertaken on board a vessel, ship, boat or any other water-based craft wholly or partly intended for gambling.

[1] AMLC Regulatory Issuance No. 03, Series of 2021; 2021 AML/CFT Guidelines for DNFBPs
[2] AMLC Regulatory Issuance No. 03, Series of 2021; 2021 AML/CFT Guidelines for DNFBPs

16. **PCSO sweepstakes and lottery games** – includes game of chance such as traditional sweepstakes, scratch and match variety, Small Town Lottery (STL), 6-pick number games (i.e. Lotto 6/42, Mega Lotto 6/45, Super Lotto 6/49, Grand Lotto 6/55 and Ultra Lotto 6/58), 6-digit (6D) and 4-digit (4D) Suertres Lotto and EZ2 Lotto games, and KENO Lotto Express.

17. **Cockfighting** – shall encompass and mean the commonly known game or term "cockfighting derby, pintakasi or tupada", or its equivalent terms in different Philippine localities.

18. **eSabong** - is defined as the online/remote or off-site wagering/betting on live cockfighting matches, events, and/or activities streamed or broadcasted live from cockpit arena/s licensed or authorized by the Local Government Units having jurisdiction thereof.

19. **Games/Sports Sanctioned by the Games and Amusement Board** – a license is also required for those clients engaged in the following activities:

    a. Professional Basketball and Other Professional Sports

        - 3 Point Shootout
        - Chess
        - Cockfighting and Cockfighting International Derby
        - Dance Sport
        - ESports
        - Motocross Racing
        - Professional Basketball
        - Professional Billiard
        - Professional Cycling
        - Professional Darts
        - Professional Football
        - Professional Golf
        - Professional Jetski
        - Professional Table Tennis
        - Professional Tennis
        - Professional Volleyball

    b. Boxing and Other Contact Sports

        - Professional Boxing
        - Professional Mixed Martial Arts
        - Muay Thai
        - Wrestling
        - Kickboxing

    c. Horse Racing Betting

- Horse Racing

20. **OGB clients** – the collective term used by the bank for clients engaged in gaming and gaming-related services/businesses

    For purposes of these guidelines, gaming-related services/activities shall refer to service provider and/or gaming support provider, as defined above.

6.15.4 On-Boarding Documentary Requirements

The following documentary requirements shall apply to business entities engaged in gaming or providers of gaming-related services:

1. SEC Registration for corporation or partnership; DTI registration for sole proprietorship;
2. Articles of Incorporation/Partnership (*for corporation or partnership*);
3. License or Accreditation from the appropriate government agency (*refer to Section C. Licensing/Accrediting Authorities*);
4. AMLC Registration - Provisional Certificate of Registration (PCOR) or Certificate of Registration (COR) (*for POGOs and Casinos, including internet and ship-based casinos, with respect to their casino cash transactions related to their gaming operations* and Offshore Gaming Operators, as well as their service providers, supervised, accredited or regulated by the PAGCOR or any Appropriate Government Agencies (AGA));
5. Latest General Information Sheet (GIS) for corporation or equivalent official document where the owners, directors, and officers are disclosed;
6. Board or Partner's resolution duly certified by the corporate/partners' secretary, or other equivalent document, authorizing the signatory to sign on behalf of the entity;
7. Evidence of source of income/wealth such as Audited Financial Statements (AFS) or Annual Tax Return filed duly stamped by BIR;
8. Business/Company Profile, either provided as integral part of the official annual report, disclosure in the official website, or document signed by the CEO or equivalent position or owner;
9. Listing of banks where the entity has business relationship;
10. Filled-up listing of major counterparties (*e.g. suppliers, service providers, financier, large customer*) – **see Annex V: Counterparty Disclosure Form**;
11. Filled-up **Due Diligence Questionnaire – see Annex W** (*this questionnaire is also mandatory for all sole proprietorship business and those IT/Technology, BPO, Consultancy and technical service entities not related to gaming*);
12. GIS of any corporate stockholder of the client (*regardless of the percentage of holdings*);
13. GIS of a company who holds indirect ownership of the corporate client;
14. Business Permit;
15. Rental/Lease Agreement (*if applicable*);
16. Other official documents supporting the source of funds and purpose of the business relationship or intended use of the account to be opened.

For clients engaged in cockfighting and/or eSabong whichever applicable:

17. SEC Registration for corporation or partnership; DTI registration for sole proprietorship;
18. Articles of Incorporation/Partnership (*for corporation or partnership*);
19. Latest General Information Sheet (GIS) for corporation or equivalent official document where the owners, directors, and officers are disclosed;
20. Board or Partner's resolution duly certified by the corporate/partners' secretary, or other equivalent document, authorizing the signatory to sign on behalf of the entity;
21. City/Municipal License for the operation and maintenance of cockpits
22. Mayor's Permit/Municipal License for the relevant gaming activities from the location of the company office and of the cockpit arenas/venues where the eSabong feeds will be coming from;
23. Detailed location sketch of company office & base of operations;
24. Photocopy of BIR Registration Certificate;
25. eSabong platform documentations, i.e. website and/or desktop or mobile application documents indicating, among others, the main functions, web design and contents, accounting documents and other salient details like compliance with AML/CFT laws.
26. Certification from an independent gaming laboratory certifying that the betting system of the eSabong platform was extensively tested and has been found compliant with the following standards:
    a. All data are captured, accounted and reported by the system;
    b. Game is fair, secure and able to be audited and operated correctly.
27. List of contracted local government unit (LGU)-licensed cockpit arena's;
28. Letter of No Objection (LONO), in any form, interposing no objection to the conduct of sabong operations in said cockpit arenas/venues and the taking and broadcasting of feeds therefrom;
29. Certification from an independent gaming laboratory attesting to Internet Protocol (IP) blocking of all other IP addresses excluding Philippine IP addresses designated by the applicant.
30. Other official documents supporting the source of funds and purpose of the business relationship or intended use of the account to be opened.

In case of a foreign corporation, the official documents equivalent to the above (nos. 1-15) shall be required. In case of a foreign corporation with a branch or office here in the Philippines, the requirements and the due diligence required in the succeeding provisions shall apply to both the foreign parent company and the branch/office here in the Philippines.
For individuals (*proprietor or authorized representatives*), the following information shall be required and recorded in the EDD Form:

1. IDs applicable to individuals;
2. List of Banks where he/she has previous or existing business relationship;
3. List of entities and/or organizations where the client is an officer, stockholder, or director.

Documents required per internal policy of a unit/department not included in the above listing shall not be affected.

6.15.5 Additional On-Boarding Information Requirement

Through interview and initial review of required/submitted/applicable documents, the Authorized Personnel conducting the due diligence shall document the following additional information in the EDD Form or in such other form prescribed by the Compliance Division:

1. **Understanding of the nature and complexity of the business.** This disclosure shall at least include description of the following:

    a. Background and history of the business;
    b. Description of services or goods provided;
    c. Types of clients catered by the business;
    d. Major supplier of goods or services;
    e. Direct competitors;
    f. Ownership structure;
    g. Nature of relationship with the counterparties;
    h. Geographical coverage of business operation;
    i. Other information that supplements the explanation of the nature of the business shall also be gathered if available.

2. **Purpose of the business relationship or account to be opened.** This disclosure shall document all the purpose for which the account/business relationship is intended to be used.

    If the intended use/purpose of the business relationship is for ‘’low-risk” activity such as payroll or application for ordinary loan (except back-to-back), only the standard enhanced due diligence requirement per MTPP will apply. Otherwise, the enhanced due diligence requirement of this guidelines shall be observed. Regardless of purpose, if the source of fund is from gaming and gaming-related business, the customer must be default High Risk.

3. **Average daily credit transactions.** The information may be derived from the financial statements or disclosure of the client. This will include deposits, fund transfer in and inward remittances. This information will be used for transaction monitoring purposes.

4. **Ultimate Beneficial Owner (UBO).** Using the GIS of the client corporation (for direct owners) and other GIS of corporate stockholders/indirect owners, the ultimate beneficial owner shall be established according to AMLC guidelines in determining UBOs. The disclosure shall be made in the **UBO Determination Form (see Annex N)**. If obtaining the GIS of a direct and indirect stockholder from the entity client is not possible, the Authorized Personnel conducting the due diligence shall gather information from other credible sources such as those readily available in the internet (e.g. iSEC View in the SEC website).

5. **Ownership, Operation and Management of Cockpits** – Only Filipino citizens not otherwise inhibited by existing laws shall be allowed to own, manage and operate cockpits.

6. **Establishment of Cockpits** – Only one cockpit shall be allowed in each city or municipality.

7. **eSabong Platform Requirements and Standards**

    a. The eSabong platform shall not accept bets emanating outside the Philippines and shall not be accessible in any way whatsoever outside the Philippines.
    b. The eSabong system or service must comply with the following standards:
        - Player Registration - The eSabong system's player registration must have minimum capabilities and/or functionalities for Know Your Customer (KYC) process;
        - Account Funding and Withdrawal - Shall be done only through AMLC-compliant channels, such as over-the-counter and online banking, eWallet systems, and through other legitimate money transfer services. Only those payment solutions or money transfer services accredited by the Bangko Sentral ng Pilipinas shall be considered legitimate.
        - Membership Verification and Monitoring - The eSabong system shall have the capability to ensure that only the registered player is using his/her account to bet on eSabong.
    c. The eSabong operator shall design and implement a registration process for its agents, coordinators, or promoters to ensure the identity, probity, as well as the responsibility and accountability of the latter.
    d. The eSabong operator shall comply with the AML/CFT Laws, and Rules and Regulations issued and shall be issued by the AMLC, PAGCOR, and other relevant government agencies, including but not limited to, RA 10927, an Act Designating Casinos as Covered Persons under RA 9160, as amended, and its Casino Implementing Rules and Regulations; AML/CFT Guidelines for Casinos; and Customer Due Diligence Guidelines for Land-based Casinos.

Information required per internal policy of a unit/department not included in the above listing shall not be affected.

6.15.6 Due Diligence Requirements Upon On-Boarding

1. **Initial validation of compliance with the license granted.** A gaming entity whose license is granted by CEZA, APECO or AFAB is only allowed to operate within the respective jurisdiction of the economic zone. The Authorized Personnel conducting the due diligence is expected to:

    a. Review the principal place of business, as provided in the Articles of Incorporation and business registrations versus the office address provided in the application form and the location of CBS branch where the customer is applying to open an account.

    b. Require a separate license from PAGCOR if the client is operating outside the jurisdiction of the economic zone authority granting the license.

    For **service provider** or **gaming support provider**, the license may indicate the specific gaming entity to whom they are allowed to render such services. Thus, they cannot render such support/services to gaming entities not specifically provided in the license.

2. **Validation of the License/Accreditation with the Licensing Authority.** The Authorized Personnel conducting the due diligence shall validate the registration or accreditation of the corporate entity through the following means:

Issuing Authority	Means of Validation
SEC	- Through iSEC View in the SEC website
PAGCOR	- For granted POGO licenses, the list is available in the PAGCOR website: http://www.pagcor.ph/regulatory/offshore-gaming.php - For list of eSabong Operators Licensed and Allowed to Commence Operations, please see PAGCOR website: https://www.pagcor.ph/regulatory/pdf/esabong/list-of-pagcor-licensed-e-sabong-operators.pdf - For casino, other gaming entity, and support or service provider registered with PAGCOR – refer to AML Department for email validation with PAGCOR
APECO, AFAB and CEZA	- For casino, other gaming entity, and support or service provider registered with other licensing authority (e.g. APECO, AFAB, and CEZA) – coordinate with the AML Department for email validation.

The result of validation/confirmation shall be printed and attached to the EDD Form.

3. **Use of the Due Diligence Questionnaire (DDQ).** For gaming entities and providers of gaming-related services, the check box of items 1 to 6 shall be checked as YES, accordingly.

   The DDQ is also applicable to all sole proprietorship (*any type of business*), non-gaming-related BPOs, IT/Technology, Consultancy, or other technical services provider, and clients with personal account with high volume or high value of deposits (*collectively referred to as "non-gaming clients"*). The following minimum guidelines shall apply whenever a non-gaming client answers YES on the items of the DDQ:

4. **Analysis of counterparties and ultimate beneficial owners.** For the analysis, the following documents and information will be needed:

   a. UBO Determination Form
   b. Latest GIS of the client – for the listing of stockholders, directors and officers
   c. Latest GIS of direct and indirect corporate stockholders of the client – for the listing of stockholders, directors and officers
   d. List of Major Counterparties
   e. List of entities and/or organizations where the individual client is an officer, stockholder, or director

f. Other information that may be pulled out from readily available sources (e.g. internet)

The Authorized Personnel conducting the due diligence shall prepare a matrix or tabular presentation showing the interrelations of the following:

a. The entity client
b. The entity client's stockholders, directors and officers
c. The direct corporate stockholder's stockholders, directors and officers
d. The indirect corporate stockholder's stockholders, directors and officers
e. The counterparties (*and stockholders if available*)
f. The individual client (*signatory/representative*)
g. The entities or organizations where the individual client is an owner, stockholder, director or officer.

With the above interrelations being established, the Authorized Personnel shall determine if the client corporation and the identified counterparties are owned, controlled or managed by the same person or group of persons.

The above analysis will also facilitate subsequent transaction monitoring.

5. **Reconciliation of the company profile, purpose and intended business relationship.** In reconciling the information, the Authorized Personnel conducting the due diligence will need the following documents:

a. Articles of Incorporation – disclosing the primary and secondary purposes of the corporation, the date of incorporation and the initial amount of capital authorized, subscribed and paid.
b. License/Accreditation from PAGCOR or other appropriate government agency – disclosing the nature of the authority/accreditation granted expiration/duration, and any limitations (*e.g. provisional license, limits for support or service provider*).
c. Latest GIS – for the disclosed purpose, current ownership structure, and financial data
d. Documentation of the understanding of the nature and complexity of the business.
e. Purpose of the business relationship or account to be opened.
f. Rental agreement (if any).
g. Average daily credit transactions.

The disclosures on the above documents such as the nature and complexity of the business, financial data and the purpose of the account/business relationship with the bank must all be consistent with the primary purpose of the corporation. The result of such reconciliation shall be documented in the EDD Form.

Financial data such as total assets, cash and cash equivalents, total equity, authorized capital stock, and others shall be look into to spot any inconsistency. Examples of inconsistencies are as follows:

a. The company is a gaming support or service provider but bulk of the assets are in the form of cash and cash equivalents, this may indicate that the company is operating as a gaming entity (without license) or perform functions beyond the license/accreditation granted;

b. The authorized capital stock in the Articles of Incorporation (AOI) is lower than what is provided in the Audited Financial Statements (AFS), which may indicate that the AFS provided is falsified or the AOI provided is not updated to reflect the important changes;

c. The gross sales or the net income is too low despite of high cash in AFS or as deposited in the Bank and several years of operation, which may be an indication that the client is evading taxes;

d. The cash and cash equivalent in the AFS is lower than the balance of the client's account with CBS or other banks, which may indicate undeclared funds that may be related to tax evasion or unlawful activities;

e. The estimated daily credit to the account may be too high considering the annual gross sales which may indicate undeclared source of funds and possibly related to unlawful activities.

The above examples are not exhaustive. The Authorized Personnel conducting the due diligence may spot other inconsistencies relating to the financial information obtained. Such inconsistencies detected shall be inquired with the client and be resolve in favor of the due diligence conducted by the Bank.

6. The basic and enhanced due diligence procedure for on-boarding and updating of customers provided in the MTPP not covered in the above provisions shall be performed.

See **Annex X** for the Checklist of Documentary Requirements.

6.15.7 Common Indicators to Detect Undeclared Gaming Activities

The following indicators are more helpful in detecting undeclared gaming or gaming-related activities of suspected customers, who are usually doing business in the guise of BPO, IT/Technology Company, Consultancy or other technical service provider:

1. The client and the counterparty (*e.g. customer, supplier*) have common stockholders/owners, directors, or officers,
2. The foreign company (parent or otherwise) was incorporated in known tax haven jurisdictions (*e.g. British Virgin Islands, Turks and Caicos, Isle of Man or Samoa*);
3. The UBOs are those who control the funds of the account;
4. The customers are usually service or gaming support providers;
5. Large and complex remittances without clear underlying business, support or justification. Sometimes, these transactions are facilitated by MSBs;

6. Use of individual account in conducting business transactions;
7. The owner of the business or the UBO has also a remittance or forex dealer/money changer business and/or real estate company;
8. The existence and proliferation of illegal bookie joints and other forms of organized illegal gambling connected with all play-for-pay sports and amusement games;
9. The use of formation agents that are not registered as DNFBPs with the AMLC;
10. The international inward remittances come from individuals or entities in countries where online gaming is prohibited (*e.g. People's Republic of China*);
11. The international inward remittances of the client and the counterparty come from the same country and the same sender.
12. Large cash transactions;
13. Transaction seems to be inconsistent with the customer's apparent financial standing or the usual pattern of activities;
14. Activity is inconsistent with what is expected from the declared business;
15. Conflicting reasons and supporting documents for substantial transactions (wire transfer or cash-based);
16. Unclear large foreign exchange transactions, which appear inconsistent with the business model.

The above indicators are not grounds for outright filing of STR. When a customer who initially declared as not engaged in gaming or gaming-related activity has any of the above indicators, the Authorized Personnel of the Bank shall initially require the filling-up of the Due Diligence Questionnaire (DDQ). If the customer declared involvement in gaming or gaming-related activities, immediate updating of customer records shall be performed to comply with the requirements of the guidelines.

However, if the customer is engaged in activities other than gaming, such fact shall be established by requiring additional official documents. Whenever the identified indicator is not resolved to fully establish the real activities of the client, the account shall be closed and a suspicious transaction report must be filed.

6.15.8 Approval Requirements

Business relationship with a gaming entity or entities engaged in gaming-related activities shall be approved up to the Group Head of the business group prior to opening of any account and to updating of customer information, records, or both.

The following minimum documents shall be provided to the approving officers:

1. Background of the company/business
2. Signed EDD Form applicable to gaming/gaming-related customers
3. Matrix of Counterparties and UBOs
4. Other documents that may be required by the approver

The branch / business unit shall likewise furnish the following with all current records of the customer simultaneous with the seeking of the approval of the Group Head:

1. Chief Compliance Officer – Compliance Division
2. AML Compliance Department Head – AML Compliance Department
3. AML Policies Officer – AML Compliance Department

6.15.9 Documentation of the Enhanced Due Diligence Performed and Approval

The process and results of the enhanced due diligence performed shall be documented in the **EDD Form (see Annex Y)** applicable to gaming and gaming-related clients.

6.15.10 Deferring of Gathering of Documents

In consideration to the larger number of documents requested compared to other high risk clients of the bank, OGB clients may defer submission certain documents for a maximum of one (1) month reckoned from the date of request/ date of updating of client's KYC records.

Documents Not Deferrable:

1. SEC Registration for corporation or partnership; DTI registration for sole proprietorship;
2. Articles of Incorporation/Partnership (*for corporation or partnership*);
3. License or Accreditation from the appropriate government agency (*refer to Section C. Licensing/Accrediting Authorities*);
4. AMLC Registration - Provisional Certificate of Registration (PCOR) or Certificate of Registration (COR) (*for POGOs and Casinos, including internet and ship-based casinos, with respect to their casino cash transactions related to their gaming operations and Offshore Gaming Operators, as well as their service providers, supervised, accredited or regulated by the PAGCOR or any Appropriate Government Agencies (AGA)*);
5. Board or Partner's resolution duly certified by the corporate/partners' secretary, or other equivalent document, authorizing the signatory to sign on behalf of the entity;
6. Listing of banks where the entity has business relationship;
7. Filled-up listing of major counterparties (*e.g. suppliers, service providers, financier, large customer*) – **see Annex V: Counterparty Disclosure Form**;
8. Filled-up Due **Diligence Questionnaire – see Annex W** (*this questionnaire is also mandatory for all sole proprietorship business and those IT/Technology, BPO, Consultancy and technical service entities not related to gaming)*;
9. Business Permit;
10. Other official documents supporting the source of funds and purpose of the business relationship or intended use of the account to be opened.

For clients engaged in cockfighting and/or eSabong whichever applicable:

11. SEC Registration for corporation or partnership; DTI registration for sole proprietorship;
12. Articles of Incorporation/Partnership (*for corporation or partnership*);

13. Board or Partner's resolution duly certified by the corporate/partners' secretary, or other equivalent document, authorizing the signatory to sign on behalf of the entity;
14. City/Municipal License for the operation and maintenance of cockpits;
15. Mayor's Permit/Municipal License for the relevant gaming activities from the location of the company office and of the cockpit arenas/venues where the eSabong feeds will be coming from;
16. Detailed location sketch of company office & base of operations;
17. Photocopy of BIR Registration Certificate;
18. eSabong platform documentations, i.e. website and/or desktop or mobile application documents indicating, among others, the main functions, web design and contents, accounting documents and other salient details like compliance with AML/CFT laws;
19. Certification from an independent gaming laboratory certifying that the betting system of the eSabong platform was extensively tested and has been found compliant with the following standards:
    a. All data are captured, accounted and reported by the system;
    b. Game is fair, secure and able to be audited and operated correctly;
20. List of contracted local government unit (LGU)-licensed cockpit arena's;
21. Letter of No Objection (LONO), in any form, interposing no objection to the conduct of sabong operations in said cockpit arenas/venues and the taking and broadcasting of feeds therefrom;
22. Certification from an independent gaming laboratory attesting to Internet Protocol (IP) blocking of all other IP addresses excluding Philippine IP addresses designated by the applicant;
23. Other official documents supporting the source of funds and purpose of the business relationship or intended use of the account to be opened.

In case of a foreign corporation, the official documents equivalent to the above (*nos. 1-15*) shall be required. In case of a foreign corporation with a branch or office here in the Philippines, the requirements and the due diligence required in the succeeding provisions shall apply to both the foreign parent company and the branch/office here in the Philippines.
For individuals (*proprietor or authorized representatives*), the following information shall be required and recorded in the EDD Form:

1. IDs applicable to individuals;
2. List of Banks where he/she has previous or existing business relationship;
3. List of entities and/or organizations where the client is an officer, stockholder, or director.

Documents Deferrable for a maximum of one (1) month:

1. Latest General Information Sheet (GIS) for corporation or equivalent official document where the owners, directors, and officers are disclosed;
2. Evidence of source of income/wealth such as Audited Financial Statements (AFS) or Annual Tax Return filed duly stamped by BIR;
3. Business/Company Profile, either provided as integral part of the official annual report, disclosure in the official website, or document signed by the CEO or equivalent position or owner;
4. GIS of any corporate stockholder of the client (*regardless of the percentage of holdings*);
5. GIS of a company who holds indirect ownership of the corporate client;

6. Rental/Lease Agreement (*if applicable*);

For clients engaged in cockfighting and/or eSabong whichever applicable:

7. Latest General Information Sheet (GIS) for corporation or equivalent official document where the owners, directors, and officers are disclosed;

In case of a foreign corporation, the official documents equivalent to the above (*nos. 1-15*) shall be required. In case of a foreign corporation with a branch or office here in the Philippines, the requirements and the due diligence required in the succeeding provisions shall apply to both the foreign parent company and the branch/office here in the Philippines.
For individuals (*proprietor or authorized representatives*), the following information shall be required and recorded in the EDD Form:

1. IDs applicable to individuals;
2. List of Banks where he/she has previous or existing business relationship;
3. List of entities and/or organizations where the client is an officer, stockholder, or director.

Deferring submission of documents shall be approved up to the Group Head of the branch or business unit. Request for approval shall likewise include Compliance Division as recipients. In addition, deferral of documents submission shall not apply to on-boarding.

Compliance Division, along with the Department, Division, or Group Head, shall follow up the branch or business unit. AML Compliance Department shall report the status updates to the AML Committee.

6.15.11 Non-Compliance with The Bank's Requirements

Whenever the Bank is unable to completely perform the required due diligence or the result of the due diligence performed is unsatisfactory, the Bank may deny or restrict the transaction or terminate the business relationship with the client and shall file a suspicious transaction reports whenever appropriate.

6.15.12 Framework for Gaming and Gaming-related Clients

As gaming and gaming-related clients are considered high risk due to the nature of their industry and their operations, a framework is crafted to further enhance the Bank's existing controls in handling gaming and gaming-related clients. The framework serves as a complement to this guidelines. Refer to **Annex Z** for the Framework for Gaming and Gaming-related Clients.

6.16 GUIDELINES IN ACCEPTING BUSINESS RELATIONSHIP WITH MONEY SERVICE BUSINESS (MSB) CLIENTS

6.16.1 Coverage

This new amendment to the MTPP covers current and prospective MSB clients wherein the business relationship with the Bank is being or will be directly used to facilitate their licensed activity (Account for Licensed Activity). The succeeding procedures will be applied prior to establishment, renewal or updating of business relationship.

However, **Remittance Agents** or **Sub-Agents** are required to apply for accreditation and pass the accreditation requirements of the Bank's Treasury Operations Department (TOD). Thus, remittance agents applying to open an account with any branch, to facilitate its remittance operations, shall be referred to the TOD for evaluation and accreditation.

6.16.2 Definition of Terms

1. **Money Service Business (MSB) –** collective term used to refer a Remittance and Transfer Company (RTC), and Money Changer/Foreign Exchange Dealer (FXD).

2. **Remittance and Transfer Company (RTC) –** any entity that provides money or value transfer services (MVTS). RTC includes the following:
    a. Remittance Agent (RA)
    b. Remittance Platform Provider (RPP)
    c. E-Money Issuer (EMI)

3. **Money or Value Transfer Service (MVTS) –** refers to financial services that involve the acceptance of cash, cheques, other monetary instruments or other stores of value and the payment of corresponding sum in cash or other form to a beneficiary by means of a communication, message, transfer, or through a clearing network.

4. **Remittance Agent (RA) –** any entity that operates a remittance business network which includes any or combination of the following:
    a. Remittance Direct Agent (RDA) – entity that is covered by a direct contracted remittance agreement or similar agreement to act in behalf of a third party engaged in remittance business.
    b. Remittance Agent Network Provider (RANP) – any entity that provides a network to perform remittance business.
    c. Other similar entities as may be determined by the Monetary Board

5. **Remittance Platform Provider (RPP) –** entity that provides a shared or common platform/IT infrastructure and maintains settlement accounts in order to provide funds for remittance transactions within its network.

6. **E-Money Issuer (EMI) –** any entity authorized by the BSP to provide money transfer or remittance services using electronic stored money value system and similar digital financial services.

7. **Remittance Sub-Agent (RSA)** – any person authorized by the RTC to perform certain relevant undertakings in the remittance business. This includes any person that is allowed by an RDA, RNAP

and/or EMI to do any part of the remittance business in their behalf. For purposes of registration, an RSA with at least one (1) branch shall be considered as an RA.

8. **Money Changer (MC)/Foreign Exchange Dealer (FXD) –** any entity who engages in money changing/foreign exchange dealing business. This includes Authorized Agent Banks' subsidiary/affiliate forex corporations (AAB-forex corps), among others.

9. **Account for Licensed Activity (ALA) –** pertains to the account or business relationship with the Bank that is directly used by the MSB client for the operation of its licensed activity (i.e. remittance, money changing, forex dealing). This type of account or business relationship requires overall review of the MSB client's Anti-Money Laundering and Anti-Terrorist Financing policies, aside from the existing procedures of enhanced due diligence for High Risk accounts.

10. **Account for Other Activity (AOA) –** pertains to the account or business relationship with the Bank that is not used by the MSB client for the operation of its licensed activity (i.e. payroll, petty cash fund, operating expenses fund). Review of Anti-Money Laundering and Anti-Terrorist Financing policies shall not be required for MSBs with only this type of account or business relationship with the Bank.

6.16.3 Information and Documentary Requirements

Pursuant to BSP Circular 950 as amended by BSP Circular 1022 and without prejudiced to other account opening documents and forms implemented that are not included herein, all MSBs shall submit at least the following requirements:

Individual/Single Proprietorship	Partnership/Corporation
1. Valid IDs – (of owner, agent, ultimate beneficial owner)	1. Valid IDs – (of authorized signatories transacting with the bank, principal officers, ultimate beneficial owner)
2. Duly accomplished CIF (of owner, agent, ultimate beneficial owner)	2. Duly accomplished CIF (of authorized signatories, principal officers, ultimate beneficial owner)
3. DTI Registration	3. SEC Certificate of Registration
4. Latest financial statement audited by a reputable audit firm and latest Income Tax Return submitted to BIR	4. Latest financial statement audited by a reputable audit firm and latest Income Tax Return submitted to BIR
5. BSP Certificate of Registration	5. Articles of Incorporation or Partnership
6. AMLC Certificate of Registration	6. Board/Partnership Resolution allowing business relationship with the Bank, and appointment of Authorized Signatories
7. AML/CTF Policies	7. By-Laws or Constitution
8. Duly accomplished AML Questionnaire (**see Annex AA**)	8. Duly accomplished AML Questionnaire (**see Annex AA**)

9. List of other business or organization from which the client (owner or ultimate beneficial owner) is a stockholder/owner, director or officer	9. 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
10. List of banks where the client has current or former banking relationship	10. BSP Certificate of Registration
11. Proof of address such as latest utility bills, bank or credit card statement or similar document recently issued showing the address. These documents should be addressed to the name of the business or the owner.	11. AMLC Certificate of Registration
	12. Board approved AML/CTF Policies
	13. List of banks where the client has current or former banking relationship
	14. Certificate of Registration of other secondary licensed activities, if any
	15. GIS or similar official document of corporations who hold at least 20% of the MSB client's voting shares

For entities registered outside 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 and should also be authenticated by the Philippine consulate or notary public, where the said entities are registered.

Other information and documents may be requested from the MSB in the course of the due diligence performed by the Bank.

6.16.4 Purpose, Terms and Conditions of Business Relationship

The MSB customer, upon application for opening an account, shall execute an **Application for Business Relationship (see Annex AB)** that contains the following:

1. Name of the MSB;
2. The licensed activity;
3. Purpose for the account or business relationship;
4. Terms and Conditions

The application form shall be the basis of the determination of additional documents, due diligence, and approval required.

6.16.5 Required Enhanced Due Diligence Procedures

1. Minimum Enhanced Due Diligence (EDD) Procedures:

   Given the High Risk classification, the following minimum validation procedures shall apply to all MSBs:

Individual/Single Proprietorship	Partnership/Corporation
1. Confirming the date of birth from a duly authenticated official document;	1. Validating source of funds or source of wealth from reliable official documents such as audited financial statements, ITR, bank references, etc.
2. Verifying the address through sending thank you letters and evaluation of utility bills, bank or credit card statement, or other documents showing address or through on-site visitation;	2. Inquiring from the supervising authority the status of the entity;
3. Contacting the customer by phone or email;	3. Verifying the address through on-site visitation of the company, sending thank you letters, or other documents showing address;
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;	4. Contacting the entity by phone or email;
5. Determining the veracity of the declared source of funds;	5. Negative news review on the corporation, the principal officers, authorized signatories and ultimate beneficial owners;
6. Negative news review on the business, owner, agent (if any), and ultimate beneficial owner (if any);	6. Watchlist verification, thru Base60, of the corporation, principal officers, authorized signatories and ultimate beneficial owner, persons owning at least 20% of the capital stock;
7. Watchlist verification, thru Base60, of the business, owner, agent (if any), and ultimate beneficial owner (if any);	7. Validation required for the ID and source of fund of an individual shall be applied to the authorized signatories, principal officers, and ultimate beneficial owner (if any);
8. Review of the latest audited financial statements to see any negative disclosures pertaining to regulatory sanction due to AML violations and similar nature;	8. Review of the latest audited financial statements to see any negative disclosures pertaining to regulatory sanction due to AML violations and similar nature;
9. Verify registration with government databases available.	9. Verify registration with the government databases available.

2. Additional EDD Procedure – Evaluation of AML/CTF Compliance:

    a. In evaluating the AML/CTF policies of the MSBs, the following provisions will be checked if present:

        - Face-to-face contact requirement

- Gathering of identification documents
- Gathering of at least the minimum information from the customer (i.e. remitter, beneficiary)
- Screening of the customer's name from various watchlisht (i.e. OFAC, UN, EU, HMT)
- Risk assessment and due diligence of clients
- Screening/monitoring of the customer transactions to detect possible suspicious transaction
- Requiring supporting documents on large transactions or transactions initially determined as not commensurate to the customer's profile
- Criteria for suspicious transaction
- Compliance with the requirements of covered transaction filing
- Compliance with the requirements of suspicious transaction filing
- Compliance with the record-keeping requirements
- Provision for appointment of a compliance officer handling AML/CTF compliance
- Compliance with the AML training requirements

Absence or insufficiency of any of the above provisions will be communicated to the MSB customer for correction/updating.

b. In the evaluation of the duly accomplished AML Questionnaire, the following minimum procedures shall be performed:

- Match the answers with the applicable documents presented by the MSB such as the AML/CTF policy, BSP and AML Certificate of Registration, KYC documents;

- Answers will be compared with the answers in the accomplished questionnaire of the immediately preceding period to check for any changes;

- Answers to any question that is opposite to the expected answer or not the same with the immediate answer on the previous questionnaire on file shall be subject to further inquiry and confirmation with the MSB;

- The questionnaire must be signed by the MSB's designated Compliance/AML Officer or officers designated to handle AML/CTF compliance.

c. Customer identification and transaction forms of the MSB will also be gathered and assessed by the Bank. The following minimum procedures shall be performed:

- On customer identification form, ascertain if the mandatory information per BSP Circular 950 as amended by BSP Circular 1022 are present and are treated as mandatory per policies of the MSB;

- On transaction form, ascertain if the transaction amount (forex and peso, if applicable), customer name (remitter and beneficiary, as applicable), required customer details (i.e. address), and information on the IDs submitted are present.

d. Upon assessment of the AML/CTF policy, AML Questionnaire and Forms of the MSB, the Bank will provide a formal assessment of the overall AML compliance of the MSB. Each factors will be scored and that will determine the overall rating of AML compliance of the MSB. The rating shall be expressed in terms of:

Descriptive Rating	General Assessment of AML Compliance	Actions to be taken
Satisfactory	The MSB generally complies with the minimum requirements of the Bank on AML Compliance **with minor or no issues** noted upon review of the AML/CTF policy, AML Questionnaire, MSB Forms and other documents.	May allow business relationship with the Bank with commitment to resolve any minor issues noted.
Needs Improvement	The MSB generally complies with the minimum requirements of the Bank on AML Compliance but with **moderate issues** noted upon review of the AML/CTF policy, AML Questionnaire, MSB Forms and other documents.	May allow business relationship with the Bank, provided: 1. The account shall not be used for its licensed activity until moderate issues are resolved; 2. Commitment to resolve minor issued noted, if any; 3. No remittance of any kind or fund transfer in behalf of its customer shall be allowed until the moderate issued noted are resolved.
Unsatisfactory	The MSB is **not compliant** with the minimum requirements of the Bank on AML Compliance due to **major to severe issues** noted upon review of the AML/CTF policy, AML Questionnaire, MSB Forms and other documents.	Business relationship with the Bank shall not be used for the MSB's licensed activity. No remittance of any kind or fund transfer in behalf of its customer shall be allowed. Can only use the account to facilitate its licensed activity **after one (1) full year** from the date of resolution of ALL moderate to severe issues noted.

The "Action to be taken" above is reflective of the degree of AML compliance of the MSB only. More restrictive actions may be imposed depending on the results of the overall assessment of the MSB after considering the overall results of enhanced due diligence.

e. For MSBs not engaged in the remittance business, the assessment shall be done by the Branch/Business Unit where the Customer Information Sheet was accomplished, subject to Compliance Testing.

6.16.6 Senior Management Approval

1. Group Head approval shall be obtained prior to the start of the business relationship with the Bank regardless of the purpose of the account. If the account or business relationship previously not used for licensed activity will be used to facilitate its licensed activity (regardless of number of transactions), approval up to the Group Head shall be required.

2. The manner of approval may be by original signature or via email by the designated approver. When seeking approval, the following minimum documents shall be provided to the designated approver:

    a. Application for Business Relationship
    b. ECRAF
    c. Results of EDD
    d. Assessment of AML/CTF policy
    e. Others required by the approver or other Bank policies

3. The branch / business unit shall likewise furnish the following with all current records of the customer simultaneous with the seeking of the approval of the Group Head:

    a. Chief Compliance Officer – Compliance Division
    b. AML Compliance Department Head – AML Compliance Department
    c. AML Policies Officer – AML Compliance Department

6.16.7 Subsequent Monitoring of Transactions

Accounts of all MSBs shall be subject to strict monitoring. Emphasis will be given to transactions of MSBs that are reflected either in the Large Transactions Report (FCBS) and Transaction Alerts (Base60). In reviewing the subsequent MSB transactions, the Branch/Unit shall ensure that:

1. The transaction is performed within the purpose for which the account was created, as reflected in the Application for Business Relationship or other contract.

2. For transactions executed by the MSBs in behalf of their own customer, minimum information per BSP Circular 950 as amended by BSP Circular 1022 is obtained. The MSB may present their own customer/application form or use the Bank's prescribed form if the former is not sufficient.

3. For any transaction that breaches the Bank's established thresholds or is inconsistent with the profile or past transactions of the MSB or its customer, the Bank shall require the underlying documents supporting the transaction's legality, purpose and economic justification.

4. In the performance conduct of annual review for the renewal or updating of business relationship, subsequent compliance with the preceding rules on monitoring of transactions will also be assessed.

6.16.8 Updating of MSB Customer Information

In addition to the existing policies on updating of accounts, the following documents shall be required from the MSB customer upon updating:

Document	Frequency of Updating
1. Latest Audited Financial Statements and ITR	Annually
2. Valid IDs	During annual updating if IDs previously presented have already expired or with changes in personal information
3. AMLC Certificate of Registration	During annual updating if AML COR has expired or with amendment/s
4. Latest General Information Sheet	Annually
5. AML/CTF Policies	During annual updating if AML/CTF Policies have recent amendments
6. AML Questionnaire	Annually

The required Enhanced Due Diligence Procedures above shall be applied during the updating or renewal of business relationship with the Bank.

In addition, a separate assessment based on the subsequent monitoring of transactions shall be part of the overall assessment of the MSBs AML compliance upon renewal or updating of business relationship with the Bank.

The approval of the Group Head is required upon updating of client information.

The branch / business unit shall likewise furnish the following with all current records of the customer simultaneous with the seeking of the approval of the Group Head:

1. Chief Compliance Officer – Compliance Division

2. AML Compliance Department Head – AML Compliance Department
3. AML Policies Officer – AML Compliance Department

6.16.9 Deferring of Gathering of Documents

In consideration to the larger number of documents requested compared to other high risk clients of the bank, MSB clients may defer submission certain documents for a maximum of one (1) month reckoned from the date of request/date of updating of client's KYC records.

Documents Not Deferrable:

Individual/Single Proprietorship	Partnership/Corporation
1. Valid IDs – (of owner, agent, ultimate beneficial owner)	1. Valid IDs – (of authorized signatories transacting with the bank, principal officers, ultimate beneficial owner)
2. Duly accomplished CIF (of owner, agent, ultimate beneficial owner)	2. Duly accomplished CIF (of authorized signatories, principal officers, ultimate beneficial owner)
3. DTI Registration	3. SEC Certificate of Registration
4. BSP Certificate of Registration	4. Articles of Incorporation or Partnership
5. AMLC Certificate of Registration	5. Board/Partnership Resolution allowing business relationship with the Bank, and appointment of Authorized Signatories
6. Duly accomplished AML Questionnaire (**see Annex AA)**	6. By-Laws or Constitution
7. List of other business or organization from which the client (owner or ultimate beneficial owner) is a stockholder/owner, director or officer	7. Duly accomplished AML Questionnaire (**see Annex AA**)
8. List of banks where the client has current or former banking relationship	8. 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
9. Proof of address such as latest utility bills, bank or credit card statement or similar document recently issued showing the address. These documents should be addressed to the name of the business or the owner.	9. BSP Certificate of Registration
	10. AMLC Certificate of Registration
	11. List of banks where the client has current or former banking relationship
	12. GIS or similar official document of corporations who hold at least 20% of the MSB client's voting shares

Documents Deferrable for a maximum of one (1) month:

Individual/Single Proprietorship	Partnership/Corporation
1. Latest financial statement audited by a reputable audit firm and latest Income Tax Return submitted to BIR	1. Latest financial statement audited by a reputable audit firm and latest Income Tax Return submitted to BIR
2. AML/CTF Policies	2. 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
	3. Board approved AML/CTF Policies
	4. Certificate of Registration of other secondary licensed activities, if any*

*The Certificate of Registration of other secondary licensed activities is only deferrable if the purpose of the account is not for the processing of transactions involving the secondary licensed activities.

Deferring submission of documents shall be approved up to the Group Head of the branch or business unit. Request for approval shall likewise include Compliance Division as recipients. In addition, deferral of documents submission shall not apply to on-boarding.

AML Compliance Department shall report the status updates to the AML Committee.

6.16.10 Grounds for Non-Acceptance or Discontinuance of Business Relationship

Upon opening of the account or during renewal or updating or business relationship, the Bank shall not allow establishment, renewal or updating of business relationship with MSB on the following grounds:

1. Failure to comply with the documentary and information requirements of the Bank;
2. Material inconsistencies on the information and documents submitted;
3. Violation on the terms and conditions on the Application for Business Relationship or other similar contract;
4. Attempt or actual use of the account for MSBs licensed activity or telegraphic transfer or inward remittance, despite Unsatisfactory assessment of AML compliance;
5. Involvement in a money laundering case or unlawful activities;
6. Other grounds for closure on other policies of the Bank.

6.16.11 Annual Review of Account and Transactions

The annual review of account and transactions of MSB clients shall be done by BSOMD every 30th June of the year. See **Annex AC** Standard Template on Annual Analysis of MSB Clients.

6.17 GUIDELINES ON ACCEPTING CLIENTS ENGAGED IN CASH-INTENSIVE BUSINESSES

6.17.1 Cash-Intensive Business

A Cash-Intensive Business (CIB) is an entity that *receives a significant amount of receipts in cash*[3]. Money launderers may run or use cash-based business to commingle illegally obtained funds with cash actually generated by the business. While most CIBs are conducting legitimate business, some aspects of these businesses may be susceptible to money laundering or terrorist financing. The following are risk scenarios associated with cash intensive businesses because of the opportunity for perpetrators to:

- Launder large amounts of cash, which are proceeds of criminal activity, by claiming that the funds originate from economic activities;
- Launder amounts of cash, which are proceeds of criminal activity, by justifying its origin based on fictitious economic activities (both for goods and services);
- Finance, through often small amounts of cash, terrorist activities without any traceability

It is for these reasons that CIBs are considered as high-risk businesses that demands application of appropriate due diligence and ongoing monitoring.

6.17.2 Identifying CIBs During On-Boarding

Companies that qualify as cash-intensive businesses can vary. These types of entities have high volume of transactions paid via cash rather than remittance or check. Below are samples of businesses that can be categorized as CIBs:

- Gasoline Stations
- Water Refilling Stations
- Junkshops
- Food Cart Business
- Bars, Cafes, and Restaurants
- General Merchandise Businesses
- Hardware Stores
- Spare Parts & Car Accessories Dealer
- Car Repair/Maintenance Shop
- Car Washes
- Textile/Clothing Retailers
- Convenience Stores
- Laundromats

[3] Taken from https://www.irs.gov/pub/irs-utl/cashchapter1_210627.pdf

- Cigarette Distributor
- Liquor Store
- Parking Garage
- Trucking
- Vending Machine Operator

Determination of a cash-intensive business is not via the entity's name but rather by its business activities. Corporations, sole proprietorships and partnerships with gross sales receipts of at least Php5, 000,000.00 or more monthly shall initially be considered as CIBs by the Bank (the threshold will be reviewed and adjusted, when necessary). This shall be determined during onboarding through the interview conducted by the branch personnel, visits to the business site/warehouse and validation of submitted documents, among others. Once confirmed to be a CIB, the Bank's Customer Acceptance Policy as stated in the MTPP shall apply.

6.17.3 Additional On-Boarding Requirements

In addition to the regular on-boarding requirements, all clients with cash-intensive business shall open an account under the true and registered name of the entity. Likewise, the CIF shall be tagged as a cash-intensive business and be subject to enhanced transaction monitoring. It should be noted that these clients are not high risk by default.

Through interview and initial review of required/submitted/applicable documents, the Authorized Personnel conducting the due diligence shall document the following additional information in the EDD Form:

a. **Understanding of the nature and complexity of the business.** This disclosure shall at least include description of the following:

    a. Background and history of the business;
    b. Description of services or goods provided;
    c. Types of clients catered by the business;
    d. Major supplier of goods or services;
    e. Direct competitors;
    f. Ownership structure;
    g. Nature of relationship with the counterparties;
    h. Geographical coverage of business operation;
    i. Other information that supplements the explanation of the nature of the business shall also be gathered if available.

b. **Purpose of the business relationship or account to be opened.** This disclosure shall document all the purpose for which the account/business relationship is intended to be used.

If the intended use/purpose of the business relationship is for ''low-risk" activity such as payroll or application for ordinary loan (except Back-to-Back and Revolving Credit Line), only the standard enhanced due diligence requirement per MTPP will apply. Otherwise, the enhanced due diligence requirement of these guidelines shall be observed.

c. **Average daily credit/debit transactions.** The information may be derived from the financial statements or disclosure of the client. This will include deposits, fund transfer, inward remittances, withdrawals, outward transfer and inward checks. This information will be used for transaction monitoring purposes.

d. **Ultimate Beneficial Owner (UBO).** Using the GIS of the client corporation (for direct owners) and GIS of corporate stockholders/indirect owners, the ultimate beneficial owner shall be established according to AMLC guidelines in determining UBOs. The disclosure shall be made in the **UBO Determination Form**. If obtaining the GIS of a direct and indirect stockholder from the entity client is not possible, the Authorized Personnel conducting the due diligence shall gather information from other credible sources such as those readily available in the internet (*e.g. iSEC View in the SEC website*).

Information required per internal policy of a unit/department not included in the above listing shall not be affected.

The branch/unit shall use the CIB Checklist during on-boarding. The checklist shall be included in the client's KYC folder. Refer to **Annex AE**.

6.17.4 Risk Rating

The clients covered by this guidelines shall not be treated by the Bank as default high risk clients. Customer risk classification shall be based on the computed risk score in ECRAF/ACRA.

6.17.5 Ongoing Monitoring

Alerts investigators shall inform branches or business units on potential high-risk structures of low/normal risk businesses alerted for review should it meet criteria and behavior of high risk customer segments.

In the course of their investigation of alerts generated during transaction monitoring, alerts investigators may come across businesses that display behavior/characteristics similar to that of CIBs but lack proper tagging in the Bank's records (i.e. incorrect risk rating) or lack of documentation to support scale of business. In such instance, the alerts investigator shall inform the branch of account of their findings for the branch to review that account if it can be classified as a CIB and if tagging as high risk is necessary. The branch may obtain supporting documentation as necessary.

Further to the monitoring done by the alerts investigators, the Business Manager, Branch Service Head and Branch Operations Head shall perform daily review/monitoring of Significant Activity Report (SAR)

and conduct on-going due diligence on the business relationship and scrutiny of transactions subject of SAR. Any transaction of a suspicious nature shall be reported under the Bank's procedures for reporting suspicious transactions.

The branch/unit shall use the CIB Checklist during updating of the client's information. The checklist shall be included in the client's KYC folder. Refer to **Annex AE**.

6.17.6 Non-Compliance with the Bank's Requirements

Whenever the Bank is unable to completely perform the required due diligence or the result of the due diligence performed is unsatisfactory, the Bank may deny or restrict the transaction or terminate the business relationship with the client and shall file a suspicious transaction report whenever appropriate.

6.18 GUIDELINES IN HANDLING CLIENTS AND TRANSACTIONS FROM HIGH RISK PHILIPPINE AREAS

6.18.1 Definition of Terms

1. **High Risk Philippine Area** – any city, municipality, province, or region in the Philippines that is determined to have terrorism or insurgency related activities (see **Annex P – List of High Risk Philippine Areas**)
2. **Transactor** – the person or individual who makes the transaction, other than, or on behalf of, the account holder. Transactor may also be the accountholder himself.
3. **Party** – one of the individuals or entities directly involved in the transaction. This includes the accountholder, sender, beneficiary, counterparty, and transactor.

6.18.2 Determination of High Risk Philippine Areas

A city, municipality, or province or region within the Republic of the Philippines shall be considered as high risk location if it has at least one of the following characteristics:

1. With terrorism or insurgency activities, as cited by the Department of National Defense, and Philippine National Police.
2. Declared as a terrorism or insurgency hotspot by the aforementioned government agencies in the previous item.

The risk rating for each specific area shall be provided by the Compliance Department to Branches and Business Units for their reference. The said ratings shall effect the computation of the Automated Customer Risk Assessment (ACRA) in the bank's core banking system.

6.18.3 Updating of List of High Risk Philippine Areas

The list of High Risk Philippine Areas shall be updated monthly or as needed.

Amendments, including additions, changing of names, and de-listing shall be presented to the AML Committee for approval prior to dissemination to all units.

6.18.4 Clients from High Risk Philippine Areas

A client, whether an individual or entity, shall be considered by the Bank as from a high risk Philippine area if:

1. The client's declared residential address, whether permanent or present, is within a high risk Philippine area.
2. The client's declared office/business address or address of the employer or principal place of business is within a high risk Philippine area.

6.18.5 Transactions Involving High Risk Philippine Areas

A transaction is considered to be in a high risk Philippine area if:

1. At least one of the parties' declared personal address and/or office/business address is within a high risk Philippine area.
2. The funds to be transferred is bound for or will come from a high risk Philippine area.
3. The source of the funds to be transacted is from a high risk Philippine area.
4. The beneficiary/ultimate beneficiary of the transaction is from a high risk Philippine area.

6.18.6 On-Boarding of Customers

Business relationship shall only be established if the customer is not part of the Sanctions List or the ATC Designated Persons List. To determine whether business relationship can be established, the branch or business unit must ensure that the following actions are timely and properly done:

- Screening against the Internal Watchlist for all new customers and parties before any economic benefit may be made to the customer
- Performance of Due Diligence measures such as gathering of information, identification and customer risk profiling
- In case of potential target match or target match, deny on-boarding and file RISA.

Customers from high risk Philippine areas are not automatically tagged as high-risk. Same treatment applies to parties' previously tagged coming from these high-risk areas. Following existing policy, risk classification is based on the result of ECRAF/ACRA.

6.18.7 Processing of Transactions

A transaction involving a high risk Philippine area shall only be processed if none of the parties, source of the funds, and the beneficiary/ultimate beneficiary (if determined) is part of the Sanctions List or the

ATC Designated Persons List. In addition, the branch or business unit must ensure that the following actions are timely and properly done:

- Screening against the Internal Watchlist (all parties, the source of the funds, and the beneficiary/ultimate beneficiary) before permitting the customer to engage in any transaction
- Remittance transactions bound for any high risk Philippine area are subject to Transaction Enhanced Due Diligence (TEDD)
- In case of potential target match and target match, deny transaction and file RISA.

6.19 GUIDELINES IN HANDLING CLIENTS AND TRANSACTIONS FROM HIGH RISK COUNTRIES AND JURISDICTIONS

The high risk countries and jurisdictions (high risk countries) are geographical locations with known AML/CFT deficiencies and with active sanctions programme.

As a form of control, the following are the guidelines in handling customers and transactions from high risk countries/jurisdictions:

1. As Democratic People's Republic of Korea (DPRK), also referred to as North Korea, and Iran are countries subject to a call for action / black list under FTAF and these countries have comprehensive sanctions programme, no inward/outward remittance is allowed. Account opening for individual or entities is also not allowed. The same is true with Russia with expanded sanctions imposed by US, EU and other countries following its invasion of Ukraine.

2. For the rest of the listed countries/jurisdictions, inward or outward remittance may be allowed subject to independent comment or approval of the senior management. Account opening for individual customers are tagged as high risk; whereas account opening for entities residing or incorporated in these countries are conditionally allowed subject to the following: tagged as high risk, approval from senior management, a justification from the branch/unit and not part or included in the Sanctions Lists.

Refer to **Annex P** for the List of High Risk Countries/Jurisdictions.

PART VII
ON-GOING MONITORING OF CUSTOMERS

PART VII: ON-GOING MONITORING OF CUSTOMERS

On-going monitoring is a process of determining and implementing a periodic review of all information regarding the customers with whom the Bank has a business relationship. The on-going monitoring shall be carried out on a periodic basis for as long as the Bank has a business relationship with the customer. On-going monitoring of customers is demonstrated in the following stages:

1. Pre-transaction Monitoring Controls
2. Post-transaction Monitoring Controls
3. Monitoring of Negative News Report
4. Internal Watchlists Monitoring
5. Sanctions Lists Monitoring
6. Updating of Customer Records

7.1 PRE-TRANSACTION MONITORING CONTROLS

For transactions that are processed by the branch/unit that are initiated by the client or another person for the account of the client, part of the review controls should contain a brief assessment of the transaction to determine if further due diligence is required. Further due diligence may be in the form of requiring additional information or documents from the customer, performing validation procedures or conduct of transaction enhanced due diligence, before the transaction is finally approved for processing.

For transactions initiated or involving transactors, the beneficiary and the purpose of the transaction must be gathered. In the event the transactor mention a beneficiary other than the account holder of a depositor of the Bank, the mentioned beneficiary shall likewise be recorded/documented. Each transaction of the transactor shall have a clear purpose to reduce the risk of the transaction being used for ML/TF purposes.

7.1.1 Fund/Wire Transfers

Because of the risk associated with dealing with fund/wire transfers, where a Bank may unknowingly transmit proceeds of unlawful activities or funds intended to finance terrorist activities, the following procedure shall be observed:

7.1.1.1 The Bank, as the originating financial institution:

The Authorized Personnel shall not accept instructions to fund/wire transfer from a non-customer originator unless it has conducted the necessary customer due diligence to establish the true and full identity and existence of the said originator.

As a rule, the Bank shall not process any wire transfer from a non-customer originator. In the case of a customer who is a Remittance company/agent who performs wire/fund transfer transaction in behalf of its own clients (not a customer of CBS), the requirements of the KYCC policy shall apply (*see section 7.1.4 of the MTPP*).

A. The Authorized Personnel shall ensure that all wire transfers are always accompanied by the required information such that:

1. Cross-border and domestic fund/wire transfers and related message **not exceeding Php50,000** or its foreign currency equivalent, shall include accurate and meaningful originator and beneficiary information which shall remain with the transfer or related message through the payment chain:

    - Name of the originator
    - Name of the beneficiary
    - Account number of the originator and beneficiary, or in its absence, a unique reference number

2. For cross-border and domestic fund/wire transfers and related message **exceeding Php50,000** or more, or its equivalent foreign currency, the following information shall be obtained and accompany the wire transfer:

    - Name of the originator
    - Originator account number where such an account is used to process the transaction or a unique transaction reference number which permits traceability of the transaction
    - Originator's address, or national identity number, or customer identification number, or date and place of birth
    - Name of the beneficiary
    - Beneficiary account number where such an account is used to process the transaction or a unique transaction reference number which permits traceability of the transaction

B. **Purpose and Applicability.** To provide guidance on the implementation of the requirements of the Money Laundering and Terrorist Financing Prevention Program (MTPP) on cross-border wire transfers, these guidelines aim to ensure that:

1. The beneficiary of a cross-border outward remittance transaction is not among the Specially Designated Nationals (SDNs) identified by governments or organization of foreign countries who are subject to sanctions. If the beneficiary is a positive match in the SDNs, blocking/freezing of the transaction and account must be appropriately performed.

2. If the country of destination is among those included in the list of High Risk Countries/Jurisdictions, blocking/holding of transaction is implemented or if applicable, enhanced due diligence and determination of the applicability of existing sanction programs are performed prior to transaction execution.

3. Transactions passing through established thresholds or red-flags are subjected to prior enhanced due diligence, and approved by the authorized officer as defined in these guidelines.

4. Good business relationship with our domestic and foreign correspondent banks and with the BSP or AMLC is maintained by ensuring that outward remittances are subjected to prior due diligence.

5. The Bank and its remittance facility shall not be used to facilitate money laundering, terrorist financing and other unlawful activities.

   The following provisions shall also apply to cross-border telegraphic transfers to Money Service Businesses (MSBs) with remittance license, with the requirements of the Know-Your-Customer's Customer (KYCC) policy as supplement. Please refer to KYCC Policy on MSB Transactions in section 7.1.4 (A), (B), (C) of the MTPP.

C. **Initial Review Requirements.** Upon receipt of the Application for Telegraphic Transfer Form, make sure that the following are immediately conducted:

1. Ensure that the required information per outward remittance policy is complete.

2. Review the **purpose** of the outward remittance transaction – the purpose of remittance should be expressed in **specific terms**. In case of several types of goods involved, the purpose may be expressed in terms of general classification of the goods. For purchase of goods, aside from the specific type of goods, the name of the vessel that will carry the goods purchased, and the port name (origin and destination) shall be included, if available.

   Examples:

   (Wrong) Payment for purchase of goods
   (Wrong) Payment of Invoice no. 1234
   (Correct) Payment of Invoice no. 1234 various automotive parts
   (Correct) Payment for purchase of Electric Drills; shipped via XYZ Shipping
   (Correct) Partial payment of loan
   (Correct) Proceeds of sale of house and lot

3. Establish the **relationship** between the client-remitter and beneficiary via interview and/or other documents presented. Disclose such relationship beside the 'Beneficiary Name" field of the telegraphic transfer form.

D. **Watchlist and Negative News Screening.** The following watchlist screening and verification procedure **shall be performed by the processing branch/unit to ALL cross-border outward remittance**:

1. **Country of Destination** – ensure that the country of destination:

   - Is not among in the list of High Risk Countries/Jurisdictions where **no outward remittance transaction is allowed** (see **Annex P**: for the list of SDCs for Outward Remittance)

   - If among those high risk countries/jurisdictions where transaction is allowed but requiring Transaction Enhanced Due Diligence (TEDD), ensure that a TEDD is performed and the TEDD Form is accomplished. (See **Annex AJ**: TEDD Form)

   - If among those high risk countries/jurisdictions where "independent comment" of a designated independent unit is required, ensure that such comment is obtained **prior** to the transaction execution and senior officer approval.

2. **Beneficiary Bank** – via inquiry in the Base60 Watchlist, ensure that the beneficiary bank is not among the Specially Designated Nationals (SDNs) from OFAC or sanctioned individuals or entities by UN, EU or HMT.

3. **Beneficiary** – via inquiry in the Base60 Watchlist, ensure that the beneficiary is not among the Specially Designated Nationals (SDNs). These are individuals or entities included in the sanctions lists (i.e. OFAC, UN, EU, HMT). Ensure also that if the beneficiary is among those in the selected Internal Watchlist, **transaction enhanced due diligence is performed**.

4. **Client-Remitter or True Remitter** (in case of remittance by an MSB) – via inquiry in the Base60 Watchlist, ensure that the true remitter is not among the Specially Designated Nationals (SDNs). These are individuals or entities included in the sanctions lists (i.e. OFAC, UN, EU, HMT). Ensure also that if the beneficiary is among those in the selected Internal Watchlist, **transaction enhanced due diligence is performed**.

Positive match in any of the sanctions lists (i.e. OFAC, UN, EU, HMT) shall warrant denial of transaction and filing of STR. In addition, positive match with the UN (UNSC) shall warrant **automatic freezing** of the customer's account, whereas termination of business relationship shall be implemented for the rest (positive match with OFAC, EU, HMT). Positive match with the internal watchlist requires performance of TEDD.

Positive Match in watchlist name screening is achieved when:

1. **For individual-beneficiary** – there's match in the name (first and last) and date of birth of the watchlist person and beneficiary. If there's no date of birth available in the watchlist, the Branch/Unit shall utilize the internet to search for other information common to the individual-beneficiary and the watchlist person.

2. **For entity/corporate-beneficiary** – the entity/corporate-beneficiary name is the same with that of the watchlist person.

3. **For beneficiary bank** - the beneficiary bank name is the same with that of the watchlist person.

4. **For client-remitter or true remitter in case of remittance by an MSB** – same criteria for name matching in item nos. 1 and 2 above, for individual-beneficiary and juridical entity/corporate, respectively.

   The screenshot of the Base60 watchlist inquiry shall be printed and attached to the Telegraphic Transfer Form for record purposes. The result of positive match must be recorded in the print-out.

E. **Threshold and Red Flag Test.** The processing branch/unit shall ensure that threshold and red-flag tests are performed and that those passing the test are subjected to Transaction Enhanced Due Diligence (TEDD).

1. THRESHOLD TEST:

a. Cross-border outward remittance passing the following THRESHOLDS will be automatically subject to Transaction Enhanced Due Diligence (TEDD):

Outward Remittance Transaction (Foreign Currency Denominated)	Single transaction of at least:
• If the client-remitter is an **individual** (**or sole proprietorship**)	$20,000 or its equivalent 3rd currency
• If the client-remitter is a juridical entity/corporate	$50,000 or equivalent 3rd currency

The thresholds provided herein shall effectively be applied also to transactions subject to KYCC (for MSB transactions).

b. The following specific transactions passing the above thresholds are **exempted** from subsequent TEDD requirement, provided it has **none of the red flags** enumerated in item no. ii (Red Flag Test) below:

- Subsequent transactions pertaining to payment of contractual obligation to the **same beneficiary** (e.g. for service or product) where the payment schedule and the amount of periodic payments are stated in the official contract, provided that the source of funding such payments and underlying purpose are satisfactorily established in the TEDD of the first transaction, and copy of official contract is on-hand.

- Subsequent transactions pertaining to loan and related payments to the **same registered financial institution-beneficiary**, where the copy of official loan contract is provided and the source of payment was established in the TEDD already performed for the initial transaction.

- The recurring transaction is for the pursuance of its primary business purpose/s, provided that the **beneficiary is the same** and normal transaction level (*in amount, volume, timing and frequency*) of the customer is established by the Branch/Unit.

- The beneficiary of the transaction is a registered domestic bank.

- The transaction of the customer has the same nature, purpose, and beneficiary with the previous transaction initially subjected to TEDD, provided that official documents supporting the nature, purpose and source of fund of the transaction has been established in the TEDD of the initial transaction.

Regardless of the above, TEDD shall be required **for each transaction** whenever the country of destination is among the list of High Risk Countries/Jurisdictions.

2. RED FLAG TEST:

Regardless of amount, the transactions with the following **RED FLAGS** shall be subject to the conduct of Transaction Enhanced Due Diligence (TEDD):

a. Amount of remittance is inconsistent with the documented source of fund of the client-remitter.
b. Purpose of remittance is inconsistent with the profile or nature of business of the client-remitter.
c. The frequency of cross-border outward remittance transaction is not normal considering the nature and/or size of business of the client-remitter.
d. The transfer has no legal, trade/commercial or economic sense.

e. Country of destination is a High Risk country (*See **Annex P** for the list of High Risk Countries/Jurisdictions*)
f. The client-remitter/transferor is a High Risk client (*except if covered by the KYCC policy*).
g. The client-remitter/transferor is the subject of a recent negative news report per watchlist screening (in Base60) or Internet Search (*required for High Risk and PEP*).
h. The client-remitter/transferor is the subject of suspicion in a previous STR filed or AMLC inquiry or Freeze Order (*per watchlist screening*).
i. The purpose of the cross-border outward remittance is "Gift" or "Donation".
j. The goods to be paid are precious stones (*e.g. diamond, gem, ruby*).
k. The goods to be paid are precious metals (*e.g. gold, silver, platinum, nickel*).
l. The goods to be paid are highly valued art works, collector's piece or antiques.
m. The goods to be paid are chemicals (*e.g. fertilizer, petroleum products*).
n. The goods to be paid are guns, ammunition, explosives, military equipment or raw materials or major parts thereof that will be used to manufacture such.
o. The goods to be paid are of any kind of wild animal (*living or otherwise*) or parts thereof.
p. The transaction is possibly or actually related to a known unlawful activity.
q. There is reasonable suspicion that the transaction is executed to avoid detection of the true country of destination, or to avoid the above thresholds, or to avoid the preceding red-flags or the reporting requirements of the Philippine AMLA.
r. The client-remitter is not the buyer of the goods or services being paid (*e.g. the client ordering the remittance as payment is not a party to the contract/underlying transaction*)
s. And other similar type and nature of transactions that warrant close monitoring according to the bank's assessment and discretion.

F. **Transaction Enhanced Due Diligence (TEDD) Requirement.** Transactions passing the Threshold or Red-flag tests will prompt the performance of TEDD. The TEDD involves the following activities:

1. Gather basic documents supporting the declared purpose of the transaction and relationship between the client-remitter and beneficiary (*e.g. certified true copy of transaction invoice or similar documents to support the transaction/s*).

   If the basic document/s supporting the purpose of the transaction cannot be obtained, the reason shall be indicated in the TEDD Form and the Authorized Officer shall gather information from the customer via interview to establish the

specific purpose of the transaction and the relationship between the remitter and the beneficiary.

2. Conduct review of transaction/s, and properly document the review in the TEDD Form (see **Annex AJ**). The purpose of the review is to detect any suspicious indicators present in the transaction.

3. Require submission of official documents supporting the legitimate purpose of the transaction (*e.g. Customs' clearance, import license, insurance certificate, description of goods, and underlying contracts*) in case of **suspicion** or **if the transaction does not make considerable sense** according to the customer's profile and information.

4. Require submission of official documents supporting the source of funding (*e.g. financing agreement, loan contract, letter of credit, etc.*) if the funding of transaction comes from other/independent sources, or the declared source of income of the customer is deemed insufficient to fund the transaction.

5. Perform Internet Search (*e.g. Google, etc.*) on top of the sanction screening to spot any negative news/information that may affect the decision to approve the transaction. The search shall apply to the client-remitter, beneficiary, beneficiary bank and other parties to the transaction.

6. Seek comment from an independent unit (i.e. AML Department) in case the country of destination is among the High Risk Countries/Jurisdictions in **Annex P**.

7. Provide recommendation whether to process or deny the transaction. Transaction shall be denied and STR shall be filed in any of the following cases:

    a. The suspicion on the transaction was not resolved despite the submission and review of documents provided by the customer;

    b. The suspicion on the transaction was not resolved due to non-submission and deliberate refusal of the customer to provide documents required under item nos. 3 and 4 above;

    c. The result of the verification of customer is Positive Match in the following:

        I. sanctions lists (OFAC, UN, EU, HMT);
        II. internal watchlist "FO" (subject to Freeze Order);

Highest approval in section "G" (Independent Comment and Senior Officer Approval) below must be required in the following, regardless of amount:

a. The customer is a positive match in the internal watchlists.

The customer is a positive match to any recent negative news or information pertaining to money laundering or other unlawful activity upon performance of an internet search.

8. Secure senior officer approval for the conducted TEDD.

The above TEDD procedures shall also apply to MSB-executed cross-border transfer with the **original remitter** being the subject of TEDD. To facilitate the performance of TEDD, the requirements of Know-Your-Customer's Customer (KYCC) must also be submitted and satisfied on top of the "Certification of Due Diligence" to be provided by the MSB (*refer to MTPP 7.1.4 Money Service Business, C. Due Diligence Standards for MSB Transactions, no.3*).

Whenever the original remitter in an MSB-executed outward remittance transaction is considered a default High Risk client per Bank policy, **prior enhanced due diligence** on the original remitter must be performed (*with proper coordination with the MSB*) **as if** such original remitter is a client of the Bank.

G. Independent Comment and Senior Officer Approval

1. For **cross-border** outward remittances where independent comment is required, the comment of the designated independent unit must be secured prior to approval and transaction execution.

2. Independent comment to be provided by the designated independent unit (e.g. AML Department) shall pertain only to the transaction inquired by the branch/unit and **shall not be applied to subsequent transactions**, regardless of the similarity of facts presented. The email comment must be printed and attached to the Application for Outward Telegraphic Transfer Form.

3. Approval of an officer on the TEDD performed is required prior to transaction execution. Thus, the accomplished TEDD Form and comment of the independent unit (if required) must be forwarded to the approving officer for review. The approval must be documented in the TEDD Form, or attached to the TEDD Form if approval was made electronically via IBM Lotus Notes/Email.

Matrix of Approval for TEDD performed based on the following transaction amounts:

CROSS-BORDER OUTWARD REMITTANCE TRANSACTION	
	Approving Authority:

For Foreign Currency Denominated	Branches	Other Units*
Up to $100,000 or its third currency equivalent	Endorsed by Branch Service Head (BSH) and approved by Division Head	Division Head
More than $100,000 to $500,000 or its third currency equivalent	Endorsed by Branch Service Head (BSH) and approved by Division Head	Division Head
More than $500,000 or its third currency equivalent	Endorsed by Branch Service Head (BSH), recommended by Division Head, and approved by Group Head	Group Head
Positive match in internal watchlist (other than "FO" and "PDEAPNP") or the customer is a subject of recent negative news pertaining to money laundering or unlawful activity, **regardless of amount**.	Endorsed by Branch Service Head (BSH), recommended by Division Head, and approved by Group Head	Group Head

*Minimum requirement for Head Office Units

The above approval requirement applies only to the TEDD performed by the Branch/Unit. The above shall not affect the existing approval requirements for processing outward remittance transaction.

Whenever the previous TEDD is being relied upon, the Authorized Personnel of the Branch/Unit shall ensure that the above approval matrix is strictly complied with. Thus, if subsequent transaction warrants higher approval considering a larger amount, appropriate approval must be obtained.

H. Servicing Branch/Unit is not the Branch/Unit of Account (Inter-Branch).

In case the client-remitter does not maintain an account with the servicing branch, and the transaction passes the "threshold" and/or "red-flag" test, the servicing branch must coordinate with the branch of account who will conduct the following:

1. Performance of TEDD

2. Secure approval of the authorized officer as stated in the Matrix of Approval.

THRESHOLD TEST:

a. Cross-border outward remittance passing the following THRESHOLDS will be automatically subject to Transaction Enhanced Due Diligence (TEDD):

Outward Remittance Transaction (Foreign Currency Denominated)	**Single transaction of at least:**
• If the client-remitter is an **individual** (**or sole proprietorship**)	$20,000 or its equivalent 3rd currency
• If the client-remitter is a juridical entity/corporate	$50,000 or equivalent 3rd currency

The thresholds provided herein shall effectively be applied also to transactions subject to KYCC (for MSB transactions).

b. The following specific transactions passing the above thresholds are exempted from subsequent TEDD requirement, provided it has none of the red flags enumerated in item no. ii (Red Flag Test) below:

- Subsequent transactions pertaining to payment of contractual obligation to the same beneficiary (e.g. for service or product) where the payment schedule and the amount of periodic payments are stated in the official contract, provided that the source of funding such payments and underlying purpose are satisfactorily established in the TEDD of the first transaction, and copy of official contract is on-hand.

- Subsequent transactions pertaining to loan and related payments to the same registered financial institution beneficiary, where the copy of official loan contract is provided and the source of payment was established in the TEDD already performed for the initial transaction.

- The recurring transaction is for the pursuance of its primary business purpose/s, provided that the beneficiary is the same and normal transaction level (in amount, volume, timing and frequency) of the customer is established by the Branch/Unit.

- The beneficiary of the transaction is a registered domestic bank.

- The transaction of the customer has the same nature, purpose, and beneficiary with the previous transaction initially subjected to TEDD, provided that official documents supporting the nature, purpose and source of fund of the transaction has been established in the TEDD of the initial transaction. Regardless of the above, TEDD shall be required for each transaction whenever the country of destination is among the list of High Risk Countries/Jurisdictions.

RED FLAG TEST:

Regardless of amount, the transactions with the following RED FLAGS shall be subject to the conduct of Transaction Enhanced Due Diligence (TEDD):

a. Amount of remittance is inconsistent with the documented source of fund of the client-remitter.
b. Purpose of remittance is inconsistent with the profile or nature of business of the client-remitter
c. The frequency of cross-border outward remittance transaction is not normal considering the nature and/or size of business of the client-remitter.
d. The transfer has no legal, trade/commercial or economic sense.
e. Country of destination is a High Risk country (See **Annex P** for the list of High Risk Countries/Jurisdictions.
f. The client-remitter/transferor is a High Risk client (except if covered by the KYCC policy).
g. The client-remitter/transferor is the subject of a recent negative news report per watchlist screening (in Base60) or Internet Search (required for High Risk and PEP).
h. The client-remitter/transferor is the subject of suspicion in a previous STR filed or AMLC inquiry or Freeze Order (per watchlist screening).
i. The purpose of the cross-border outward remittance is “Gift” or “Donation”.
j. The goods to be paid are precious stones (e.g. diamond, gem, ruby).
k. The goods to be paid are precious metals (e.g. gold, silver, platinum, nick
l. The goods to be paid are highly valued art works, collector’s piece or antiques.
m. The goods to be paid are chemicals (e.g. fertilizer, petroleum products).
n. The goods to be paid are guns, ammunition, explosives, military equipment or raw materials or major parts thereof that will be used to manufacture such.
o. The goods to be paid are of any kind of wild animal (living or otherwise) or parts thereof.
p. The transaction is possibly or actually related to a known unlawful activity.
q. There is reasonable suspicion that the transaction is executed to avoid detection of the true country of destination, or to avoid the above thresholds, or to avoid the preceding red-flags or the reporting requirements of the Philippine AMLA.
r. The client-remitter is not the buyer of the goods or services being paid (e.g. the client ordering the remittance as payment is not a party to the contract/underlying transaction)

s. And other similar type and nature of transactions that warrant close monitoring according to the bank's assessment and discretion.

The Branch of Account shall be given two (2) hours turnaround time to provide the accomplished TEDD Form upon receipt of the email request from the Servicing Branch. To ensure receipt of the TEDD request, the Servicing Branch shall also call the Branch of Account informing of the email request.

The following pro-forma email shall be used by the **servicing branch** in requesting for confirmation from the branch of account:

Email Subject: Requesting Confirmation of Compliance for Outward Telegraphic Transfer of _____ (state customer's full name)

To XXXX Branch,

This is to request confirmation of compliance with the AML/CFT guidelines for the outward remittance of (customer's full name) with the following details:

Outward Telegraphic Transfer application amount:	*(amount)*
Currency Type:	*(currency type: e.g. USD)*
Country of Destination:	*(name of country)*
Beneficiary:	*(name of beneficiary)*
Purpose of the Outward Remittance:	*(detailed and specific purpose)*
Underlying Transaction:	*(Nature and particulars of the transaction to be funded/settled by the outward remittance)*

Please answer the following "Due Diligence" questions:

Due Diligence Questions:	***Answer with "Yes" or "No"***
1. Was there prior TEDD performed for transactions with the same purpose and beneficiary name above?	
*2. If **YES** in no. 1, was the TEDD approved by the authorized Officer?*	

*3. If **NO** in no. 1, was the TEDD performed and approved for the above transaction?*	
4. Does the branch of account have any reservation in processing the transaction?	
5. Do you recommend processing of the subject transaction?	

(Attach the TEDD Form and official documents gathered from the client, if applicable)

Kindly provide your response immediately for the speedy processing of the transaction.

The **branch of account** must perform **TEDD** whenever necessary. The following pro-forma email shall be used by the **branch of account** in responding to the request for confirmation of the servicing branch. Ensure that the complete email history is included in the response:

Email Subject: Re: Requesting Confirmation of Compliance for OTT of (client name)

To XXXX Branch,

This is to confirm compliance with the AML/CFT guidelines for the outward remittance of the above client with the following results:

Due Diligence Questions:	***Answer with "Yes" or "No"***
1. Was there prior TEDD performed for transactions with the same purpose and beneficiary name above?	*(Yes or No)*
*2. If **YES** in no. 1, was the TEDD approved by the authorized Officer?*	*(Yes, No or NA)*
*3. If **NO** in no. 1, was the TEDD performed and approved for the above transaction?*	*(Yes, NO or NA)*
4. Does the branch of account have any reservation in processing the transaction?	*(Yes or No)*
5. Do you recommend processing of the subject transaction?	*(Yes or No)*

The **servicing branch** should be responsible in the performance of the following in line with the conduct of Due Diligence:

1. Watchlist screening of the parties to the outward remittance transaction.
2. Screening of the country of destination and seeking comment of the independent unit if applicable.
3. Determination if the transaction passed the **threshold and red-flag test**.
4. Gathering from the client-remitter of the required official documents per TEDD requirement.

If the client-remitter also maintains an account with the servicing branch/unit and simply wishes to debit his/her account with another branch to fund the application for outward remittance, the entire due diligence procedures provided in this guidelines will be performed by the servicing branch only.

7.1.1.2 The Bank, as the intermediary financial institution:

A. Ensure that, for cross-border wire transfers, all originator and beneficiary information that accompany a wire transfer are retained in the payment message. Where technical limitations prevent the required originator or beneficiary information accompanying a cross-border wire transfer from remaining with a related domestic wire transfer, the Bank should keep a record of all the information received from the originating financial institution or another intermediary financial institution for at least five (5) years;

B. Take reasonable measures, which are consistent with straight-through processing, to identify cross-border wire transfers that lack required originator information or required beneficiary information;

C. Conduct transactional watchlist screening on the payment parties, both for the originator, beneficiary and the originating bank;

D. The applicable policies on cross-border transfers shall be applied by the Authorized Personnel for transactions of the Bank as an intermediary party to a remittance transaction.

7.1.1.3 The Bank, as the beneficiary financial institution:

A. **Purpose and Applicability.** To provide guidance on the implementation of the requirements of the Money Laundering and Terrorist Financing Prevention Program (MTPP) on cross-border inward wire transfers, these guidelines aim to ensure that:

1. Cross-border inward remittances flagged by the Treasury Operations Department (TOD) are subjected to enhanced due diligence.

2. Good business relationship with our domestic and foreign correspondent banks and with the BSP or AMLC is maintained by ensuring that flagged inward remittances are subjected to due diligence prior to crediting.

3. The Bank is not used to facilitate money laundering, terrorist financing and other unlawful activities.

   Check if the identity of the beneficiary has been previously and satisfactorily verified. If yes, maintain this information in accordance with the record-keeping policy of the Bank. Should the originator and beneficiary be of the same person, the beneficiary institution (bank) may rely on the due diligence performed by the originating bank, as part of the third-party reliance in case of domestic wire transfers.

   Real-time or post monitoring must be implemented in order to identify cross-border wire transfers lacking the required originator or beneficiary information. The Authorized Personnel must ensure that the originator or the information of the beneficiary, as applicable, is available for review and careful examination by the Compliance Division, Internal Audit and/or the Regulators.

B. **Threshold and Red Flag Test.** Prior to crediting, the Treasury Operations Department (TOD) shall scan for the following cross-border inward remittances:

1. First time remittance amounting at least $10,000 or other foreign currency equivalent;
2. Remittance passing through the following thresholds;

Inward Remittance Transaction (Foreign Currency Denominated)	**Single transaction of at least:**
• If the client-remitter is an **individual** (**or sole proprietorship**)	$20,000 or its equivalent 3rd currency
• If the client-remitter is a juridical entity/corporate	$50,000 or equivalent 3rd currency

   The thresholds provided herein shall effectively be applied also to transactions subject to KYCC (for MSB transactions).

3. If the originator/remitter is a central bank of any country by name;

4. If the beneficiary-client is a foundation by name (i.e. name with the word foundation);

5. If the beneficiary-client is a money service business by name (e.g. names with the words “remittance”, “remit”, “foreign exchange”, “exchange”, “forex”, or “money”, “changer”);

6. Sanctioned jurisdictions or jurisdictions with weak AML/CFT laws, regulations, and compliance (see **Annex P** for the list of High Risk Countries/Jurisdictions) for Inward Remittance);

7. Unusually large amount of transaction as independently determined by the Treasury Operations Department.

8. Material discrepancy in name, if the recommendation is to credit the remittance.

In the above circumstances, the TOD shall email first the Branch/Unit requiring the conduct of transaction enhanced due diligence on the inward remittance.

C. **Recall of Inward Remittance.** The Treasury Operations Department (TOD) shall inform the Branch/Unit on recall of the cross-border inward remittance per advisory of the correspondent bank.

Recall request from the correspondent bank due to **fraud** or **other unlawful activity** mentioned in the SWIFT message shall prompt the branch/unit to:

1. File an STR on the remittance transaction requested for recall; and

2. Conduct TEDD on the customer’s profile and transactions, including determination of the counterparties, to assess the appropriateness on termination of business relationship.

D. **Watchlist and Negative News Screening.** For inward remittances flagged by the Treasury Operations Department (TOD), watchlist and negative news screening must be performed to the following:

1. Original remitter of the remittance
2. Originating Bank and/or money service business
3. Other parties identified
4. Country of origin

For the sanctions list screening, the Base60 must be utilized. The screenshot of the Base60 watch list inquiry shall be printed and attached to the TEDD Form. **Positive Match** in watchlist screening is achieved when:

1. **For individual-remitter (or other party-individual)** – there's match in the name (first and last) and date of birth of the watchlist person and remitter. If there's no date of birth available in the watchlist, the Branch/Unit shall utilize the internet to search for other information common to the individual-remitter and the watchlist person.

2. **For entity/corporate-remitter (or other party-entity/corporate)** – the entity/corporate-remitter name is the same with that of the watchlist person.

3. **For originating bank** – the originating bank name is the same with that of the watchlist person.

4. **For country of origin** – the originating country is among the countries where remittance is prohibited. For countries included in the list of High Risk Countries/Jurisdictions per **Annex P**, the appropriate due diligence is conducted and documented in the TEDD Form.

Positive match in any of the **sanctions lists** (*i.e. OFAC, UN, EU, HMT*) shall warrant denial of transaction and filing of STR. In addition, positive match with the UN list shall warrant **automatic freezing** of the customer's account. Upon Freezing, the Branch/unit shall inform the Compliance Division and Legal Department for the assistance of the preparation of the freeze order return. Termination of business relationship shall be implemented for the rest of the sanctions lists (positive match with OFAC, EU, UN, HMT).

For the negative news screening, the Authorized Personnel of the branch/unit shall make a search through the internet (e.g. Google) to check for any negative news pertaining to the above. The beneficiary-client shall also be subject to negative news screening.

In case of suspicion that the inward remittance is directly or indirectly related to the negative news (*on unlawful activity*)/freeze order/AMLC inquiry/STR previously filed involving the **remitter** or **beneficiary-client** or **third party** (if any), such inward remittance shall be denied for crediting. Other negative news that does not warrant the denial of the crediting of the remittance, including those pertaining to the country of origin or the remitting bank, shall be disclosed in the TEDD including the reason why it does not affect the transaction.

E. **Transaction Enhanced Due Diligence Requirement.** Transactions passing the Threshold or Red-Flag Tests will prompt the performance of TEDD. The TEDD involves the following activities:

1. Gather the following additional information from the beneficiary-client:

    a. Specific purpose of the remittance

b. Nature of relationship between remitter and beneficiary-client (and other parties to the transaction)
c. Source of funding of the inward remittance

2. Conduct review of transaction/s, and properly document the review in the TEDD Form (see **Annex AJ**). The purpose of the review is to detect any suspicious indicators present in the transaction.
3. Perform Internet Search (*e.g. Google, etc.*) on top of the sanction screening to spot any negative news/information that may affect the decision to approve the transaction. The search shall apply to the client-remitter, beneficiary, beneficiary bank and other parties to the transaction.
4. Seek comment from an independent unit (i.e. AML Department) in case the country of destination is among the specially designated countries for inward remittance in **Annex P**.
5. Provide recommendation whether to process or deny the transaction. Transaction shall be denied and STR shall be filed in any of the following cases:

    a. The suspicion on the transaction was not resolved despite the submission and review of documents provided by the customer;

    b. The suspicion on the transaction was not resolved due to non-submission and deliberate refusal of the customer to provide documents required to support the transaction;

    c. The result of the verification of customer is Positive Match in the following:

        I. sanctions lists (OFAC, UN, EU, HMT);
        II. internal watchlist "FO" (subject to Freeze Order);

    d. There is suspicion that the inward remittance is directly or indirectly related to the STR or Freeze Order or AMLC Inquiry or negative news implicating the remitter or the beneficiary-client to an actual/possible unlawful activity.

    Highest approval in section "F" (Senior Officer Approval) below must be required in the following, regardless of amount:

    a. The customer is a positive match in the internal watchlists.

    b. The beneficiary-customer or the true remitter is a positive match to any recent negative news or information pertaining to unlawful activity upon performance of an internet search, and the inward remittance is

determined to be **not related** in any way to such unlawful activity mentioned in the negative news.

6. Secure authorized officer approval for the conducted TEDD.

The above TEDD procedures shall also apply when the beneficiary of a foreign inward remittance is an MSB with the TEDD being applied to the original beneficiary (*client of the MSB*). To facilitate the performance of TEDD, the requirements of Know-Your-Customer's Customer (KYCC) must also be submitted and satisfied on top of the "Certification of Due Diligence" to be provided by the MSB (*refer to MTPP 7.1.4 Money Service Business, C. Due Diligence Standards for MSB Transactions, no.3*).

Whenever the client of an MSB (*the true beneficiary*) in a cross-border inward remittance transaction is considered a default High Risk client per Bank policy, **prior enhanced due diligence** on the true beneficiary shall be performed (*with coordination of the MSB*) **as if** such true beneficiary is a client of the Bank.

The Authorized Personnel of the Branch/Unit may rely on the previous TEDD performed provided that ALL of the following conditions exist:

1. Same true originator;

2. The remittance covers payments of goods/services in the ordinary course of business;

3. No negative news pertaining to the true remitter or beneficiary on the previous TEDD performed;

4. No positive match in the sanctions or internal watchlists on the previous TEDD performed;

5. No red-flags as provided in section B (*items 3 to 8*);

6. The previous TEDD did not result into filing of STR and/or termination of business relationship; and);

7. Separate senior officer approval (*see section F*) is required depending on the amount of the remittance.

The reliance to prior TEDD shall not apply to cross-border inward remittance to beneficiary-clients who are High Risk per Bank's policy.

F. **Independent Comment and Senior Officer Approval.**

For **cross-border** inward remittances where independent comment is required, the comment of the designated independent unit must be secured prior to approval and transaction execution. Independent comment to be provided by the designated independent unit (e.g. AML Compliance Department) shall pertain only to the transaction inquired by the branch/unit and **shall not be applied to subsequent transactions**, regardless of the similarity of facts presented.

Approval of the authorized officer on the TEDD performed shall be required **prior** to the crediting of the remittance. Thus, the accomplished TEDD Form shall be forwarded to the approving officers for their review. The approval shall be documented in the TEDD Form or shall be provided electronically via the officer's official email.

Matrix of Approval for TEDD performed based on the following transaction amounts:

CROSS-BORDER INWARD REMITTANCE TRANSACTION		
For Foreign Currency Denominated	**Approving Authority:**	
	Branches	**Other Units***
Up to $100,000 or its third currency equivalent	Endorsed by Branch Service Head (BSH) and approved by Division Head	Division Head
More than $100,000 to $500,000 or its third currency equivalent	Endorsed by Branch Service Head (BSH) and approved by Division Head	Division Head
More than $500,000 or its third currency equivalent	Endorsed by Branch Service Head (BSH), recommended by Division Head, and approved by Group Head	Group Head
Positive match in internal watchlist (other than "FO" and "PDEAPNP") or the customer is a subject of recent negative news pertaining to money laundering or unlawful activity, **regardless of amount**.	Endorsed by Branch Service Head (BSH), recommended by Division Head, and approved by Group Head	Group Head

The above approval requirement applies only to the transaction enhanced due diligence performed by the Branch/Unit. The above shall not affect the existing approval requirements for processing inward remittance transaction.

G. **Standard Reply for Branches/Units.**

Upon completion of the TEDD, the branch/unit shall respond to the email of TOD copy furnished the approving officers of the transaction (if applicable) using the following format:

If the transaction PASSED the TEDD requirement:

*"Please be informed that the inward remittance described in the previous email **PASSED** the enhanced due diligence conducted by the branch (or unit) as documented in the TEDD Form retained as part of the KYC/transaction documents.*

In compliance also with the approval requirement of the policy, the transaction enhanced due diligence on the above remittance was approved by the following officers as disclosed in the TEDD Form or separate documentation:

Position Title ***Approving Officer's Name (N/A if not applicable)***

1. *Branch Service Head*
2. *Business Manager*
3. *Area Head*
4. *Region Head*

*Kindly cause the **CREDITING** of the amount to the account described in your previous email."*

If the transaction FAILED the TEDD requirement:

*"Please be informed that the inward remittance described in the previous email **FAILED** the enhanced due diligence conducted by the branch (or unit) as documented in the TEDD Form retained as part of the KYC/transaction documents.*

*Kindly cause the **RETURN** of the amount to the remitting bank citing the following reason: (e.g. transaction did not pass the bank's required due diligence)."*

The Branch/Unit is required to complete the above due diligence and provide the appropriate response to the TOD based on the results of the due diligence not later than 04:00pm of the day. On-the-crediting of remittance for responses beyond 04:00pm shall be left to the discretion of the TOD.

7.1.2 Buyers of Cashier, Manager, Certified or Gift Check

A. Branch/business units may sell gift's, manager's or certified checks only to its existing customers and shall maintain a register of said checks indicating the following information:

1. True and full name of the buyer or the applicant if buying on behalf of an entity;
2. Account number;
3. Date of issuance;
4. MC number;
5. Name of the payee;
6. Amount;
7. Date Paid/cancelled;
8. Purpose of such transaction; and
9. Remarks.

B. Buyers of Gift's, Manager's or checks in blank or payable to cash, bearer or numbered account. A branch/unit may issue gift/manager's checks in blank or payable to cash, bearer or numbered account subject to the following conditions:

1. The amount of each check shall not exceed P10,000;
2. The buyer of the check is properly identified in accordance with the customer acceptance and identification policies;
3. Required information were indicated in the MC/GC register;
4. The Branch/unit which accepts as deposits, said cashier's, manager's, certified or gift checks or similar instruments issued in blank or payable to cash, bearer or numbered account shall conduct transaction enhanced due diligence (TEDD) to ensure that said instruments are not being used / resorted to by the buyer or depositor in furtherance of a money laundering activity;
5. The deposit of said instruments shall be subject to the same requirements of scrutiny applicable to cash deposits; and
6. Transactions involving said instruments should be accordingly reported to the AMLC if there is reasonable ground to suspect that said transactions are being used to launder funds of illegitimate origin.

C. In the event the payee of the purchased manager's check is not an accountholder of the bank, the branch/unit must screen the payee against the bank's watchlist. The results of the watchlist screening shall form part of the transaction documents. This shall be done regardless of the amount of the manager's check.

7.1.3 Second-endorsed Checks

Stricter guidelines in the acceptance of second-endorsed checks including the application of enhanced due diligence to ensure that they are not being used as instruments for money laundering or illegal activities.

Acceptance of second-endorsed checks are limited from properly identified customers and only after establishing that the nature of the business of said customer justifies, or at least makes practical, the deposit of second-endorsed check. In case of isolated transactions involving deposits of second-endorsed check by customer who are not engaged in trade or business, the true and full identity of the first endorser shall be established and the record of the identification shall also be kept for five (5) years.

7.1.4 Money Service Business (MSBs)

A. The branch/unit shall require the clients who are MSBs (*i.e. foreign exchange dealers/money changers/ remittance agents and transfer companies*) to submit proof of registration with the Bangko Sentral ng Pilipinas (BSP) as part of their customer identification document, and shall only deal with these entities if they are duly registered as such. Also, these clients shall be required to use company accounts for their remitting, foreign exchange dealing and money changing business.

   Remittance and transfer companies, foreign exchange dealers and money changers presenting greater risk shall be subject to enhanced due diligence, which includes, among others, requiring proof of registration with the AMLC, reviewing and assessing their AML/CFT program or MTPP to have reasonable assurance on their AML compliance, obtaining additional information and securing senior management approval for establishing business relationship.

B. Know-Your-Customer's Customer (KYCC) Policy on MSB Transactions.

   Transactions of money service business (*i.e. remittance company/agent, foreign exchange company/money changer*) executed in behalf or for the benefit of their own clients (who are not a CBS client) shall be subject to the KYCC policy. In assessing whether KYCC shall apply, the transaction must be: (1) executed/performed by the MSB in behalf of its own client; and (2) the account of the MSB with the Bank will be used to execute such transaction. Thus, KYCC shall be applicable to outward remittance (*domestic or cross-border*) or fund transfer out executed by the MSB, through its account with CBS, where there is an originator other than the MSB.

   If the MSB represented that there is no other originator, the Authorized Personnel shall look at the purpose and details of beneficiary in the application for outward remittance or fund transfer out. If such purpose or beneficiary has obviously no logical relationship with the business of the MSB (*e.g. the beneficiary is an individual or non-financial institution*), then this is proof-positive that the transaction is executed in behalf of another originator.

   This determination is required at the point of transaction. Should the client refuse to provide the true originator's information or other reliable proof that the transaction has no other originator, the Authorized Personnel of the processing branch/unit shall deny such transaction.

   KYCC shall not apply if the client of the MSB is also a customer of the Bank. However, the Authorized Officer of the branch/unit shall assess the reason of the customer in performing the transaction thru the MSB instead of directly executing the transaction in the customer's name using his/her own account.

C. Due Diligence Standards for MSB Transactions

   The following shall be observed for MSB transactions:

1. The Authorized Personnel of the branch/unit shall conduct screening of the true originator (other than the MSB) and the beneficiary of the transaction thru the Watchlist database in the Base60 AML System. Should either the true originator/remitter or beneficiary is a positive match with any of the sanctions list (*i.e. OFAC, UN, EU, HMT*), the transaction shall be denied and an STR shall be filed.

2. The MSB shall be required to provide the minimum information of their own client to the Bank whenever such transaction qualified under section 7.1.4B above. Such minimum information can be provided either via the Customer Information Sheet (CIS) which is a form provided by the Bank or thru a copy of the existing application form of the MSB, provided that all minimum information required in the CIS are present.

3. The MSB ordering such transaction shall provide to the Bank a "Certification of Due Diligence", attesting the following:

    a. The gathering and validation of identification documents of their client, pursuant to BSP circular 706, as amended by BSP circulars 950 and 1022.

    b. Performing the following due diligence requirements pursuant to the above circular, to include: i) authentication of the source of funds or the true originator of the transaction (client of the MSB); ii) authentication of the purpose of the transaction, and that official documents are gathered supporting the existence, validity and legality of the transaction.

    c. The copy of the above documents will be presented to the Bank within three (3) banking days upon demand.

4. If the client of the MSB (*who is not a CBS client*) falls within the definition of a default High Risk customer type under section 6.8, the Authorized Personnel of the branch/unit shall perform separately an enhanced due diligence with full cooperation of the MSB. Whenever the Bank is unable to conduct fully its EDD responsibilities, no transaction shall be allowed for that particular high risk client of the MSB.

7.1.5 Real-time Transaction Monitoring Through Fraud Management System (FMS)

The bank is required by the Bangko Sentral ng Pilipinas (BSP) to implement automated and real-time fraud monitoring and detection systems to identify and block suspicious or fraudulent online transactions. The expected sophistication and capabilities of the bank's FMS should be commensurate to the risks associated with its digital financial and payment platforms. As fraud and cyber threats evolve, the bank's FMS must be constantly calibrated to be able to process surges in transactions, collectively analyze customer profiles/behavior, and detect new fraud patterns.

The bank may employ a combination of rule-based, machine-learning, and other technologies to ensure robustness of its FMS. Fraud rules and mechanisms to be adopted or integrated with the implementation of the FMS may include:

a. **Geolocation blocking –** the FMS may stop transactions outside the usual location or country or trigger enhanced due diligence procedures.
b. **Transaction velocity checks/thresholds –** the FMS should detect and/or block transactions with unusual velocity, such as multiple transactions which might be performed by automated bots or malware. Moreover, transaction limits may be assigned to financial accounts such as number of transfers per day, maximum transfers per account, etc.
c. **Changes in mobile device and account information controls –** the FMS should be able to detect and monitor changes in mobile device and account information. As an example, surges in new mobile registration of customers within a short timeframe might signal automated account takeover attacks. The bank may likewise automatically block transactions after change of device or account information within a certain timeframe (e.g. 24-hour cooling off period).
d. **Blocking of transactions from blacklisted merchants/sites –** the FMS may include rules to block transactions from known malicious sites and insecure merchants.

7.2 POST-TRANSACTION MONITORING CONTROLS

For transactions initiated by the client or another person for the account of the client, on-going monitoring includes end-of-day review of significant transactions, management of Alerts from the AML System and conduct of post-validation checking to establish that the transactions of the client are within the established profile.

7.2.1 Monitoring of Significant Activity

The Significant Activities Report (SAR) generated daily for individual and non-individual deposit customers whose debit and/or credit transactions sum up to at least P100,000.00 for the day for Branches. Apart from marketing and cross-selling purposes, the report shall also be used in determining unusually large transactions on the account which may lead to further review or investigation.

The following process shall be performed in the daily review of the SAR:

1. The Report shall be reviewed independently by the Business Manager, Branch Service Head and Branch Operations Head on a daily basis. In the day-to-day review of the report, the Authorized Personnel reviewing the report shall, at a minimum, take note of: (a) sudden unusually large credit to the account; (b) frequent credits of Php500,000 or less; (c) large amount credit and the same (or almost the same) amount is debited to the account on the same day; and (d) any other unusual or inconsistent transaction considering the profile and transaction history of the customer.

2. If necessary, further review of the account which may include review of reports of previous transactions or review of the account movements via the system, to determine if the same transaction occurred in the past and to establish a pattern of account activity.

3. To indicate that review has been performed, the Authorized Officers shall affix his/her signature on each page of the Report. A check mark shall also be provided in the credits and debits of each client in the report to signify review. A distinct mark shall be indicated beside the debit or credit value that

was subjected to further review/validation (*e.g. TEDD*), and a brief description as to the additional information gathered and result of the review, or the reference to the documentation of the review shall be written in the page of the SAR.

Other units shall have their own monitoring of activities that are significant to them, considering the usual amounts of transactions and volume processed per customer.

7.2.2 The Base60 AML System

The Base60 as referred in this MTPP is a browser-based system that can be accessed thru the corporate intranet. It is a complete end-to-end AML solution, sophisticated, risk-based monitoring and alert system that detect the subtle patterns that could indicate suspicious behavior.

The two (2) main purposes of the Base60 are: a) to facilitate the Bank's compliance with the reportorial requirements imposed by the AMLC; and b) serve as a tool of the Bank in monitoring the transactions of its customers.

7.2.3 Transaction Monitoring Function of Base60

Base60 AML system monitors the transactions of the Bank's customer by capturing transactions that qualify the Alert scenarios set-up in the system. There are four (4) general types of Alerts provided in the Base60, namely:

1. KYC Screening
2. High Risk and Transaction Screening
3. Possible Unusual Activities
4. Unusually Significant Transactions

The transactions alerted by the Base60 are required to be investigated for appropriate disposition and approval. With the implementation of the version 5.1 of Base60, 1 to 6 of the Alerts above are now being managed directly by the Compliance Division, whereas, the rest of the alerts are still being managed by the branch/unit.

7.2.4 Alerts

An Alert generated by the Base60 AML system serves as an early indicator to potential money laundering activities, as they represent possible exceptions to what is defined as "normal" transaction behavior. Alerts are classified into:

1. KYC Alert – alert generated by the KYC screening scenario. It pertains to customers flagged as a possible match with any of the sanctioned individuals or entities (*i.e. OFAC, UN, EU, HMT*), designated terrorists by the Anti-Terrorism Council (ATC), PEP, or with the bank's internal watchlist. This alert is examined by comparing the profile of the customer against the profile of the watchlist person.

Determine if there is a "name match", "potential target match", or "target match". If there is a positive match on the Sanctions Lists or the ATC List of Designated Persons, immediately cause the termination of business relationship, and file the suspicious transaction report (STR).

2. Transaction Alert – alert generated from the transaction scenarios (*items 2 to 4 of section 7.2.3 above*). This alert pertains to a transaction or series of transactions that met the specific transaction parameters or thresholds set-up in the system. This alert is examined by understanding the profile of the customer and assessing if the alerted transactions are "within the normal course of business" as provided in the customer profile.

7.2.5 Participants in the Alert Management

1. Branch/Unit Approver – handles the initial review and investigation within five (5) banking days from the date of alert generation or re-assignment date. See **Annex AF** for the Alerts Management Guidelines for Branches and Business Units.

2. Compliance Investigator – handles the review, investigation, re-assignment and disposition of alerts within eight (8) banking days from the date of alert generation or completion of the Branch/Unit. AML Compliance Investigator is an officer of the AML Compliance Department in-charge of alert management. See **Annex AG** for the Alerts Management Guidelines for Compliance Investigators and Approvers.

3. Compliance Approver – review and approve (or reject) the recommended disposition of the Compliance Investigator within ten (10) banking days from the alert is submitted for approval. A Compliance Approver is an officer of the AML Compliance Department in-charge of alert approval and monitoring. **See Annex AG** for the Alerts Management Guidelines for Compliance Investigators and Approvers.

4. Compliance Final Approver – review and approve (or reject) the alerts recommended for "Report as STR" disposition within one (1) banking day from the alert is submitted for final approval.

7.2.6 Disposition of Alerts

At the end of the assessment, the investigator shall recommend disposition of an alert. The result of the assessment, as well as the answers in the screening questions shall provide basis as to the type of disposition to be selected.

1. Clean – disposition is selected when the assessment of the transactions on the alert being reviewed is at least satisfactory or there is consistency between the profile and the transaction (*for transaction alerts*) or the KYC alerts is a negative match.

2. False Positive – disposition is selected when the assessment of the transaction is very satisfactory, and the result of such assessment can be applied to future alerts of similar type for a period of up to ninety (90) days, depending on assessment.

As there is subsequent suppression of similar alerts, this type of disposition shall only be used to regular or recurring transactions that are established, beyond satisfaction, to be consistent with the profile of the customer.

Regardless of the regularity of the alerted transactions, False Positive shall not be used to any of the following:

a. First time alerts (customers with no Alert History)
b. Alerts pertaining to customers classified as High Risk
c. Alerts pertaining to PEP customers
d. Alerts pertaining to customers with previously filed STR or subject of negative news report
e. Alerts pertaining to customers with previous AMLC Inquiry or Freeze Order
f. Alerts pertaining to Unusually Large Transaction that is either cross-border inward or outward remittance
g. Other similar instances where False Positive disposition may not be warranted (*e.g. corporate designated authorized signatory/ies tagged as "High Risk" in risk profiling*)

3. Report as STR – disposition is selected when the unresolved inconsistencies on the alert managed qualified in the criteria for suspicious transaction. Upon disposition, a brief narrative shall be provided in the "Remarks" portion. This narrative should be the brief summary of the Report on Incident of Suspicious Activity (RISA) filed. See **Annex R** for the Guidelines in Writing a High Quality Report on Incident of Suspicious Activity (RISA) Narrative.

7.2.7 Whitelisting of Alerts

What is a Whitelist?
A whitelist is a list of clients whose identities are well-established and whose transactions are known to be legitimate. A whitelisted client passed all the conditions provided for in the Bank's policy on whitelisting.

What will happen if a client is "whitelisted"?
Transactions of clients included in the white list will no longer trigger an AML or transactional alert in the AML system. However, the whitelist is not permanent list, for it is subject to review and renewal annually. Thus, the list can change. Further, a whitelisted customer can be dropped/delisted at any time once the conditions are present.

Please refer to **Annex AH** for the Guidelines on Whitelisting of Clients from Alerts Generation and **Annex AI** for the Whitelisting Request Form.

7.2.8 Alert Justification

Alert justification shall contain the rationale for the selected disposition. The statement shall include reference to the due diligence performed, supporting documents, and the results of the review.

The justification should be the supporting statement for the selected justification.

7.2.9 Role of Bank Units on AML Monitoring and Reporting

Person Responsible	Roles & Responsibilities	Deadline
Service Associates or its equivalent for HO units	Investigate the alerts and provide disposition as Investigating Officer	Within five (5) banking days from the date of alert generation or date of re-assignment in case of re-assigned alerts
Branch Service Heads or its equivalent for HO units	Review and approve the alerts recommended disposition: Clean and False Positive	
	Submit photocopies/scanned copies of required documents pertaining to Suspicious Transaction	Upon submission of the Report on Incident of Suspicious Activity (RISA); included as attachment
Reserve Team Lead, Quality Assurance Officers and Assistant Quality Assurance or its equivalent for HO units	Ensure that all alerts are properly investigated and timely dispositions are done in the Base60 AML System by the Investigating Officer	Within five (5) banking days from the date of alert generation or date of re-assignment in case of re-assigned alerts
	Endorse all alert disposition that warrants a suspicious transaction reporting	

7.2.10 Role of Bank Units on Accuracy and Completeness of CTR Reports

Person Responsible	Responsibilities
Branch Service Heads / Designated Unit Compliance Coordinators (UCCs) or its equivalent for HO units	Review accuracy of customer information details encoded by Service Associates in the CIF against the accomplished CIS and Signature Card of the client

7.3 MONITORING OF NEGATIVE NEWS REPORT AND UPDATING OF WATCHLISTS

7.3.1 **Daily Monitoring Function.** The Authorized Personnel of the AML Compliance Department shall monitor negative news reports sourced from reputable online or printed source on a daily basis. The news search will focus on news articles pertaining to money laundering or offenses related to any of the thirty-six (36) unlawful activities or predicate crimes (*see number 34 of Part II Definition of Terms*). As a minimum, the following source shall include:

1. At least two (2) major newspaper of general circulation or its online counterpart

2. Website of the following law-enforcement and other relevant government agencies:

    a. Philippine National Police (PNP) – www.pnp.gov.ph
    b. National Bureau of Investigation (NBI) – www.nbi.gov.ph
    c. Philippine Drug Enforcement Agency (PDEA) – www.pdea.gov.ph
    d. Bangko Sentral ng Pilipinas (BSP) – www.bsp.gov.ph

e. Anti-Money Laundering Council (AMLC) – www.amlc.gov.ph
f. Securities and Exchange Commission (SEC) – www.sec.gov.ph
g. Department of Justice (DOJ) – www.doj.gov.ph
h. Office of the Ombudsman – www.ombudsman.gov.ph
i. Department of Interior and Local Government (DILG) – www.dilg.gov.ph

3. Website of at least two (2) major TV network channels

Other sources may be used as supplement for gathering of additional information pertaining to the subject of negative news. In addition, the branches shall also provide inputs with a larger focus on local news.

7.3.2 **Processing of Negative News Gathered.** The following minimum procedures shall be followed by the Authorized Personnel of AML Compliance Department:

1. The Authorized Personnel of the AML Compliance Department or the branch personnel shall exercise all efforts to get as much information pertaining to the subject of the negative news report. As much as possible, the following information shall be included:

    a. Complete Name (*first, middle and last name or registered name of the entity/corporation*)
    b. Date of birth or registration (in case of entity/corporation)
    c. Current/Previous position (in case of government official)
    d. Date of publication of the article / date of knowledge
    e. Source of the negative news article
    f. Specifics/reference
    g. Negative news classification

2. The Authorized Personnel of the AML Compliance Department shall create an excel database to record the subject of the negative news report, and update this on a daily basis.

3. The name of the subject negative news report shall be electronically inquired in the Base60 AML System to find any possible match with existing bank clients.

4. In case there's a possible match, the AML Authorized Personnel shall direct the inquiry to the Compliance Coordinator of the branch/unit via email. The email shall include the name of the subject of negative news, the negative news article and instructions.

5. Upon receipt by the branch/unit compliance coordinators of the notice from AML Compliance Department, the branch/unit shall be required to conduct the following:

    a. Compare the overall profile of the customer against the available information provided in the negative news report and other information provided by AML Compliance Department, and provide confirmation if they are one in the same or not.

b. If the branch/unit customer is one in the same with the person/entity subject of negative news report, a review of the transaction shall be conducted to see any unusual amounts or movements to the account.

Regardless of the result of the review, the ECRAF shall be amended to reflect the inclusion of the customer in the negative news. The positive "suspicious indicator" in the ECRAF will be selected for the high risk classification of the account. Consequently, the branch/unit authorized officer shall conduct transaction enhanced due diligence (TEDD) on the account on the transactions and shall tag the customer as HIGH RISK in the FCBS/Source system.

c. Whether or not the customer is a positive match with subject of negative news report, the branch/unit Authorized Personnel shall provide a formal response via email detailing the results of determination of positive/negative match, and the results the TEDD (if required).

d. Such email response shall be provided to the Authorized Personnel of the AML Compliance Department within three (3) banking days from the date emailed by the AML Compliance Department.

7.3.3 **Database of Persons with Negative News.** All names provided in the negative news report shall be consolidated in an excel file, and shall be loaded in the internal watchlist database maintained in the Base60 AML System. The updating of the database shall be done every end-of-month. Upon updating of the internal watchlist, a scan shall be performed on the customer database maintained in the Base60 AML System, either within or outside the system to ensure that any possible match on newly opened accounts after initial screening by the AML Compliance Department up to the date of loading from the Internal Watchlist will be detected and acted upon in accordance with the above procedures. Uploading of the names of the persons subject to negative news in the internal watchlist shall be approved at least by the AML Compliance Department Head. Deletion from the internal watchlist also requires approval of at least the AML Compliance Department Head.

7.4 GUIDELINES ON NEGATIVE NEWS REPORTING (BOTTOM-UP APPROACH)

For the Bank to be more effective in its fight against money laundering and terrorist financing, a more appropriate approach in updating the watchlist database shall be implemented branch-wide. Part of the process improvement is the bottom-up approach on negative news reporting.

This new approach, through the coordination of AML Compliance Department and the branches, shall allow the Bank to cover personalities not usually mentioned in the national level. The combination of scouting through local and national news will allow the Bank to further improve the coverage of its watchlisting capability on adverse/negative news reporting.

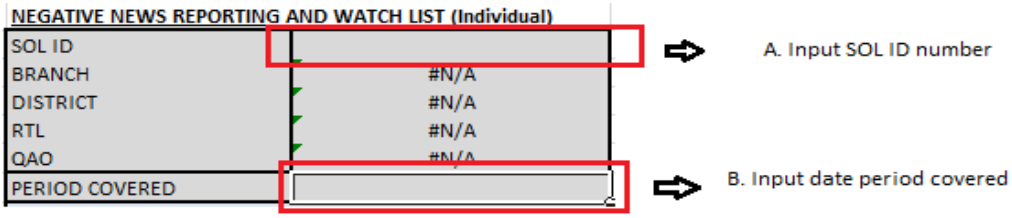
Respective QAOs and RTLs per district will assist to gather the negative news reports within their respective jurisdictions. This is vital in order to serve better its purpose in expanding the negative news reporting coverage in relation to the customer due diligence (CDD) process of the branch.

7.4.1 Data Inputs in the Template

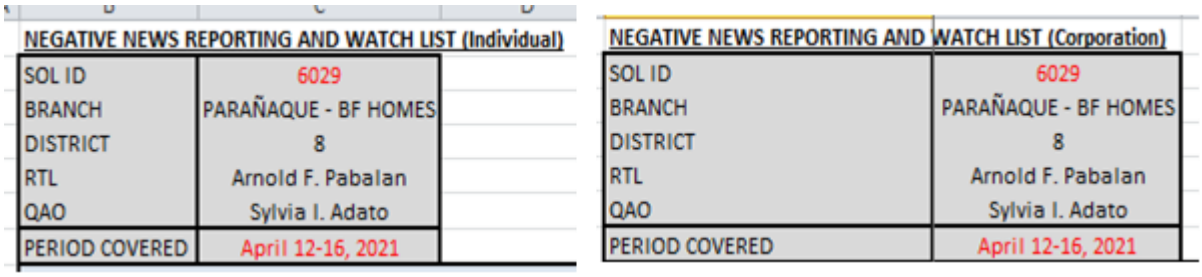
Excel file/s should contain the following information in table given below. Date of birth/Date of Registration should be provided if the branch can exhaust the information or can be left blank if not sited or is not readily available.

1. The only two active worksheets that the branch shall work on are 'Individual' and 'Corporation'.

    a. The branch to open worksheet 'Individual' and only indicate the SOL and it will provide the information needed both in Individual and Corporation worksheets.
    b. Input the date period covered and it will auto-populate in the other worksheet.



Once SOL ID and date period covered are encoded, it will fill details as such, and so with the other worksheet.



NEGATIVE NEWS REPORTING AND WATCH LIST (Individual)

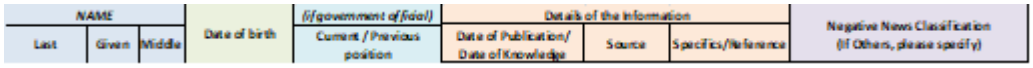
SOL ID	6029
BRANCH	PARAÑAQUE - BF HOMES
DISTRICT	8
RTL	Arnold F. Pabalan
QAO	Sylvia I. Adato
PERIOD COVERED	April 12-16, 2021

NEGATIVE NEWS REPORTING AND WATCH LIST (Corporation)

SOL ID	6029
BRANCH	PARAÑAQUE - BF HOMES
DISTRICT	8
RTL	Arnold F. Pabalan
QAO	Sylvia I. Adato
PERIOD COVERED	April 12-16, 2021

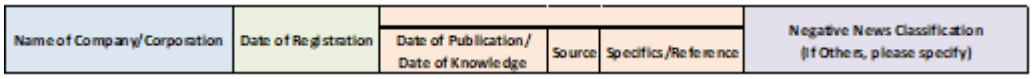
2. After the branch has identified the (local) news, it must have the following details captured:

Individual



NAME			Date of birth	(if government official)	Details of the Information			Negative News Classification
Last	Given	Middle		Current / Previous position	Date of Publication/ Date of Knowledge	Source	Specifics/Reference	(If Others, please specify)

Corporation

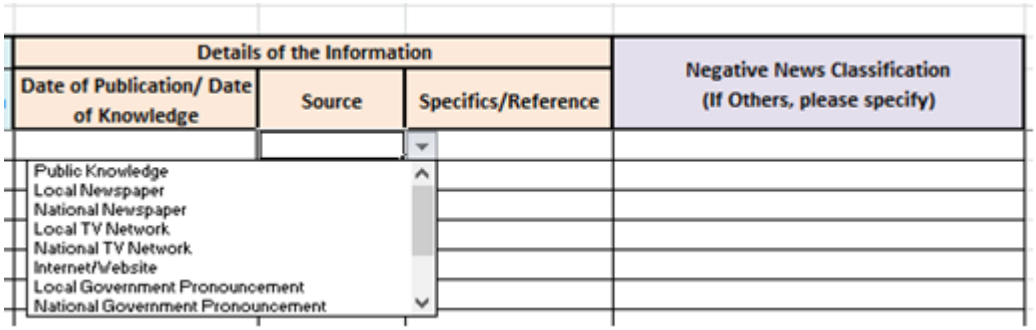


Name of Company/Corporation	Date of Registration	Date of Publication/ Date of Knowledge	Source	Specifics/Reference	Negative News Classification (If Others, please specify)

For any information of the particular negative news that cannot be gathered (i.e, birth date), we may leave it blank. The primary information needed are the name of individual or corporation concerned, the source of news (date of publication/knowledge), and the classification of negative news.

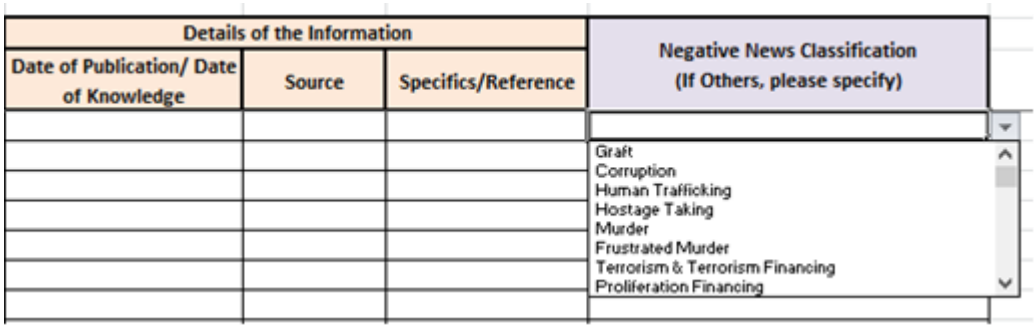
'Source' has a dropdown list to categorize the classification of the news. This applies to both 'Individual' and 'Corporate' sheets. Public knowledge can be another term for 'grapevine'. Some areas or jurisdictions may have high profile individuals that are not highly publicized. Hence, the possibility of an individual or entity having a bad record in an area, but a clean slate on a neighboring town/city.

Source:



'Negative News Classification' has a dropdown list to categorize the classification of the news. This also applies to both 'Individual' and 'Corporate' sheets.

Classification:



In the event that there will be none to report by the branch, their respective RTLs and QAOs should indicate and still submit a report, indicating 'NONE TO REPORT' for compliance monitoring purposes.

7.4.2 Classification of Negative News

Classification of Negative News are chosen via dropdown menu in the template. In the event the classification is not in the choices, "Others" can be selected. The branch personnel shall then state the classification for the particular entry.

Below are the negative news classifications to be chosen in the template:

Negative News Classification			
Graft	Plunder	Malversation of Funds	Hijacking
Corruption	Extortion	Fraud & Estafa	Counterfeit
Human Trafficking	Escaped Convict	Rape	Bribery
Hostage Taking	Illegal Gambling	Illegal Recruitment	Piracy
Murder	Vandalism	Sexual Exploitation	Forgery
Frustrated Murder	Carnapping	Theft and Burglary	Illegal Exactions and Transactions
Terrorism & Terrorism Financing	Kidnapping	Lible & Cyber Libel	Felony
Proliferation Financing	Assault & Physical Violence	Falsification of Public Documents	Child Exploitation
Illegal Possession of Firearms	Obstruction of Justice	Swindling	Robbery
Tax Evasion	Drug Trafficking	Smuggling	Others

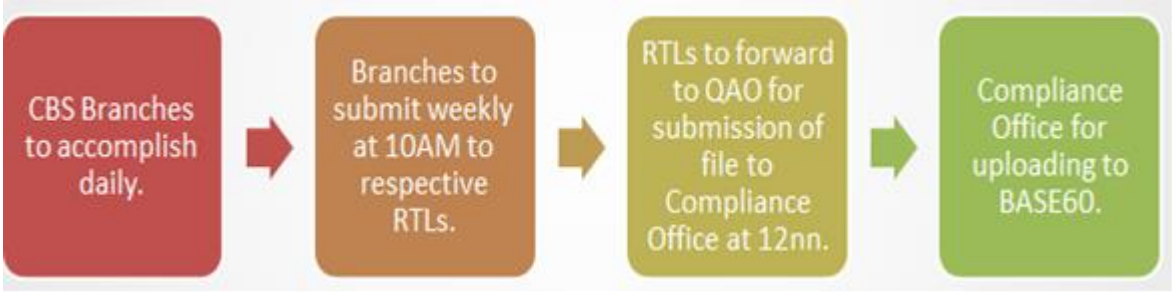
7.4.3 Sources of Negative News

As the bank will be implementing the "bottom-up" approach in its negative news reporting, the primary source of the branches will be local news. There are various sources for local news per region that may be not of reach for other CBS Branches. Each branch will have to source negative information per their local news network and news print. News print is published newspapers which are accessible also through the internet.

7.4.4 Reporting Process

Negative News Reports will be accomplished daily by the branches both for Individual and Corporation subject to adverse and derogatory news reports. Fully accomplished NNR templates shall be submitted weekly, every Friday, to their respective RTLs for consolidation.

The report will be consolidated by the RTLs, and will submit the same to their QAOs, every Friday morning at 10:00AM for consolidation.



7.5 INTERNAL WATCHLIST MONITORING

The internal watchlist database of the Bank shall include the following:

a. Customers with filed Suspicious Transaction Report (STR) which are the subject of suspicion.

b. Customers with filed Reports on Crimes and Losses (RCL) which are the perpetrators.

c. Employees of the Bank with filed Reports on Crimes and Losses (RCL) which are the perpetrators.

d. Persons captured in the negative news monitoring of the AML Compliance Department.

e. Persons reported in the news and/or news articles to have been identified with involvement in any of the thirty-four (34) predicate crimes of AMLA as determined and approved by the Chief Compliance Officer or its designated alternate. Except for reasons relating to negative credit standing/issues, positive match in any of the above internal watchlist shall warrant at least the tagging of a customer as HIGH RISK (*included as suspicious indicator in ECRAF*). Thus, enhanced due diligence is required.

7.6 SANCTIONS LISTS MONITORING

Contains listing of individuals or entities sanctioned by governments or international organizations due to their involvement in unlawful activities. The following sanctions list is currently maintained in the Base60 AML System:

1. OFAC – listing published by the Office of Foreign Assets Control of the U.S. Department of Treasury, collectively known as Specially Designated Nationals (SDNs). These SDNs included individuals and companies owned or controlled by acting for or on behalf of the targeted countries. It also includes individuals, groups, or entities, such as terrorist and narcotics traffickers designated under programs that are not country specific.

2. UN – listing provided by the United Nations consisting of individuals, groups and corporations listed as members or associated to Al Qaida, Taliban or other terrorist groups.

3. EU – contains the consolidated listing of persons, groups and entities subject to Common Foreign and Security Policy (CFSP) related financial sanctions imposed by the European Union.

4. HMT – contains a consolidated listing of asset freeze targets and list of persons subject to restrictive measures in view of Russia's actions destabilizing the situation in Ukraine. This is provided by the Office of Financial Sanctions Implementation of the United Kingdom related to financial sanctions imposed by Her Majesty's Treasury.

Screening against the customer database in the Base60 shall be performed to ensure that no accounts of persons in the sanctions list were opened up to the date of updating of the Sanctions List.

7.7 TRANSACTION ENHANCED DUE DILIGENCE (TEDD)

7.7.1 **What is TEDD.** The TEDD is a series of due diligence procedure required for transactions that are considered high risk in an AML/CFT perspective. Whenever the regulation or any provisions of this MTPP requires enhanced due diligence on a particular transaction, the TEDD procedures herein shall apply.

TEDD requires the gathering of additional information and/or documents in order to provide a more informed assessment of a particular transaction of the customer. TEDD requires the following:

1. Gathering of transaction party details which include the originator, beneficiary, other parties, the accounts, and nature of participation of the other parties, if applicable.

2. Gathering the transaction details or Alert details (*if TEDD is a result of management of Alerts*).

3. Gathering of additional information and/or documents supporting the transaction under review, if applicable.

4. Due diligence details, this is the assessment portion of the TEDD process. Here the Authorized Personnel answers specific due diligence questions pertaining to the transaction. The answers to the questions will be the guiding information for the Authorized Personnel to come up with the appropriate recommendation.

5. Based on the assessment, the recommendation may be any of the following:

    a. Do not execute the transaction and file STR
    b. Do not execute the transaction due to non-AML/CFT issues
    c. Execute the transaction. With minor non-AMLCFT issues noted
    d. Execute the transaction. No AML/CFT issues noted
    e. Clear the Alerted Transaction
    f. Report as STR the Alerted Transaction
    g. Re-classify the customer to High Risk
    h. Terminate the business relationship with the client

The above procedures, additional documents/information, assessment and recommendation shall be documented in the TEDD Form – See **Annex AJ**. For the TEDD Form Instruction Manual, see **Annex AK**.

7.7.2 **When to Conduct TEDD.** As a general rule, whenever enhanced due diligence for a particular transaction is required under this MTPP, the TEDD policy shall be applied, and on a per transaction basis. However, so as not to render continuous inconvenience both to the customer and branch/unit, TEDD under the following circumstances may be conducted **only once**:

1. When the series of transaction pertains to payment of contractual obligation (*e.g. for service or product*) where the payment schedule and the amount of periodic payments is stated in the official contract, provided that the source of funding for the payments are established on the first TEDD, and such official contract is on-hand.

2. The series of transaction pertains to loan and related payments to a registered financial institution, where the official loan contract is provided and the source of payment was established in the initial TEDD performed.

3. The recurring transaction is for the pursuance of its primary business purpose, provided that normal transaction level (*both in value and volume*) shall be established by the Branch/Unit Authorized Personnel pertaining to the customer. Whenever there's unusual increase in either value or volume, as observed by the Authorized Personnel, a subsequent TEDD shall be performed for the unusual increase.

4. The beneficiary of the transaction is a registered Domestic Bank.

5. The transaction of the customer has the same nature and purpose with the previous transaction initially subjected to TEDD, provided that official documents supporting the nature, purpose and source of funds of the transaction has been established in the initial TEDD performed.

Regardless of the above or the similarity of the details of the previous and subsequent transactions, TEDD for each **cross-border** outward remittance shall be required whenever the country of destination is among the list of High Risk Countries/Jurisdictions – **See Annex P** for Outward Remittance.

Unless otherwise covered by the exempted transactions under 7.2.2, TEDD shall be conducted if an MC Purchase transaction for an Individual is at least PHP 1,500,000; and PHP 10,000,000 for corporate. The threshold will be reviewed and adjusted, when necessary. In addition, buy or sell of foreign currency amounting to at least USD 400,000 or its equivalent in other currency. TEDD shall likewise be done upon the branch/unit's notice of red flags which may pertain to unlawful activities.

7.7.3 **Minimum Approval for TEDD.** Matrix of Approval for TEDD performed based on the following transaction amounts:

BANK TRANSACTIONS (EXCLUDING CROSS-BORDER OUTWARD REMITTANCE TRANSACTION)		
For Foreign Currency Denominated	**Approving Authority:**	
	Branches	**Other Units***
Up to Php500,000 or its third currency equivalent	Endorsed by Branch Service Head (BSH) and approved by Division Head	Division Head
More than Php500,000 to Php1,000,000 or its third currency equivalent	Endorsed by Branch Service Head (BSH) and approved by Division Head	Division Head
More than Php1,000,000 or its third currency equivalent	Endorsed by Branch Service Head (BSH), recommended by Division Head, and approved by Group Head	Group Head
Positive match in internal watchlist (other than "FO" and "PDEAPNP") or the customer is a subject of recent negative news pertaining to money laundering	Endorsed by Branch Service Head (BSH), recommended by Division Head, and approved by Group Head	Group Head

or unlawful activity, **regardless of amount**.		

*Minimum requirement for Head Office Units

The above approval requirement applies only to the TEDD performed by the Branch/Unit. The above shall not affect the existing approval requirements for processing outward remittance transaction.

7.8 UPDATING OF CUSTOMER RECORDS

The frequency of updating of customer records shall be based on the latest risk classification of customer. Accordingly:

Latest Customer Risk Profile	When to Update
Low Risk	Every 3 years
Normal Risk	Every 2 years
High Risk	Every year

However, if material information is present that warrants the updating, the records and due diligence of the customer shall be updated immediately.

At the minimum, the following documents shall be updated:

1. Customer Information Sheet (CIS)
2. Identification Documents, if expired already
3. Customer Risk Assessment (using the ECRAF)
4. UBO Determination Form
5. Documents required for High Risk customers (depending on the requirement for each high risk customer type)

For purposes of this section, material information warranting immediate updating shall include, but not limited to any of the following:

1. Change in customer type/classification
2. Recent suspicious transaction report pertaining to the customer
3. Recent inclusion in the negative news of the customer
4. Recent AMLC Inquiry or Freeze Order on the customer
5. Recent inclusion in the internal watchlist (*except for negative credit information*)
6. Presence of Suspicious Indicator (*as described in **Part G** of the ECRAF Implementing Guidelines V2.3*) that does not warrant immediate termination of the business relationship

PART VIII
SANCTIONS PROGRAM AND TARGETED FINANCIAL SANCTIONS

PART VIII: SANCTIONS PROGRAM AND TARGETED FINANCIAL SANCTIONS

This policy sets principles and standards of managing money laundering risk, countering terrorist/proliferation financing and sanctions breaches. It also governs the Bank's controls and mechanisms in combating terrorist financing and proliferation financing which are made consistent and in line with the country's laws on terrorism and its related offenses.

8.1 SCOPE AND APPLICATION

This policy shall apply to all China Bank Savings Inc.'s branches and business units. This policy establishes the minimum expectations in handling sanctions screening and review of transactions that can be potentially used for terrorism financing, and pursuance of terrorism and proliferation activities.

8.1.1 The Bank, including its directors, officers and employees, shall not associate itself with any individual or entity that is sanctioned under the United Nations Security Council (UNSC), US Department of Treasury's Office of Foreign Assets Control (OFAC), European Union (EU), Her Majesty's Treasury (HMT), Philippine Anti-Money Laundering Council (AMLC) and the Philippine Anti-Terrorism Council (ATC).

8.1.2 The Bank shall not allow its products, services and business relationship with other financial institution be used for any activities to aide money laundering, terrorism financing and pursuance of terrorist and proliferation activities.

8.1.3 The Bank, through its Compliance Division, shall maintain a database or accessible source of sanctioned individuals, entities and jurisdictions to be used for sanctions inquiry, which database shall be updated from time to time.

8.1.4 Each Branch/Unit shall have its designated Sanctions Officer who shall oversee that the sanction screening requirement is complied with in on-boarding, updating of customer records and transactions requiring such screening. The Sanctions Officer shall be as follows:

a. Branches – Branch Service Head and Branch Operations Head
b. Business Units – Officer conducting the customer or transaction due diligence and officer approving the customer or transaction due diligence.

The Sanctions Officer shall be responsible for ensuring that the sanction screening required under their respective functions are complied with.

8.1.5 Sanctions Expert from the AML Compliance Department – shall be designated to resolve all inquiries pertaining to the sanctions program whenever such is required or necessary to be elevated for an independent opinion. For this purpose, the AML Compliance Department Head, Policy and Training Officer, and the Alert Management Team Leader are designated as Sanctions Experts.

8.2 SANCTIONS CATEGORY

a. **Targeted Sanctions** – aimed at specifically named entities or individuals such as key leaders in a country or territory, named terrorists, significant narcotics traffickers and proliferators of weapons of mass destruction. Imposed sanctions under this category may include freezing of assets and travel bans.

b. **Sectoral Sanctions** – aimed at key sectors of an economy to prohibit a very specific subset of financial dealings within those sectors to impede future growth.

c. **Comprehensive Sanctions** – generally prohibit all direct or indirect import/export, trade, brokering, financing or facilitating against most goods, technology and services. These are often aimed at regimes responsible for gross human rights violations and nuclear proliferation.

8.3 SANCTIONS SCREENING

For purposes of this policy, sanctions screening shall be classified into:

a. **Name Screening** – involves matching of names with the names in the Targeted Sanctions database or source, the UNSC Consolidated List, or those designated by the ATC. This includes name screening of individuals, entities, and vessels.

b. **Transaction Screening** – involves determination of applicability of Sectoral or Comprehensive Sanctions on a transaction, including its underlying purpose, goods/services, and involved countries.

8.4 TARGETED TRANSACTIONS

8.4.1 **Customer On-boarding** – requires name screening of the following upon on-boarding regardless of risk classification:

a. Customer name
b. Beneficiary/Ultimate Beneficial Owner
c. Authorized Representatives/Signatories/Attorney-in-fact
d. Directors and Principal Officers

For foreign entities or domestic entities with foreign operation or dealings, the following shall also be determined for sanctions purposes:

a. Foreign country of operation – for sectoral and comprehensive sanctions review
b. Foreign countries where they buy or sell to – for country name screening and comprehensive sanctions review
c. The goods the company deal with and their potential dual-use – for sectoral sanctions review
d. Foreign counter-parties – for sectoral and comprehensive sanction review

8.4.2 **Subsequent to On-boarding** – name screening on a daily basis of the customers. Subsequent name screening of directors and principal officers shall be performed during updating of customer records.

8.4.3 **Occasional Financial Activity**[4] – name screening of the non-client individual transactor/beneficiary prior to the processing of transaction.

8.4.4 **Cross-border Outward Remittance** – name screening for targeted sanctions. The parties to be included for screening shall at least include the remitter, true remitter (if any), beneficiary, ultimate beneficiary (if any), third parties to the transaction, and beneficiary bank including other financial institutions involved. If the underlying transaction involves goods, screening applicable to Trade Transactions below shall apply. If the purpose involves provision of service, sanctions review shall be performed for sectoral and comprehensive sanctions purposes.

8.4.5 **Cross-border Inward Remittance** – name screening for targeted sanctions of remittances reaching or above the established thresholds or those with identified red-flags. The parties to be included shall at least include the remitter, beneficiary, ultimate beneficiary (if any), third-parties to the transaction, and remitting bank, including other financial institutions involved. If the underlying transaction involves goods, screening applicable to Trade Transactions below shall be followed, as applicable.

8.4.6 **Trade Transactions** – screening shall be applied to the following:

a. Parties to the transaction, including third-parties – name screening for targeted sanctions
b. Goods – sanctions review for sectoral and comprehensive sanctions. The sanctions officer shall also determine if the goods can be dual-used.
c. Countries, including the port of loading, port of discharge, origin of goods, country of applicant, country of beneficiary – sanctions review for sectoral and comprehensive sanctions.
d. Financial Institutions involved in the transaction – name screening for targeted sanctions, and sanctions review for sectoral and comprehensive sanctions.
e. Vessels – name screening for targeted sanctions.

8.4.7 **Employee On-boarding** – as part of Know-Your-Employee (KYE) initiatives, name screening will be performed to new hires prior to their official on-boarding.

8.4.8 **Other Transactions** – as determined by the AML Committee.

8.5 SANCTIONS SCREENING RESULT

8.5.1 **Name Match** – when the name of an individual or entity matches with one or more entries on the consolidated list or other sanctions list. This requires further investigation to determine positive or negative match.

Existence of the name match shall be documented such as printing of the result of screening, if there are names appearing upon conduct of the name search.

[4] May include non-client transactions such as large cash deposit, check or MC encashment, remittance claim, buying/selling of foreign currency, and the like.

8.5.2 **Target Match** – there is a target match:

a. **Individuals** – if the first name, last name, aliases, nationality, date of birth and last known address matches all of the information on the consolidated list or sanctions lists. If there is no date of birth or other identifier information that cannot provide assurance the Authorized Personnel or Sanctions Officer on whether it is a target match or not, this is considered as a **Potential Target Match**

b. **Entity** – pertains to businesses in whatever form or type or ownership. There is a target match if the name of the business matched with all of the information on the consolidated list or sanctions lists.

c. **Vessels** – pertains to the name of the vessel and unique IMO number used to transport the goods. There is a positive match if the name of the vessel or aircraft matched with the sanctioned vessel or aircraft.

However, it is important to note that the vessel name can be subject to change to go around the sanction designation. Thus, if can reasonably be obtained, the unique identification code of the vessel (e.g. International Maritime Organization or IMO number) is an absolute identifier that can be used, regardless of the name of the vessel.

d. **Country** – the country can be searched in the list of designated countries (**see Annex P**) for any sectoral or comprehensive sanctions. The search will also include the port of loading, port of discharge, origin of goods, country of applicant, and country of remitter/beneficiary.

e. **Goods/Services** – The first layer requires review of the subject goods to determine if included in the list of dual used goods. Dual-Use Goods are items, software and technology, which can be used for both civil and military end use or in connection with the development, production, handling, operation, maintenance, storage, detection, identification or dissemination of weapons of mass destruction or their means of delivery (*RA 10697 – Strategic Trade Management Act of 2015*). The second layer requires review of the countries involved to ensure that there are no sanctions for the import and/or export of those goods/ services.

If the result of the investigation yields a positive match, the Sanctions officer shall print the screening result, prepare the Report on Incident of Suspicious Activity (RISA) and attach supporting documents for submission to the AML Compliance Department.

8.5.3 **Negative Match** – possible match that turned out to be negative due to mismatch in information.

8.6 INVESTIGATION AND ESCALATION

8.6.1 For Name Screening

a. Whenever a party a transaction is a target match/potential target match with any of the names in the UNSC sanctions list or those designated by the ATC, denial of business relationship and immediate freezing of accounts without delay (if existing client) is required. Immediate freezing shall also apply to funds held by the Bank where any of the parties to the transaction is a target match/potential target

match with the UNSC list or those designated by the ATC. Any of the Sanctions officers shall file a Report on Incident of Suspicious Transaction (RISA) along with the supporting documents to be forwarded to the AML Compliance Department within three (3) hours from the time of discovery or determination.

If freezing of account is required pursuant to Section 8 of AMLC Regulatory Issuance No. 4, the relevant details of the account or funds or assets subject to freeze shall also be forwarded to Legal Division within three (3) hours from the time of discovery or determination for the filing of the Freeze Order Return.

If the individual has a direct or indirect ownership with a corporate client of the Bank, the details of the account of the entity shall be included in the report for the review of AML Compliance Department. Should the investigation determine that the individual's transactions pass through the entity's account, it shall likewise be subject to STR filing and account freezing due to possible involvement.

b. Any of the Sanctions officers shall file a Report on Incident of Suspicious Transaction (RISA) along with the supporting documents to be forwarded to the AML Compliance Department within three (3) hours from the time of discovery or determination.

c. Submission of the Report on Incident of Suspicious Transaction (RISA) Form along with the supporting documents shall be done via email to all Alerts Management Officers, cc: AML Compliance Department Head, AML Compliance Officers, Business Manager, District Head, Region Head, Reserve Team Lead (or equivalent officers if filed by the Head Office Units)

d. Investigation by the Sanctions Experts and escalation to the AML Committee shall be performed to enable reporting as suspicious transaction within the next working day from the date of determination.

8.6.2 For Transaction Screening

a. Whenever the transaction or any country involved is possibly subject to Sectoral or Comprehensive sanction, the Sanctions Officer of the Branch or Unit shall conduct transaction enhanced due diligence (TEDD), and shall forward it along with the supporting information and documents to the Sanctions Expert for opinion/advise for proper disposition.

b. Transactions positively identified as subject to Sectoral or Comprehensive Sanctions shall be blocked immediately and filing of Report on Incident of Suspicious Transaction (RISA) Form along with the supporting documents to the AML Compliance Department shall be made within three (3) hours from determination.

8.7 POLICY ON TERRORIST FINANCING AND PROLIFERATION OF WEAPONS OF MASS DESTRUCTION

This policy governs the Bank's controls and mechanisms in combating terrorist financing and proliferation financing which are made consistent and in line with the country's laws on terrorism and its related offenses.

Terrorist Financing (TF) is among the general offenses covered under financial crimes. Republic Act No. 10168, otherwise known as the Terrorist Financing Prevention Suppression Act of 2012 (TF Law) that criminalizes and designates TF as a money laundering predicate offense.

In 2020, Republic Act 11479 otherwise known as the Anti-Terrorism Law of 2020 repealed and replaced the Human Security Act of 2007 as the country's primary law against terrorism.

On 14 October 2020, the Anti-Terrorism Council passed a resolution approving the Implementing Rules and Regulations (IRR) of the Anti-Terrorism Act of 2020. The IRR contains very detailed provisions on terrorism and terrorism-related crimes, on surveillance, on designation of terrorist individuals and organizations, on proscription, on the examination of bank accounts, among others.

Targeted Financial Sanctions are put in place by the United Nations and its Security Council, or by the Philippine Government to achieve a specific foreign policy or national security objective.

a. Targeted asset freezes: these apply to named individuals, entities and bodies, restricting access to funds and economic resources. Someone subject to an asset freeze will be listed on the Consolidated List or proscribed and posted under the AMLC or Anti-Terrorism Council (ATC) websites.

b. Prohibition against dealing: prohibits any person from (a) dealing, directly or indirectly, in any way and by any means, with any property or funds that he knows or has reasonable ground to believe is owned or controlled by a designated person, organization, association or group of persons, including funds derived or generated from property or funds owned or controlled, directly or indirectly, by a designated person, organization, association or group of persons; or (b) makes available any property or funds, or financial services or other related services to a designated person, organization, association or group of persons[5].

In 2012, AMLC issued AMLC Resolutions No. TF-01 and TF-02 which provided a standing court order for UNSCR 1267/1989 (Al Qaeda Sanctions List) and UNSCR 1988 (Taliban 1988 Sanctions List). This was later on repealed by AMLC Resolution No. 35 issued on February 16, 2021 which implements Targeted Financial Sanctions on Anti-Terrorism Council designations.

These AMLC Resolutions directed all covered persons and relevant agencies to freeze without delay the property or funds, including related accounts, of designated persons or entities. The freeze orders cover not only those listed at the time of the issuance of Resolution Nos. TF-01 and TF-02 but also those included in the ATC designations.

In 2014, AMLC likewise issued AMLC Resolution No. TF-03 relative to UNSCR No. 2170 which reiterated its condemnation of the Islamic State of Iraq and the Levant (ISIL), the Al Nusrah Front (ANF), all other individuals, groups, undertakings and entities associated with AL-Qaida. The individuals listed in the said resolution are also covered under AMLC Resolution No. TF-01.

Guidelines, policies, and procedures on terrorist financing under the 2020 Sanctions Guidelines and AMLC Regulatory Issuance No. 4, Series of 2020 have also been incorporated in this policy.

[5] 2021 Sanctions Guidelines

On 31 January 2021, the AMLC released Targeted Financial Sanctions related to Proliferation of Weapons of Mass Destruction and Proliferation Financing directing covered institutions to ex parte freeze, without delay, all funds and assets that are owned or controlled, directly or indirectly, including funds and assets derived or generated therefrom, by individuals or entities designated and listed under UNSC Resolution Nos. 1718 (concerning the Democratic People's Republic of Korea) and 2231 (concerning the Islamic Republic of Iran), and their successor resolutions, as well as any binding resolution of the UNSC.

TFS related to terrorism and TF. In relation to designated persons under relevant binding terrorism-related Resolutions, including UNSCR No. 1373 pursuant to Article 41 of the UN Charter and the ATA, covered persons, upon receipt of the notice of AMLC resolution on the issuance of sanctions freeze order, are required to freeze without delay the following:

a. property or funds that are in any way related to financing of terrorism or acts of terrorism; or
b. property or funds of any person, group of persons, terrorist organization, or association, in relation to whom there is probable cause to believe that they are committing or attempting or conspiring to commit, or participating in or facilitating the commission of financing of terrorism or acts of terrorism as defined under the Terrorism Financing Prevention and Suppression Act of 2012, the ATA and their respective IRRs.

The property or funds referred to in the immediately preceding paragraph shall include all property or funds:

a. That are owned or controlled by the subject of designation and is not limited to those that are directly related or tied to a particular terrorist act, plot or threat.
b. That are wholly jointly owned or controlled, directly or indirectly, by the subject of designation.
c. Derived or generated from funds or other assets owned or controlled, directly or indirectly, by the subject of designation.
d. Of persons or entities acting on behalf of at the direction of the subject of designation.

In case of asset freeze, covered persons are generally prohibited to:

a. Deal with the frozen funds or economic resources, belonging to or owned, held or controlled by a designated person;
b. Make funds or economic resources available, directly or indirectly, to, or for the benefit of, a designated person; and/or
c. Engage in actions that, directly or indirectly, circumvent the financial sanctions prohibitions.

Covered Persons shall submit to the AMLC a detailed written return, pursuant to, and containing details required under, Rule 16.c of the TFPSA IRR.

TFS related to proliferation of WMD and PF. In relation to designated persons pursuant to UNSCR Nos. 17/8 (2006) and 2231 (2015), and their successor resolutions, as well as any binding resolution of the Security Council, covered persons are required to:

a. Freeze the following within a matter of hours from the time that the designation and the freeze order is published in the AMLC website:

    1) All funds or other assets that are owned or controlled by the designated persons, and not just those that can be tied to a particular act, plot or threat of proliferation of WMD and PF;
    2) Those funds or other assets that are wholly or jointly owned or controlled, directly or indirectly, by designated persons;
    3) The funds or other assets derived or generated from funds or other assets owned or controlled, directly or indirectly, by designated persons;
    4) Funds or other assets of persons and entities acting on behalf of, or at the direction of designated persons;

b. Block or restrain specific properties or funds that are owned or controlled by a designated person from being transacted, converted, concealed, moved, or disposed; and

c. Prohibit any person or entity from making any funds or other assets available for the benefit of designated persons, unless licensed, authorized or otherwise notified in accordance with the relevant UNSCR.

TFS related to terrorism, TF, proliferation of WMD, and PF, requires full application or implementation. The TFS shall be effective until the basis for its issuance has been lifted.

The Bank has no appetite and shall strictly prohibit any dealings with designated persons or individuals/entities that are in any way affiliated to terrorist financing/proliferation financing.

8.7.1 Sample Typologies

a. Terrorist Financing

Terrorist generally finance their activities through both unlawful and legitimate sources. Branches and business units must take note of these different financing methods of terrorists/terrorist organizations to help them detect TF red flags and file STRs whenever warranted.

1. <u>Raising Funds from Legitimate Sources</u>

Terrorist organizations receive considerable support and funding from and through legitimate sources including charities, businesses, and through self-funding by terrorists and their associates from employment, savings, and social welfare payments.

- Charities/NPOs – NPOs have access to considerable sources of funds, their activities are often cash-incentive and often, they have global presence that provides a framework for national and international operations and financial transactions. Some forms of abuse of NPOs for TF are as follows:

a) Diversion of funds through fraud – for example, donors are told that they are donating money for orphans, and the charity then uses the funds to fund terrorists.

b) The use of an entirely bogus or sham organization that poses as a legitimate charity and as a front organization for terror groups.

c) Broad exploitation – for example, the charity raises money to feed orphans and actually does so but does it through a designated terrorist organization.

- Legitimate Business – Proceeds of a legitimate business may be used as a source of funds to support terrorist organizations. Risk of fund diversion is greater especially in cash-intensive businesses. Some example of unusual activities by legitimate business involved in TF are as follows:

  a) Inconsistency between the expected transactions of a business in a certain industry and the profession of a person that the former is issuing checks/cash deposits for, e.g. a restaurant owner regularly receiving checks and cash deposits from a wood company.

  b) Large-scale flow of funds that was disproportionate to the normal business activity of a specific company.

- Self-Funding – In some cases, terrorist groups have been funded from internal sources, including family and other non-criminal sources. The amounts of money needed to mount small attacks can be raised by individual terrorists and their support networks using savings, access to credit or the proceeds of businesses under their control.

2. <u>Raising Funds from Criminal Proceeds</u>

Terrorist use criminal activity to raise funds ranges from low-level fraud to involvement in serious and organized crime. Below are criminal activities terrorists are known to have engaged in:

- Drug Trafficking – this is an attractive source of funds for terrorist groups as this enable them to raise large sums of money.

- Credit Card Fraud – terrorists make use of the money raised through the use of someone else's credit card information.

- Cheque Fraud – this usually involved bank accounts being opened using false identity documents and fraudulent deposits.

- Extortion – this is when supporters of terrorist and paramilitary groups exploit their presence within expatriate or diaspora communities to raise funds through extortion.

- Multiple types of criminal activity – the opportunism of terrorist financiers is particularly illustrated by cases where suspects move fluidity from one crime to another[6].

b. Weapons Proliferation Financing

Below are different FATF-identified indicators for possible proliferation financing-related activity:

- Transaction involves individual or entity in foreign country of proliferation concern.
- Trade finance transaction involves shipment route (if available) through country with weak export control laws or weak enforcement of export control laws.
- Transaction involves shipment of goods inconsistent with normal geographic trade patterns (e.g. does the country involved normally export/import good?).
- Based on the documentation obtained in the transaction, the declared value of the shipment was obviously under-valued vis-à-vis the shipping cost.
- Inconsistencies in information contained in trade documents and financial flows, such as names, companies, addresses, final destination etc.
- Order for goods is placed by firms or individuals from foreign countries other than the country of the stated end-user.
- New customer requests letter of credit transaction awaiting approval of new account.
- The customer or counter-party or its address is similar to one of the parties found on publicly available lists of "denied persons" or has a history of export control contraventions.
- A freight forwarding firm is listed as the product's final destination.
- Wire instructions or payment from or due to parties not identified on the original letter of credit or other documentation.
- Pattern of wire transfer activity that shows unusual patterns or has no apparent purpose.
- Transaction involves shipment of goods incompatible with the technical level of the country to which it is being shipped, (e.g. semiconductor manufacturing equipment being shipped to a country that has no electronics industry)[7].

8.7.2 Policies and Controls

a. The Bank shall strictly perform screening against Base60 and Finacle Core Banking System (FCBS) of all new customers, authorized signatories, purchaser, payee, remitter or beneficiary, beneficial owners to ensure that the Bank does not establish relationship nor offer products and services to designated persons.

[6] https://www.fatfgafi.org/media/fatf/documents/reports/FATF%20Terrorist%20Financing%20Typologies%20Report.pdf
[7] https://www.fatfgafi.org/media/fatf/documents/reports/Typologies%20Report%20on%20Proliferation%20Financing.pdf

b. The Bank shall comply with the mandate of AMLC Resolutions TF-33 and TF-34 as well as subsequent designations by the ATC to freeze and preserve without delay property or funds, including related accounts, that are maintained or registered with, possessed or controlled by the Bank, in any, which belong to any of the persons, organizations, associations or group of persons mentioned in the ATC Resolutions.

c. The Bank shall not conduct business or enter relationships, facilitate any transactions or provide services to customers residing in sanctioned countries – DPRK and Iran. Aside from being outlawed by UN as involved in proliferation financing, both countries have comprehensive sanctions program which generally prohibit all direct and indirect activity or facilitation with these territory/country, including provision of financial products and services.

d. The Bank shall conduct a UNSC Consolidated List Name Matching (reverse screening) for every update to the UNSC Consolidated List sourced directly from the UNSC website. This is for the continuous monitoring of the Bank's customers, accounts and transactions.

e. The Bank must immediately upload and update the Internal Watchlist for every newly added names/designation of terrorists' individuals and groups by the Anti-Terrorism Council.

f. A detailed guidelines on the delineation of responsibility and process of reporting of potential and target matches shall be put in place.

g. The Bank shall prohibit the following should the financial action applicable is an asset freeze:

    1. Deal with the frozen funds or economic resources, belonging to or owned, held or controlled by a designated person;
    2. Make funds or economic resources available, directly or indirectly, to, or for the benefit of a designated person; and
    3. Engage in actions that, directly or indirectly, circumvent the financial sanctions prohibitions.

    The funds and economic resources are to be frozen immediately by the Bank upon receipt of confirmation from AMLC on the filed STR. An asset freeze does not involve a change in ownership of the frozen funds or economic resources, nor are they confiscated or transferred to the AMLC for safekeeping.

    The assets freeze applies to all assets owned or controlled by listed individuals, groups, undertakings and entities. It also applies to the funds that derive from property that they own or control, directly or indirectly, or that are owned or controlled by persons acting on their behalf or at their direction.

h. Branches/business units, upon finding "probable cause" that a client is in possession or control of, or are otherwise dealing with, the funds or economic resources of a designated person, shall:

    a) Report unusual transaction identified
    b) Freeze the account

c) Not deal with them or make them available to, or for the benefit of, the designated person, unless:
   - The transaction is an authorized dealing; or
   - The transaction is exempted as a duly authorized expense

d) Submit written return to Legal Services Division

i. The Bank shall promptly submit a Suspicious Transaction Report (STR) to the AMLC within the next working day from occurrence, if it has reasonable grounds to suspect that the transaction is being made by:

   - A designated person, e.g. a potential target match; or
   - An entity owned or controlled by a designated person.

   Attempted dealings are likewise reported as suspicious transactions.

j. The Legal Services Division upon receipt of a freeze order in relation to Terrorist Financing from AMLC shall immediately inform branches to immediately freeze accounts of persons subject of the freeze order.

k. The Legal Services Division shall file a return within 24 hours to the AMLC and the business unit/branch must file an STR, if the transaction is made by a person identified as a target match, that is, a person that matches all the description and identifier information provided in the Consolidated List and/or designations made by the ATC.

8.7.3 Implementation

a. Conduct of Watchlist Screening

Business Unit/Branch

Perform screening against Base60 for all new customers, authorized signatories, purchaser, payee, remitter or beneficiary, beneficial owners against when:

1. Establishing a business relationship/opening an account
2. Sale of bank drafts
3. Over the counter payment of remittances
4. Conducting Enhanced Due Diligence

Name and Target Matches

Situation	Assessment

You have a name match for a person who is a Filipino national listed as a member of the Abu Sayyaf Group (ASG) based in Basilan and involved in kidnapping for ransom. However, the person you are dealing with is a European foreign exchange student.	*Name match*
You have a name match for an Indonesian identified as a foreign terrorist fighter. However, the man you are dealing with is a regular bank client with a different date of birth.	*Name Match*
You have a close name match for a person subject to a terrorist asset freeze and they have a similar date of birth but a different address.	*Potential **target match*** You may have identified a new *alias* being used to circumvent financial sanctions. Subject to the rules and guidelines prescribed herein, funds actually received or in the possession of the covered person shall be frozen. Apart from filing STR, the Bank should inform the AMLC **on the same day the freeze is implemented,** through email to the secretariat@amlc.gov.ph, copy furnish the Executive Director, that a freeze has been implemented pursuant to these guidelines. Said information shall be accompanied by the following details:

	a. The subject's account name, number and amount frozen; b. The subject's entry under the relevant Consolidated List; and c. The date and time the freeze or hold order is implemented. The AMLC, within 36 hours from receipt of the information, shall confirm the propriety of the freeze. ***If no confirmation is received within the said 36-hour period, the freeze shall be automatically lifted.***

b. Sanctions Exposure Monitoring of Customers with Iranian/North Korean Nationality or Address

1. The assigned Compliance Officer will request for the database of all customers with Iranian/North Korean Nationality or Address;

2. Results will be presented to AMLCOM for necessary action and to the Board for notation.

c. Uploading of updated UNSC Consolidated List and ATC Designations in Base60 and Finacle Core Banking System (FCBS)

1. On a daily basis, the assigned officer shall visit the UN Security Council website for updates to the UNSC Consolidated Lists and the AMLC website for updates regarding ATC designations of terrorist groups/individuals.

2. The assigned officer shall prepare the list of the names updated and load the same to Base60 and FCBS within 24 hours after the release of updates.

d. UNSC Consolidated List and ATC Designations Name Matching (Reverse Screening)

The Bank shall conduct screening of all existing customers in the Bank's core banking system whenever there is an update to identify potential or target matches within the entire customer database.

<u>AML Compliance Officer</u>

1. Receive from the assigned officer the list of added designated persons to the UNSC Consolidated List and ATC Resolution within 24 hours from extraction.

2. Conduct a scrubbing/name-matching of the added designated persons against the Bank's entire customer database to determine a target match or a potential target match.

   In identifying potential or target matches, consider the following information provided for designated persons:

First and Last Name	Last known address
Aliases	Employment and government role
Date of Birth	Address
Passport Details	Other information provided
Nationality	

3. If a potential target match or a target match is identified, the information shall be referred to the AML Committee (AMLCOM) for deliberation and filing of Suspicious Transaction Report (STR).

e. Filing of Suspicious Transaction Report (STR) and Implementation of Freeze Order

AML Committee (AMLCOM)

Deliberate and approve the filing of STR for potential and target matches

The Legal Services Division

Inform AMLC of the STR filed through email to the secretariat@amlc.gov.ph copy furnish the Executive Director and Compliance Division with the following details:

a. The customer's account name, number and account balance; and
b. The customer's entry under the relevant Consolidated List/ATC Resolution

If positive name match found under UNSC Consolidated List and ATC Designations, immediately freeze the account.

NOTE: The AMLC to confirm the propriety of freeze within 36 hours from receipt of the information. If no confirmation is received within the said 36-hour period, the freeze shall be automatically lifted. The enterprise management of freeze orders and the submission of Written Return of Freeze Order shall be performed by the responsible offices and officers.

f. Freeze Orders directly received from AMLC

Freezing of Accounts or Properties of the Subject of Freeze Order and Readily Identified Related Accounts. The following procedures shall be strictly observed in handling the accounts or properties of a person who is a subject of freeze order. "Subject of Freeze Order" shall refer to the named personalities and entities provided in the order whose accounts or properties are subject to freeze order.

1. Upon receipt of the Freeze Order by the Bank's General Services Department or any appropriate department where the order was served, the forthwith forwarding/delivery of such Freeze Order to the Legal Services Division will be of utmost priority, as the Order requires immediate freezing of the subject accounts. The AML Compliance Department of Compliance Division shall also be provided a copy.

2. The Legal Services Division shall immediately provide the names listed in the Freeze and instruct the Branch/Unit, where the accounts/properties are maintained, to immediately freeze without undue delay, the accounts identified in order to prevent withdrawal or closure prior to the implementation of the Freeze Order.

   The notice and instruction of the Legal Services Division shall also be addressed to all branches/units for the latter to conduct their own search to ensure that other accounts of the subject of freeze order or related/materially linked accounts are identified and accounted for.

   Whenever an account or property can be immediately determined as a related account with reasonable certainty, such related account shall be immediately subject to freeze.

3. The Head of the Branch/Unit shall cause the freezing of the accounts or properties immediately upon receipt of the Freeze Order instruction from the Legal Services Division, simultaneously reporting to the latter any/all accounts made subject to the freeze order and the details thereof.

   It should be pointed out that it is the responsibility of the concerned Branch/Unit to preliminary identify, assess and note should there be any 'related web of accounts' to be considered. Likewise, the concerned Branch/Unit shall also make a report if there are no accounts identified to be considered as 'related web of account' and the same shall be furnished to Compliance Division and Legal Services Division;

4. The Head of the Branch/Unit concerned shall, without undue delay, cause the furnishing of a copy of the freeze order upon the customer/owner or holder of the monetary instrument or property or related accounts subject thereof.

   In no case shall notice be given to the customer prior to the freezing of accounts or properties.

g. Filing of Detailed Return Before AMLC

Submission of a Detailed Return. Within twenty-four (24) hours from receipt of the freeze order or freezing of the related account, the Legal Services Division of the Bank shall cause the submission, by

personal delivery, to the Court of Appeals and to the AMLC, a written detailed return on the freeze order.

The Bank, through the Legal Services Division, shall also submit to the AMLC, through the internet, an electronic detailed return in a format to be prescribed by the AMLC.

Contents of the Detailed Return. The detailed return on the freeze order shall specify all the pertinent and relevant information, which shall include the following:

- The names of the account holders, personal property owners or possessors, or real property owners or occupants;
- The value of the monetary instrument, property, or proceeds as of the time the assets were ordered frozen;
- All relevant information as to the status and nature of the monetary instrument, property, or proceeds;
- The date and time when the freeze order was served;
- The basis for the identification as related accounts; and
- The account numbers and/or description of the monetary instrument, property, or proceeds involved.

A detailed return shall also be filed before AMLC for cases where the AMLC directs the freeze of the funds and other assets of a person or entity who, although not specifically included in the Consolidated List or ATC designation, was nevertheless found to be acting for and in behalf or under the direction of those designated under the Consolidated List or ATC designation.

h. Reporting and Record-Keeping

a. Cases of denied/terminated business relationship, freezing of accounts or funds and block transactions due to the implementation of this policy shall be reported to the AML Committee and the Corporate Governance Committee not later than 30 calendar days from the date of occurrence.

b. Results of the screening and reports related thereto must be kept strictly confidential and all information must be treated under strict control, including safekeeping in separate files (with restricted access to other employees of the Bank) and will be made readily available to the AML Compliance Department in case AMLC conducts further investigation.

8.8 UPDATE OF SANCTIONS LIST DATABASE

8.8.1 The Sanctions List Database shall be updated immediately upon publication of the updated list online. The AML Compliance Department shall also provide available sources in the internet that can be used for name screening and sanctions review.

8.8.2 The AML Compliance Department shall assign personnel who shall monitor the updates to ensure timely updating of the database.

8.9 TRAINING AND EDUCATION

The Compliance Division shall ensure that regular and timely conduct of the necessary training and certifications are provided to the appropriate responsible officers and employees, tasked to implement this policy.

A specialized training shall be provided to the Sanctions Officers, Sanctions Expert and Senior Management approvers on the CBS Sanctions Program.

Further, Compliance Division shall ensure that all resolutions, circulars, and other issuances by the BSP and AMLC relative to terrorist financing and weapons proliferation are properly communicated to the Bank's directors, senior management, officers and staff.

Policies on terrorist financing and proliferation financing shall likewise be included during lectures, seminars and training programs conducted by Compliance Division.

PART IX
CUSTOMER RISK ASSESSMENT

PART IX: CUSTOMER RISK ASSESSMENT

9.1 RISK RATING CLASSIFICATION

The Customer Risk Levels are classified as follows:

a. **High Risk** - customer poses a major risk comparable to known money laundering typologies that it can engage knowingly or unknowingly in money laundering or terrorist financing activities although within tolerable level of risk, but subject to enhanced monitoring.

b. **Normal Risk** – customer does not pose a significant risk compared to known money laundering typologies that it can engage knowingly or unknowingly in money laundering or terrorist financing activities – it is an ideal level of risk.

c. **Low Risk** – customer poses a minor risk compared to known money laundering typologies that it can engage knowingly and unknowingly in money laundering terrorist financing activities – it is an ideal level of risk.

9.2 CUSTOMER RISK ASSESSMENT

Risk Classification is assigned to each customer upon opening of account and shall be periodically reviewed by the branch as follows:

a. Low Risk - Every 3 years
b. Normal Risk - Every 2 years
c. High Risk - Yearly

Risk rating using the ECRAF may be conducted as frequent as necessary or when there are known significant changes in the client's information material to the CBS AML Account monitoring and when adverse information or knowledge relating to an account is acquired by the branch that, based on reasonable judgment, will warrant the accelerated re-assessment of the said customer.

The customer's initial or current risk rating can be affected by a change in circumstances as well as the unusual transactions monitoring results. Therefore, customer risk rating may change at time from one rating to another.

Change of customer risk rating involving High Risk shall require the approval of Senior Officer, such as:

a. Low/Normal to High Risk
b. High risk to Normal/Low

9.3 DEFINED RISK PARAMETERS

Risk parameters are grouped into 3 clusters:

a. **Account/Entity Risk** – specific risk associated with the customer's type, nature of business, occupation or declared/anticipated transaction activity.

b. **Geographic Risk** – specific risk associated with doing business in, opening accounts for customers from, or facilitating transactions involving certain geographic locations.

c. **Products and Services Risk** – risk associated with the nature of specific products or services offered that can facilitate a higher degree of anonymity, or involve the handling of high volume of currency or currency equivalent.

9.4 CUSTOMER RISK ASSESSMENT PROCESS

Aside from the Default High Risk Customer (*see section 6.8 Default High Risk Customers for the complete list*), result of Customer Risk Assessment will be the risk equivalent of the client's score in ECRAF. The score in each risk criteria shall be summed up for the risk rating equivalent. Risk score bracket are as follows:

Risk Classification	Score Bracket
High Risk	19 or higher
Normal Risk	10 to 18
Low Risk	9

9.5 CUSTOMER DUE DILIGENCE REQUIREMENT

Upon identification of client's risk rating assignment of each customer, customer due diligence shall be conducted by the branch or concerned units as follows:

a. Low risk - Average Due Diligence (ADD)
b. Normal risk - Average Due Diligence (ADD)
c. High risk - Enhanced Due Diligence (EDD)

(*Refer to discussion in section 6.3.5 Required Due Diligence for further details*)

9.6 RISK ASSESSMENT CRITERIA AND STANDARD CUSTOMER DUE DILIGENCE

The criteria and description of the type of customers that are likely to pose low, normal or high risk and corresponding Customer Due Diligences standards such as reduced, average and enhanced due diligence will be applied and the result thereof will be used as a basis whether or not to deny the account opening.

Enhanced due diligence shall be applied to customers that are assessed as high risk for money laundering and terrorist financing. Average due diligence will be applied for customers assessed to be of low risk such as an individual customer with regular employment or economically productive activity, small account balance and transactions, and a resident in the area of the branch. Types of low risk entities includes banking institutions, trust entities and QBs authorized by the BSP to operate as such, public listed companies subject to regulatory disclosure

requirements, government agencies including GOCCs. Under no circumstances shall reduced due diligence will be applied, except for those instances expressly approved by the Board of Directors.

In Customer Risk Assessment as part of the customer acceptance policy, the following factors and considerations were taken into account:

Individual	Corporate/Entity
Political Exposure	
• Non-PEP • Domestic PEP and immediate family member of PEP • Foreign PEP	• Non-PEP from the company's directors, partners and signatories • Ownership of PEP directors, partners, signatories and/or his immediate family is less than 20% • Ownership of PEP directors, partners, signatories and/or his immediate family is 20% or more • At least one (1) of the directors/ partners/ signatories/ senior officers is a Foreign PEP
Residency or Citizenship / Place of Incorporation	
• Resident Filipino Citizen • Non-resident Filipino Citizen • Resident Alien • Non-resident Alien • Resident or Citizen of a High Risk Country	• Incorporated/Registered in the Philippines • Incorporated/Registered on a non-High Risk country • Incorporated/Registered on a High Risk foreign country
Geographical Address / Corporate Address	
• Less than 5 km from branch/unit • 5 to 10 km from branch/unit • More than 10 km from branch/unit	• Less than 5 km from branch/unit • 5 to 10 km from branch/unit • More than 10 km from branch/unit
Occupation/Nature of Work / Nature/Type of Business/Industry	
• Employed locally • Retired employee and/or Pensioner • Beneficiary of a local or national government program • OFW • Beneficiary of an OFW • Student • Self-employed or Investor • Unemployed and dependent on spouse or immediate family member's income • Other employment or self-employment abroad • Expatriate	• Government agency • Government-owned and controlled corporation • Banking Institution, Trust Entity, Quasi-bank authorized by BSP • Business not falling under "Low Risk" and "High Risk" • Non-profit / charitable institution / foundation • Money Service Business (Remittance and Transfer Company, Remittance Agent / Sub-agent, Remittance Platform Provider, Money Changer / Forex Dealer, E-Money Issuer) • Casino and gaming-related entity • Custom Brokerage

Individual	Corporate/Entity
• Current or former personnel of foreign government or international organization • Unemployed and not dependent on spouse of immediate family member	• Dealers of jewels / gems / precious metals, gun / ammunition / military equipment dealer
Source of Funds / Type of Ownership	
• Salary/Pension • Savings and Investments • Allowance from spouse, immediate family member, or government program • Trust Funds • Revenue from own business (not classified as High Risk) • Commissions • Income from profession (not classified as High Risk profession) • Remittance • Proceeds of Sale • Winnings / Rewards • Inheritance • Gifts / Donations • Income from High Risk profession (sole practitioner lawyer, broker or accountant) or income from High Risk business (ultimate beneficial owner and/or authorized signatory)	• Publicly-listed with PSE • Government-owned control • Non-stock / Stock Corporation (not PSE-listed) • Partnership • Sole Proprietorship • With foreign control (not PSE-listed)
Amount of Initial Transaction / Designated Authorized Signatories	
• Less than Php100,000 or its foreign currency equivalent • Php100,000 to Php500,000 or its foreign currency equivalent • More than Php500,000 or its foreign currency equivalent	• Individuals other than those listed as designated professionals • All signatories with risk profile of "Low' to "Normal" • Designated Professionals • One (1) signatory profiled as "High Risk" • Signatories are non-resident aliens • Two (2) or more signatories profiled as "High Risk"
Estimated Monthly Amount of Transaction (EMAT)	
• Less than Php100,000 or its foreign currency equivalent • Php100,000 to Php500,000 or its foreign currency equivalent	• Less than Php100,000 or its foreign currency equivalent • Php100,000 to Php500,000 or its foreign currency equivalent

Individual	Corporate/Entity
• More than Php500,000 or its foreign currency equivalent	• More than Php500,000 or its foreign currency equivalent
Length of Relationship	
• Existing customer for more than one (1) year • Existing customer for less than one (1) year • No prior relationship	• Existing customer for more than one (1) year • Existing customer for less than one (1) year • No prior relationship
Products and Services Availed and to be Availed	
• Peso Deposits • Loan Products • ATM Card • Remittance/Fund Transfer • Foreign Currency Deposits • Treasury Products • Internet Banking • Buy/Sell Foreign Exchange	• Peso Deposits • Loan Products • Remittance/Fund Transfer • Foreign Currency Deposits • Treasury Products • Internet Banking • Buy/Sell Foreign Exchange

The total risk rating of the client based on the Enhanced Customer Risk Assessment Form (ECRAF) accomplished by the authorized personnel during the client interview shall be the basis on what customer due diligence will be applied.

9.7 ENHANCED DUE DILIGENCE (EDD)

9.7.1 Minimum validation procedures for EDD.

The procedures performed must enable the Bank 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 email;
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. lnquiring 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 email.

9.7.2 Conducting Enhanced Due Diligence

Enhanced Due Diligence shall be applied on High Risk Clients or where the risk of possible Money Laundering or Terrorist Financing is high. The branch/unit shall perform the following other than the required conduct of average due diligence.

1. Gather additional customer information and/or identification documents, other than the minimum information and/or documents;

    a. For Individual Customers/Accounts - (i) documents submitted as supporting information on the intended nature of the business relationship/source of funds/ source of wealth (such as financial profile, lTR, Loan Application, Deed of Donation, Deed of sale, etc.);(ii) Reasons or purpose of the transactions or opening of account; (iii) list of companies where the client is a stockholder, director, officer, or authorized signatory; (iv) Result of Public search such as watchlist, Internet, News, and social media and other information available through public databases; and (v) a list of banks where the client has maintained or is maintaining an account.

    b. For Corporate Customers/Accounts - (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 (lTR, Audited Financial statement, Loan Application, Deed of Donation, Deed of sale, etc.); and (iv) reasons or purpose of transaction/opening of account.

2. Conduct validation procedures in accordance with the minimum validation for EDD 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 on-going monitoring of the account/business relationship, by, among others, tagging the client as High Risk to be subjected on Base60 Alerts for close monitoring of the transactions;

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 that the Bank may deem consider 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 branch/unit shall deny banking relationship with the customer. The branch/unit shall prepare the RISA signed by the Group Head for the deliberation of the AML Committee the possible suspicious nature of the transaction and the reporting of suspicious transaction to the AMLC when circumstances warrant.

If the branch/unit fails to satisfactorily complete the enhanced due diligence procedure or reasonably believes that performing EDD will tip-off the client, the branch/unit shall submit the RISA to the Compliance Division for the deliberation of the AML Committee the possible suspicious nature of the transaction and closely monitor the account and review business relationship.

9.8 AVERAGE DUE DILIGENCE (ADD)

Whenever average due diligence is required in customer acceptance policy, the following profiling of customers and monitoring should be conducted:

1. Verification of procedures for individual customers shall include but not limited to the following:

    - Confirming the client information such as date of birth from a duly authenticated official document
    - Verifying the permanent address through evaluation of utility bills, bank credit card statement, or other documents showing permanent address or through on-site visitation; and
    - Contacting the customer by phone, or letter (such as sending of “thank you letters”).

2. Validation procedures for corporate or juridical entities shall include but not limited to the following:

    - Confirming the name of the entity through the Articles of Incorporation or Articles of Partnership presented
    - Confirming the name, address, and citizenship or nationality of beneficial owner, if applicable, and its authorized signatories from a duly authenticated official document
    - Verifying the official address of the entity through business documents or through on-site visitation
    - Contacting the entity by phone, or letter (such as sending of “thank you letters”)
    - Verifying the nature of business of the entity through Articles of Incorporation or Articles of Partnership presented
    - Confirming the specimen signatures or biometrics of the authorized signatory from a duly authenticated ID’s/ official document

NOTE: Where additional information cannot be obtained, or any information or document provides is false or falsified, or result of the validation process is unsatisfactory, the Branch/Office/Operating Unit shall not allow account opening and/or initiate termination of the business relationship with the individual or entity without prejudice to the reporting of a suspicious transaction to the AMLC when circumstances warrant.

9.9 REDUCED DUE DILIGENCE (RDD)

Under no circumstances shall reduced due diligence will be applied, except for those instances expressly approved by the Board of Directors. But whenever reduced due diligence is applied in accordance with the customer acceptance policy, the following rules shall apply:

1. For individual customers, branch/unit 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 documents or other reliable, independent source documents, data or information.

2. For corporate, partnership, and sole proprietorship entities, a branch/unit 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.

In lieu of a valid ID, the Bank shall obtain the customer's complete name, birth date, address and nationality and ensure that it has a record of a clear photograph and signature or thumbprint.

The branch/unit 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.

9.10 WHEN TO CONDUCT EDD

Branches/Business/Operating Units shall conduct EDD when any of the following circumstance exists/occurs:

a. Reasonable doubt on the accuracy of any information or document provided or the ownership of the entity;

b. Justifies re-classification of the customer from low/normal risk to high-risk or vice versa pursuant to AMLC, BSP rules and regulations or the Bank's policy or when there is knowledge in the activity changes (e.g. low risk rate upon opening but later subject of suspicious transaction reporting or negative public information that warrant the changes of customer risk rating);

c. Change of customer risk rating involving High Risk customer shall require the approval of Senior Officer such as:

    i. Low/Normal to High Risk
    ii. High Risk to Normal/Low

d. The filing of suspicious transaction is warranted when any of the circumstances, but not limited to the following exists:

    i. Transacting without any underlying legal trade, purpose or economic justification;

ii. Transacting an amount that is not commensurate with the business or financial capacity of the customer or deviates from his profile;
iii. Structuring transactions in order to avoid being the subject of covered transaction reporting; or
iv. Knowing that a customer was or is engaged or engaging in any unlawful activity defined under the AMLA, as amended.

9.11 RISK RE-ASSESSMENT

9.11.1 Personal Account Subsequently Used for Business Transactions

The Bank shall not allow the use of individual accounts for business transactions or trade related transactions of covered institutions/persons listed below (Part II, (9) of the MTPP):

a. Banks, non-banks, quasi-banks, trust entities, foreign exchange dealers, pawnshops, money changers, remittance and transfer companies and other similar entities and all other persons and their subsidiaries and affiliates supervised or regulated by the Bangko Sentral ng Pilipinas (BSP);
b. Insurance companies, pre-need companies and all other persons supervised or regulated by the Insurance Commission (IC);
c. Securities dealers, brokers, salesmen, investment houses and all other similar persons managing securities or rendering services as investment agent, advisor or consultant mutual funds, close-end investment companies, common trust funds, and other similar persons, and other entities administering or otherwise dealing in currency, commodities or financial derivatives based thereon, valuable objects, cash substitutes and other similar monetary instruments or property supervised or regulated by the Securities and Exchange Commission (SEC);
d. Jewelry dealers in precious metals, who as a business, trade in precious metals;
e. Jewelry dealers in precious stones, who as a business, trade in precious stones;
f. Company service providers which, as a business, provide any of the following services to third parties: (i) acting as a formation agent of juridical persons, (ii) 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 person in relation to other juridical persons, (iii) providing a registered office, business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement; and (iv) acting as (or arranging for another person to act as a nominee shareholder for another person; and
g. Persons who provide any of the following services:
    i. Managing of client money, securities or other assets;
    ii. Management of bank, savings or securities accounts;
    iii. Organization of contributions for the creation, operation or management of companies; and
    iv. Creation, operation or management of juridical persons or arrangements, and buying and selling business entities.

The pattern of transaction activity and the amounts involved are the basis to determine if the personal account is used in business or trade related transactions. Under the Base60, certain alert scenarios/parameters will capture the said pattern of activity in the course of transaction review.

In the event an individual account is determined to be used for business or trade related transactions, the account must be re-assessed on whether to continue or terminate the business relationship. If deemed warranted for terminating the business relationship, an escalation to the AML Committee for appropriate action/decision shall be made. Once a decision is reached, it will be communicated to the concerned branch/business unit for its immediate execution.

Regardless of whether the business or trade-related transaction is for a covered institution or not, the personal deposit account of the client shall not be used for transactions of the business/entity.

Consequently, all personal deposit accounts must not be used for business related transactions. Business accounts must be maintained with the registered name of the business enterprise/ entity issued by regulatory agencies/bodies.

9.11.2 Prevalence of Unusually Large Transaction Alerts

The Bank should pay special attention to all complex, unusually large transactions against the client's declared profile, and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. The economic purpose of such transactions should, as far as possible, be examined and established.

Unusually large transactions on the account may lead to further review or investigation. Some of the controls implemented by the Bank to monitor unusually large transactions are:

a. Significant Activities Report – generated daily for individual and non-individual deposit customers whose debit and/or credit transactions sum up to at least P100,000.00 for a day for Branches; and

b. Base60 Alert Scenario – Unusually Large Transactions – this Base60 profile tends to capture transactions of clients with parameter of P500K for individual. (Please refer to Section 7.2.6 and Section 7.2.7 of the MTPP for the Disposition of Alerts and Alert Justifications)

Should the following suspicious indicators be present, aside from filing STR, the Bank shall reclassify the account as High Risk and perform EDD. The results of the EDD would warrant review of the business relationship to assess on whether to continue or terminate the account. If deemed warranted for terminating the business relationship, an escalation to the AML Committee for appropriate action/decision shall be made. Once a decision is reached, it will be communicated to the concerned branch/business unit for its immediate execution. The Authorized Officers may include the approval/recommendation of AMLCOM members are the Branch Head and the Service Head or its equivalent position in case of business units.

- Cannot or refuse to provide the requested additional information or documents supporting the large transactions;
- Raises doubts as to the accuracy of any of the information/supporting documents presented;
- Have no legal or trade obligation, purpose or economic justification that is consistent with the banking services availed of and expected transactions with the Bank.

- Transactions or instructions which have no apparent legitimate purpose and/or appear not to have a commercial rationale;
- Where the transaction being requested by the customer, without reasonable explanation, is out of the ordinary range of services normally requested, or is outside the experience of the financial services business in relation to the particular customer;
- Where, without reasonable explanation, the size or pattern of transactions is out of line with any pattern that has previously emerged;
- Transfers to and from high risk jurisdictions without reasonable explanation, which are not consistent with the customer's declared business dealings or interests; and
- Unnecessary routing of funds or other property from/to third parties or through third party accounts.

9.12 DEPOSIT ACCOUNT/ CLIENT ACCOUNT AML EXIT POLICY

9.12.1 The Bank shall discontinue its banking relationship with a customer under the following circumstances:

1. Customer is subject of Suspicious Transaction/s Report (STR) due to anti-money laundering, terrorist financing and proliferation financing predicate crimes;
2. Customer is subject of Suspicious Transaction/s Report (STR) due to strong indicators of money laundering as determined by the AML Committee;
3. Customer is subject of repeated filing of STRs (a minimum of 2 STRs);
4. Subject client is not cooperative in providing information or documents.

Basis: Section K, of the Terms and Conditions Governing the Opening and Maintenance of Accounts specifically on the Bank's right to close the account.

9.12.2 Procedures on the closure of accounts:

1. All accounts for closure under reason no. 3 shall be presented upon the recommendation of BSOMD Head to the AMLCOM. Accounts with KYC deficiencies upon opening and non-updating of customer records shall be subjected to the Bank's exit policy within 180 calendar days from original commitment date or from report date by Compliance Testing and Review Department, whichever comes first.

2. AMLCOM deliberates and decides on the closure of the accounts based on the justifications and recommendations provided by BSOMD.

3. If the committee, by a majority vote decides to close the account, the BSOMD Head or a representative from BSOMD shall advise the Branch thru email on the closure of the account.

4. The Branch shall close the account immediately or within thirty (30) days from receipt of the advice.

    a. Branch to notify the customer using the *pro forma* notice of closure letter

b. The letter shall either be personally delivered or sent via registered mail or authorized courier. If personally received by the client, he/she shall sign on the received portion. If client cannot personally receive delivery or refuses to receive, the letter notice shall be sent by registered mail or duly authorized courier. Proof of delivery via registered mail or courier shall be considered negative confirmation.

c. Proof of issuance and receipt of the letter must be documented and sent to BSOMD.

d. Branch shall report to BSOMD that accounts are closed with a screenshot of proof of closure.

e. A copy of the MC/DD must be issued in the name of the customer, if the account has remaining balance.

   Note: There are situations where the account is for immediate closure because of possible risk exposure on financial crimes.

   No fund transfer shall be effected to another CBS account, either to the client's other branch CBS account or to another third party CBS account.

   In case client refuses to have the accounts closed and referred the matter to his legal counsel, BSOMD shall immediately refer the case to Legal. However, the decision of AMLCOM to close the account is final.

5. BSOMD shall monitor the closure of the account and shall report to AMLCOM its final status.

PART X
INSTITUTIONAL RISK ASSESSMENT (IRA)

PART X: INSTITUTIONAL RISK ASSESSMENT (IRA)

Consistent with risk-based approach of risk assessment per BSP Circular 950, covered persons are required to identify, understand and assess their ML/TF risks, arising from customers, countries or geographic areas of operations and customers, products, services, transactions or delivery channels. The assessment methodology shall be appropriate to the nature of operations and complexity of the business of the covered person. The risk assessment shall (a) consider all relevant risk factors; (b) adequately document results and findings; and (c) be updated periodically or as necessary. Based on the risk assessment, the Bank shall take appropriate measures to manage and mitigate ML/TF risks.

10.1 THE RISK ASSESSMENT PROCESS

The Risk Assessment Process shall be divided into the following:

A. Understanding the Business
B. Determination and Impact of Inherent ML/TF Risk
C. Measurement and Evaluation of ML/TF Controls
D. Evaluation of Residual ML/TF Risk
E. Propose Action Plans on ML/TF Control Gaps

10.1.1 Understanding the Business

The initial process shall include the following sub-processes:

1. Description of the governance pertaining to ML/TF
2. Identification of the stakeholders involved in the risk assessment process
3. Identification of the risk universe
4. Creation of a risk scoring process in the valuation of risk factors, ML/ TF controls and residual risks

10.1.2 Determination and Impact of Inherent ML/TF Risk

This process is the identification of the aspects of the Bank that are inherently subject to ML/ TF risk. In the determination of inherent risk, the following are the minimum factors:

1. Products and Services of the Bank
2. Geographical Areas of Operation
3. Geographical Reach of Services
4. Customers
5. Partners or Tie-ups on Delivery of Service
6. Transactions
7. Other Relevant Factors, as may be determined by the Compliance Division

Vulnerabilities for each of the factors above shall be identified and documented, and the possible impact of vulnerability shall be measured (through scoring).

10.1.3 Measurement and Evaluation of ML/TF Controls

After determination and measurement of inherent risk, corresponding ML/TF controls shall be matched and evaluated against the inherent risks identified. Sufficiency and effectiveness of controls shall be considered in the evaluation of controls.

For the parameters/criteria in evaluating the strength of controls, refer to **Annex AM**.

10.1.4 Evaluation of Residual ML/TF Risk

Rating for the Residual Risk shall be calculated for each risk factor. The Bank-wide residual risk shall include all the residual risk rating calculated for each risk factor/category. The individual residual risk and the Bank-wide residual risk shall be translated into High, Moderate, and Low. The definition shall be set in separate and detailed scoring procedures to be formulated by Compliance Division.

10.1.5 Propose Action Plans on ML/TF Control Gaps

Action plans shall be proposed to the management and to the Corporate Governance Committee (CGCOM) to address the identified ML/TF control gaps. The proposed action plan shall at least include the following contents:

1. Detailed description of the residual risk identified and the control gap
2. The possible (or actual, if any) impact if such residual risk will not be addressed
3. The proposed action plans to address the residual risk
4. Timelines that should detail the activities to be performed, as applicable
5. Monitoring of progress until final resolution

10.2 COMMUNICATION OF RESULTS

After the review of IRA by Risk Operations Department Head, as the assigned officer to review the IRA independent from the makers, the results of the ML/TF Risk Assessment shall be communicated to the Management and to the Board of Directors through the Corporate Governance Committee (CGCOM) for proper disposition and monitoring.

Further, the audit procedures of the Internal Audit Division included the review of the ACAMS IRA report during their regular audit examination.

10.3 FREQUENCY OF BANK-WIDE ML/TF RISK ASSESSMENT

Assessment shall be conducted on a frequency commensurate to the overall risk assessment of the Bank. High risk rating shall warrant an annual risk assessment. Moderate risk assessment or low risk assessment shall warrant the conduct of risk assessment every 2 years. Material changes in any of the risk factors may warrant earlier conduct of risk assessment.

For every new product to be launched, Operational Risk Department shall inform AML Compliance Department of such fact so that the ML/TF/PF risk assessment will be conducted prior to product approval.

10.4 CBS IRA RESULTS

Please refer to **Annex AN** for the result of the Bank's IRA.

PART X
INSTITUTIONAL RISK ASSESSMENT (IRA)

PART XI: COVERED AND SUSPICIOUS TRANSACTION REPORTING

The responsibility of the Bank in this Part of the MTPP shall cover the filing of covered and suspicious transactions report, maintaining confidentiality of such reports and any part thereof, and ensuring that the record format and retention standards are followed.

11.1 COVERED TRANSACTION

Covered transaction is a transaction in cash or other equivalent monetary instrument involving a total amount in excess of Five Hundred Thousand Pesos (P500, 000.00) within one (1) banking day. The Covered Transaction Report (CTR) shall be filed to the Anti-Money Laundering Council (AMLC) through the AMLC portal within five (5) working days from the date of transaction.

To ensure that the Covered Transaction Reports (CTR) being submitted to the Anti-Money Laundering Council (AMLC) is complete and accurate, the daily validation of CTR is mandated to all the reporting units.

The reporting unit shall validate and ensure that all transactions involving above P500,000 were captured by the Base60 AML System with complete and accurate information. In case of incorrect/incomplete information of the CTR captured by Base60 AML System, the reporting unit shall prompt the Compliance Division and correct the information or provide the lacking information in Base60 AML System.

11.2 FILING OF COVERED TRANSACTION REPORT

The following guidelines shall be observed in the filing of covered transactions:

1. Covered transactions shall be automatically captured by the Base60 AML Electronic Monitoring System (referred herein as Base60).

2. All required/mandatory information pertaining to the customer, account and transaction are captured by the Base60 from the core systems (*e.g. FINACLE, NOAH*).

   Base60 has its initial validation protocol that includes validation rules to trap missing and invalid values on mandatory information during CTR generation. CTRs with missing or invalid information will be tagged by the system as “Incomplete”. For “Incomplete CTRs”, the Branch/Unit shall have three (3) banking days from the date of transaction to complete the missing mandatory information. With coordination of the Branch, the Authorized Personnel of the AML Compliance Department or other designated independent unit may initiate completion/correction of the incomplete/blank mandatory fields, provided that the information is confirmed by the Branch or unit of account.

3. The generated covered transactions of each Branch/unit are available and accessible in Base60 for review of the respective Unit Compliance Coordinators and/or authorized users. The Authorized Personnel is required to utilize the Base60 Dashboard to view the items for action of the Branch/Unit.

4. The Unit Compliance Coordinator and Approver of all Branches/concerned units shall be jointly accountable in reviewing and ensuring that all covered transactions to be reported and to be transmitted are accurate, complete and timely (*within the prescribed deadlines set herein*).

5. For system-generated CTRs, the Unit Compliance Coordinators and the Approvers of all branches and concerned units shall attest to the completeness and accuracy of the information even if the Status indicated in the CTR is "Complete", and for those with initially "Incomplete" Status, complete the missing information required under AMLA (*e.g. accountholder, address, birth date, beneficiary/payee name and address and/or as the case may be*). Thus, both the Coordinator and the designated Approvers are required to review all CTRs generated for their branch/unit on a daily basis to ensure accuracy and completeness of each.

6. In the extreme case of covered transaction not electronically captured by the Base60 and/or any of the bank applications, the Authorized Personnel shall manually enter the complete details required in the system using CTR Data Entry and Enrichment Module in the Base60. The manual input up to the Branch/Unit approval shall be accomplished within three (3) banking days from the date of transaction.

   It is of utmost importance for the Authorized Personnel to correctly input the reference number and date & time of the transaction. Once saved, both the reference number and transaction date & time cannot be edited. Thus, the CTR needs to be re-encoded entirely in case of error in reference number or date & time.

   In case there is no transaction reference number directly traceable to the transaction, the following referencing guide shall be used:

   XXXX-BBBB-NNNNNN

   Where:

   XXXX is the transaction description/prefix
   BBBB is the 4-digit branch code
   NNNNNN is the last 6 digits of the dimension posting sequence number

   The branch/unit may opt to assign a unique reference number different from the suggested format above which is easily traceable to the transaction provided the Compliance Division has been informed of such convention.

7. The Branch Service Head or designated approver (for Units) shall review and approve (or reject) the work of the Unit Compliance Coordinator for manually created CTR or any change made in the mandatory field of a CTR.

   A rejected CTR shall be re-opened and resubmitted to the Approving Officer immediately so as to meet the three (3) banking-day deadline for managing CTRs.

8. CSV files of all CTRs with "Complete" (*and "Approved" in case of manually created or amended CTR*) Status shall be generated by the AML Compliance Department on a daily basis.

Prior to generation of the CSV files, the AML Compliance Department shall conduct validation procedures through the established monitoring tools via Crystal Report to ensure that "invalid values" [*e.g. possible incorrect/missing birthday, missing or invalid address (e.g. with c/o or P.O. Box)*] are detected. Status of a CTR with an invalid value shall be reverted to "Incomplete" and the Branch/Unit Authorized Personnel are required to resolve/amend the invalid value within 24 hours from the time reverted or earlier as reasonably prescribed by the AML Compliance Department to meet the deadline for filing. A visual review shall also be conducted by the AML Compliance Department to ensure obvious format or value error are detected prior to the encryption of the CSV files. The correction of invalid values may be initiated by the AML Compliance Department or a designated independent unit, provided that the amended information is confirmed by the Brach or unit of account.

The AML Compliance Department shall ensure that encrypted CSV files of covered transactions generated for the day are filed through the AMLC portal on the same day when such CSV files are generated.

9. Submission of CTRs beyond 12:01 am of the day following the 5th banking day from occurrence of the transaction shall be considered as non-submission of CTRs and may be subject to appropriate administrative sanction, if circumstances so warrant. (*Note: monetary penalty is Php300,000 per delayed transaction, see Rules on Imposition of Administrative Sanctions*).

10. The AML Compliance Department of Compliance Division shall conduct an independent monitoring of the aging and status of CTRs through the Base60 AML System or other report generated outside the Base60. The Authorized Personnel of the AML Compliance Department shall call the attention of any Branch/Unit exceeding the 3 banking-day period on CTR management.

11.3 SUBMISSION OF COVERED & SUSPICIOUS TRANSACTION REPORTS (CTR/STR) to AMLC

The Compliance Division through the AML Compliance Department shall consolidate the reviewed/corrected CTRs/STRs and submit the same to the AMLC within five (5) banking days from the transaction/reference date for CTRs and within the next working day from the date of determination of the suspicious nature of the transaction for STRs through the AMLC electronic portal.

11.4 SUSPICIOUS TRANSACTION

Under Sec. 3 (b-1) of the AMLA, a Suspicious Transaction is a transaction, regardless of amount, where any of the following circumstances exists:

1. There is no underlying legal or trade obligation, purpose or economic justification;
2. The client is not properly identified;
3. The amount involved is not commensurate with the business or financial capacity of the client;
4. Taking into account all known circumstances, it may be perceived that the client's transaction is structured in order to avoid being the subject of reporting requirements under RA No. 9160, as amended;
5. Any circumstance relating to the transaction which is observed to deviate from the profile of the client and/or the client's past transactions with the Bank;

6. The transaction is in any way related to an unlawful activity or any money laundering activity or offense under RA No. 9160, as amended, that is about to be, is being or has been committed;
7. Any transaction that is similar or analogous or identical to any of the foregoing, such as the relevant transactions in related and materially-linked accounts, as herein defined; or
8. Any unsuccessful attempt to transact with a covered person, the denial of which is based on any of the foregoing circumstances, shall likewise be considered as suspicious transaction.

11.5 DETERMINATION AND FILING OF SUSPICIOUS TRANSACTION REPORT

In compliance with the AMLC Registration and Reporting Guidelines (ARRG), the following guidelines for the determination of the suspicious nature of transaction and the filing of STR shall be observed by the bank:

As a general rule, STRs shall be promptly filed **within the next working day from the occurrence thereof**.

Occurrence refers to the date of establishment of suspicion or determination of the suspicious nature of the transaction, which determination shall be made not exceeding ten (10) calendar days from the date of transaction.

Determination period refers to the maximum number of days allowed within which the bank, through the AML Committee, shall have decided with finality to file an STR with the AMLC should the suspicion or suspicious nature of the transaction or activity be duly established or determined, or otherwise to document the non-filing thereof. The determination period and time of STR submission shall be as follows:

Type/Source of STR	Determination Period	Time of Filing
1. Transactions attended by any of the suspicious circumstances	***10 calendar days*** from the date of transaction or determination of suspicious nature	11th calendar day from transaction date or the day immediately after suspicious nature is determined
2. Transactions or persons related to an unlawful activity	***60 calendar days*** *from the date of transaction or determination of suspicious nature*	61st calendar day or the day immediately after suspicious nature is determined
3. [8]Highly unusual or suspicious transactions	Within the day of [9]knowledge	Day 1 or within the day of knowledge
4. TMS-Generated Alerts	***60 calendar days*** from the date of transaction but series of transactions shall ***not be more than***	61st calendar day

[8] A "highly unusual" or suspicious transaction is one where, at the moment of transaction, the Authorized Personnel handling the transaction has knowledge and reason to suspect that the funds being transacted are related to an unlawful activity.

[9] Knowledge is demonstrated in the following circumstances:

- ✓ Actual Knowledge;
- ✓ Knowledge of circumstances which would indicate facts to a reasonable person; and
- ✓ Knowledge of circumstances which would put a reasonable person on inquiry

	31 consecutive calendar days *at any given time*	
5. STR using the "ZSTR" transaction code	***60 calendar days*** from flagging/ alert generation to determine the suspicious nature	61st calendar day

The following general guidelines shall be observed for reporting of suspicious transactions and/or activities to AML Compliance Department:

a. All suspicious transactions shall be reported by the Compliance Coordinator to the Compliance Division. The Compliance Coordinator should submit the report using the Report on Incident of Suspicious Activity (RISA) Form with relevant supporting documents not later than the following working day when knowledge of or suspicion on the incident/ activity has been established.

   If the source of suspicious transactions or activities is discovered by AML Compliance Department in the conduct of review and investigation of alerts and scrubbing of names in the SEC Advisory and Anti-Terrorism Council designations, no RISA Form is required. The assigned officer of AML Compliance Department shall draft an STR memorandum for review of the AMLCOM Secretariat and for endorsement to the AMLCOM.

b. Compliance Division, upon receipt of the RISA, shall review the same as to its completeness. If found to be complete in form and substance, the AMLCOM Secretariat will endorse the RISA to the AMLCOM members for voting of STR filing via email. The votes of the members shall be casts via email also.

   The STR shall be immediately submitted to AMLC upon approval of the majority members of the AML Committee.

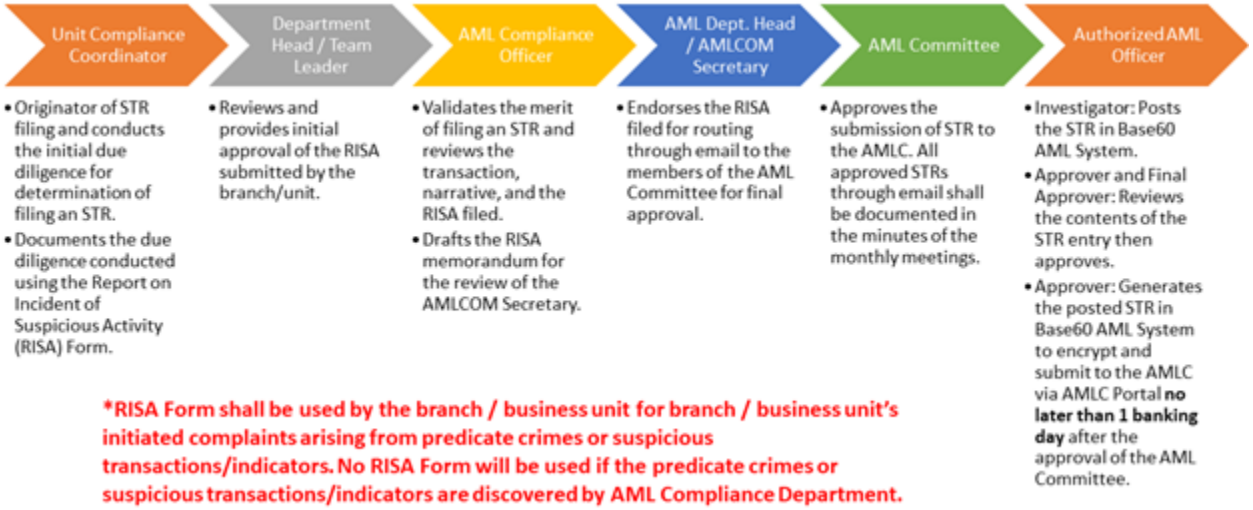
c. If upon deliberation, the AML Committee resolved that there is reasonable basis to file an STR, Compliance Division shall coordinate with the reporting unit on the decision of the AML Committee and instruct the posting of STR in Base60 AML System. Compliance Division shall generate the posted STR in Base60 AML System and submit to AMLC through AMLC web portal **within the next working day** using the AMLC electronic format. The next working day period shall be reckoned from the date of determination of the suspicious nature of the transaction by the AML Committee.

d. If upon deliberation, the AML Committee resolved that there is reasonable basis not to classify a transaction as an STR, or not to file an STR, the same must be documented. Compliance Division shall maintain a registry of all suspicious transaction reports, including transactions not resulted to an STR.

e. For other sources of STRs coming from Customer Experience Management (CEM) Department and Governance and Regulatory Compliance Department, AML Compliance Department shall be furnished with a summary of complaints or list of RCLs on a regular basis.

f. The branch or the business unit where the STR originated shall be notified of the filing of the suspicious transaction.

g. Suspicious Transaction Reporting Process Flow



11.6 SOURCES OF SUSPICIOUS TRANSACTION REPORT

STRs may be endorsed either by the Branch/unit, Compliance Division or by the Senior Management/AML Committee. STRs may come from the following:

1. Suspicious Indicators (*Transaction or profile indicators*) that caused the updating or detected upon updating of customer records where such indicator is not resolved satisfactorily, see section 6.8(n).
2. On-boarding indicators noted upon account opening or updating of customer records that were not satisfactorily resolved, *section 6.3.1.4*, or other similar indicator warranting further action.
3. Base60 Alerts disposed as "Report as STR"
4. Upon further due diligence of accounts/customers subject to AMLC Inquiry or Freeze Order.
5. Negative news monitoring as provided in *section 7.3*.
6. Report on Crimes and Losses (RCLs) pertaining to unlawful activities under AMLA.
7. Any unsuccessful attempt to transact with the Bank, the denial of which is based on any of the circumstances under Sec. 3 (b-1) of AMLA (*see section 10.4 above*), shall likewise be considered as suspicious transaction.

If the endorsement is from Compliance Division (*by the AML Compliance Department Head*), further endorsement from the Branch/unit shall not be necessary provided that such is approved by the Chief Compliance Officer.

11.7 INFORMATION SHARING FOR SUSPICIOUS TRANSACTION REPORTING

Customer Complaints. Customer Experience Management (CEM) Department shall provide AML Compliance Department a summary of all complaints received for the month no later than the 5th banking day of the next month.

Reports on Crimes and Losses (RCL). Governance and Regulatory Compliance Department shall provide AML Compliance Department the summary of the **Initial RCL** not later than 3 banking days from filing with the BSP.

Likewise, Governance and Regulatory Compliance Department shall provide AML Compliance Department the summary of the **Final RCL** not later than 2 banking days from filing with the BSP.

11.8 APPROVAL/REJECTION BY THE AML COMMITTEE

Upon the endorsement of and based on the facts presented by the Committee Secretary (*AML Compliance Department Head*) or Committee Assistant Secretary (*designated by the Committee Secretary*), the AML Committee shall review and approve (or reject) the filing of Suspicious Transaction Report to the AMLC. Such approval/rejection may be communicated via official Lotus Notes email or via signature, either of which shall be clearly documented in the minutes of the immediate AMLCOM meeting.

In extreme circumstances when the voting of the AML Committee resulted in the REJECTION of filing of STR or there is a "tie" in the voting, the Chairman of the AML Committee (*regardless of his/her vote*) shall elevate the matter to the Corporate Governance Committee (CGCOM). The CGCOM shall act as the final arbiter on the recommendation of the AML Committee Secretary to file the STR. The decision of the CGCOM shall be final and executory, and shall be recorded in the minutes.

11.9 NON-COMPLIANCE WITH THE AMLA REQUIREMENTS

The following shall be observed in closing of accounts due to non-compliance with the requirements of AMLA, its Implementing Rules and Regulations and related BSP Circulars.

The Bank shall close the account due to any of the following circumstances upon proper approval of the authorized officers:

1. Non-submission of complete KYC information and documents and failure to obtain the information and documents after efforts are fully exhausted.

2. Any information or document provided is false or falsified (e.g. fake IDs, inconsistent/ unjustifiable information).

3. The result of validation process is unsatisfactory (e.g. returned "thank you letter" due to adverse information, unregistered / cannot be reached telephone numbers)

4. Additional information for enhanced due diligence cannot be obtained (e.g. list of banks, list of companies and businesses that the client owns, information to justify legitimacy of unusually large transaction).

5. Accounts covered by the Freeze Order but subsequently lifted by the court.

The existing guidelines on Bank-initiated closure of account under the Deposit Product Manuals and other Manuals shall be observed. The account balance of bank-initiated closure of account shall be returned to the client through a Manager's Check. Payee should be account name only.

a. If the account is found to be fictitious and/or used for fraudulent purposes, the matter should be referred to Legal Services Division for proper disposition.

b. The Bank shall send to the account holder's last known address indicated in the Bank's records the notice of closing the account.

11.10 REPEATED FILING OF STR TO A PARTICULAR CUSTOMER

The business relationship to a customer whose account is not subject to freeze order but with repeated filing of STR due to repeated non-compliance with the Bank's due diligence requirements or circumvention or the use of other channels or service/transaction to avoid committing the transaction previously subjected to review or inquiry and previous filing of STR, shall be terminated without prejudice to the filing of STR for the last transactions performed.

The basis on whether to continue or terminate the business relationship with the customer depends on the number and the extent of STR filed. A minimum of two (2) STRs from any sources/nature of transactions must be filed against the client before the account shall be escalated and recommended to the AML Committee for account closure.

For every STRs filed, the Branch/Unit shall automatically upgrade the risk classification of the customers as "High" and enhanced due diligence shall be performed, without prejudice to the tipping-off policy (Section 10.13 of MTPP). The purpose of the EDD is to assess whether or not to continue the business relationship. This assessment shall be submitted to the Compliance Division through the AML Compliance Department for evaluation. **Please see Annex AL for the criteria in determining whether or not to continue business relationship with the client.**

Note: There are instances, as identified by the AML Committee, where the account is for immediate closure because of possible risk exposure on financial crimes.

11.11 LATE/ERRONEOUS REPORTING

11.11.1 CTR and STR as a major report. Both the CTR and STR shall be considered as major reports. Thus, the Branches/Units are required to prioritize the management of these reports to avoid monetary penalties and other type of sanctions.

The erring personnel of the Branch/Unit/Compliance Division shall be responsible for any unjustifiable non-compliance with the applicable deadlines, as well as the completeness and accuracy requirements prescribed in this MTPP. Any penalty levied against the Bank due to late submission, erroneous reporting or non-submission, as the case may be, shall be charged to the erring personnel after due process per policy of the Bank.

11.11.2 Notice of non-compliance from the AMLC. The AML Compliance Department shall notify the erring branch/unit in case of erroneous and late submission of CTR or STR as relayed by AMLC and shall coordinate the proper charging of any penalty due to the erring branch/unit.

11.11.3 Unforeseen events causing delay and inaccurate reporting. In case of unforeseen or fortuitous events that directly hinder the branch/unit/AML Compliance Department from reviewing, approving or transmitting

the report to the AMLC, the AML Compliance Department Head and the Chief Compliance Officer shall be immediately notified for the timely formulation of the appropriate action.

The determination of unforeseen event is not applicable anymore to delayed CTRs/STRs due to earlier violations of the deadlines prescribed in this part of the MTPP.

11.11.4 Correcting previously filed inaccurate report. In the event that an erroneous CSV file (e.g., incorrect account name, incorrect amount, duplicate, etc.) has been transmitted to the AMLC by the AML Compliance Department, the erring Unit Compliance Coordinator and Approver of the branch/unit shall be jointly responsible to make the necessary corrections in the Base60 AML System and inform AML Compliance Department via email – indicating in the subject line "CTR correction for transmission to AMLC with transaction date YYYYMMDD.

The AML Compliance Department shall cause the submission of the amended CTR in accordance with the applicable rules in the Amended Registration and Reporting Guidelines (ARRG). See **Annex D** for the copy of the AMLC Registration and Reporting Guidelines.

11.11.5 Independent monitoring. The AML Compliance Department, or a designated unit independent of the operations of the monitored Branch/Unit, shall cause the monitoring of the Branch/Unit's compliance with the deadlines prescribed in this MTPP.

11.11.6 Monetary penalties for delayed and inaccurate reporting. Delayed/non-reporting of CTR within five (5) banking days from the date of transaction and within the next working day from the date of determination of the suspicious nature of the transaction for STR (as applicable) and erroneous/inaccurate filing of CTR/STR shall be subject to an administrative sanctions and monetary penalties. [*Please see Rules of Procedure in Administrative Cases (RPAC) issued by the AMLC last July 2019 for the complete list of violations and the corresponding penalties*]. You may also refer to section 14.1 of this MTPP for immediate reference on administrative sanctions.

11.12 DEFERRED REPORTING OF LOW RISK TRANSACTIONS

In general, low risk transactions enumerated below are automatically captured and tagged as deferred by the Base60. For deferred transactions that need prior determination, such covered transaction shall be deferred using the applicable function in the Base60, subject to the approval of the AML Compliance Department of Compliance Division.

Pursuant to the 2021 AMLC Registration and Reporting Guidelines, the following are considered "non cash, no/low risk covered transactions" the reporting of which to the AMLC are deferred:

a) Transactions between BSP Supervised Financial Institutions (BSFIs) and the BSP;

b) Transactions between banks operating in the Philippines. however, limited to proprietary transactions only. Proprietary transactions carried-out for the account and sole benefit of the bank BSFI.

When a transaction is carried-out by the bank BSFI upon the instruction, as well as for the account and benefit of its customers using the depositors'/customers' own money, this is considered a non-proprietary transaction, and shall be reported as covered transaction/s.;

c) Transactions involving transfer of funds from one deposit to another deposit account of the same person within the same BSFI;

d) Roll-over of placements of time deposits and/or other client's investments, provided that there is no change in the Account number and the initial placement/contribution/investment was reported;

e) BSFI-initiated (transactions of the bank) or system generated transactions such as but not limited to:

   a. Internal operating expenses and capital expenditures that are booked as such in the books of the covered persons.

      These are necessary expenses of covered institutions for the normal day-to-day running of a business. These are transactions of covered persons and, therefore, not reportable. Such as, but not limited to payment of salaries, taxes, debt service, SSS premiums, Pag-IBIG contributions and employees' benefits.

   b. Payments of dividends or interests on investments, provided that the principal investment was previously reported;

   c. Remittance by a BSFI, acting as a collecting agent, of taxes and other government fees collected from the public, to the Bureau of Internal Revenue and other government agencies;

   d. Remittance by a BSFI, acting as a collecting agent, of customers' bills payment (e.g. utilities);

   e. Adjusting entries or reclassification of accounts;

   f. Service fees, proprietary revenue fees, arrangement fees, loan syndication fees and other form of fees incidental to loans granted or investments sold, provided that the loans granted or the sale of investment was reported at gross or at its principal amount; and

   g. Investments of covered persons in government securities, or in companies listed in the local or international Stock Exchanges.

f) Reclassification of loan to Real and other Properties Acquired (ROPA) provided that the loan availment was previously reported;

g) Loan repricing, loan renewal, loan restructuring, provided that there is no change in borrower's name, otherwise, the loan shall be considered as new loan, hence, reportable;

h) Transaction of government agencies with BSFIs, EXCEPT the following:

i. Disbursement of government agencies that passed through the Modified Disbursement Scheme (MDS), which disbursement are payable to private entities; non-governmental organizations (NGOs); non-profit, charitable or religious foundations; or to individual persons;

ii. Disbursement of government agencies coursed through other depository banks, other than the MDS accounts, that are payable to private entities; non-governmental organizations (NGOs); non-profit, charitable or religious foundations; or to individual persons;

i) Agrarian Reform Receivables; and

j) Payment for agricultural lands under the Agrarian Reform Law.

11.13 ELECTRONIC MONITORING SYSTEM FOR MONEY LAUNDERING

The bank adopted the Base60 System as the Bank's Electronic Monitoring Systems which are being utilized by the Compliance Division primarily in detecting, monitoring and reporting covered and suspicious transactions. Enhancements, modifications and system enhancement are handled by the Compliance Systems Support Department in close coordination with the Compliance Division and other affected Operations & Support units.

Several modules are available in the Base60 System that may be used to detect activity and fulfill regulatory requirements.

a. **KYC Profiling** – Enables the user to configure and modify different categories, profiles and rule engines of different peer groups and configure scenarios for profiles and watch lists.

b. **Transaction Profiling** – Enables the user to establish their own templates for customers and groups that warrant enhanced due diligence, allowing the user to systematically detect suspicious activity such as structuring, unusually large transactions The user can create a variety of profiles to cover a variety of scenarios.

c. **Enhanced Due Diligence** – Enables the use to define and configure scenario/conditions (based on the checklist) under which alerts get generated on the customer.

d. **Watchlist Monitoring** – Enables to define and configure scenario/conditions (based on the Watchlist) under which an alert can be generated on the customer/client. (The watchlist contains data about organization or country or customer that are found to be suspicious of indulging in any unlawful activities.)

11.14 TIPPING-OFF POLICY

The Branch/Unit shall not, in any way, inform the customer or any other unauthorized person the fact that the business relationship or the account with the Bank is being investigated for determination of filing of suspicious transaction.

In cases where the Branch/Unit forms a suspicion of money laundering/terrorism financing and associated unlawful activities, and reasonably believes that performing the due diligence process, particularly requesting additional information or documents, will ***"tip-off"*** the customer, the Branch/Unit need not pursue the requesting of such documents/information, but should file a Suspicious Transaction Report (STR), tag the customer as automatic High Risk (*requiring updating of ECRAF*), closely monitor the account, and review the business relationship for possible termination.

11.15 CONFIDENTIALITY OF FILING COVERED AND SUSPICIOUS TRANSACTION REPORT

ALL Bank personnel, senior officers and the members of the Board of Directors are prohibited from communicating, directly or indirectly, in any manner or by any means, to any person the fact that covered or suspicious transaction report was made, the contents thereof, or any other information in relation thereto, except in circumstances allowed by the AML laws and regulations by the Authorized Personnel of the Bank (*e.g. AML Compliance Department Head, Chief Compliance Officer*).

Violation of this provision shall be subject to administrative penalties prescribed in the Bank's Code of Ethics or other applicable policy, without prejudice to the filing of separate administrative/criminal charges.

11.16 SAFE HARBOR PROVISION

No administrative, criminal or civil proceedings shall lie against any person for having made a CTR or STR in the regular performance of his duties in good faith, whether or not such reporting results in any criminal prosecution under the R.A. 9160, as amended, its RIRR or any other applicable laws in the Philippines.

When filing a suspicious or covered transaction report to the Anti-Money Laundering Council (AMLC), the Bank, its officers and employees shall not be deemed to have violated R.A. 1405 as amended, R.A. 6426 as amended, R.A. 8791 as amended and similar laws on confidentiality of records or information.

11.17 FILES ARCHIVAL AND BACK-UP

The Base60, or through any other separate system, shall perform archival and backup procedures. The system has an archive module wherein extracted CTRs and STRs are kept. These files shall be maintained for five (5) years and/or in accordance with the Bank's policy on records retention period, whichever is longer. Transaction and Alert History may be kept for a longer period of time as provided by the Compliance Division.

PART XII
HANDLING OF FREEZE ORDER, BANK INQUIRY AND OTHER ORDERS

PART XII: HANDLING OF FREEZE ORDER, BANK INQUIRY AND OTHER ORDERS

The following guidelines shall be strictly implemented in the processing of freeze order, bank inquiry and other orders by the Court or the Anti-Money Laundering Council (AMLC).

12.1 RELATED ACCOUNTS

Related Account refers to an account, the funds and sources of which originated from and/or are materially-linked to the monetary instruments or properties subject of the freeze order or an order of inquiry, regardless of the layer of accounts that the funds had passed through or transactions that they had undergone.

Materially-linked accounts shall include the following:

a. All accounts or monetary instruments under the name of the person whose accounts, monetary instruments, or properties are the subject of the freeze order or an order of inquiry;

   Example:

   Mr. Juan dela Cruz's account number CBSSA001 is listed in the Notice of Freeze Order (NFO). Mr. dela Cruz also maintains accounts under: (1) Savings Account with account number CBSSA002 and (2) Time Deposit Account with account number CBSTD201.
   Accounts CBSSA002 and CBSTD201 are considered materially linked accounts.

b. All accounts or monetary instruments held, owned, or controlled by the owner or holder of the accounts, monetary instruments, or properties subject of the freeze order or order of inquiry, whether such accounts are held, owned or controlled singly or jointly with another person;

   Example:

   Mr. Juan dela Cruz's account number CBSSA002 is listed in the Notice of Freeze Order (NFO). Mr. dela Cruz also maintains accounts under: (1) Savings Account with account number CBSSA003 jointly with his wife, (2) In-Trust-For Time Deposit Account with account number CBSTD202 FAO of his daughter, and (3) Current Account with account number CBSCA101 under the trade name JDC Trading (a sole proprietorship entity of Mr. Juan dela Cruz).

   Accounts CBSSA003, CBSTD202 and CBSCA101 are considered materially linked accounts.

c. All accounts or monetary instruments the funds of which are transferred to the accounts, monetary instruments or properties subject of the freeze order without any legal or trade obligation, purpose or economic justification;

   Example:

The Court of Appeals issued a Notice of Freeze Order (NFO) against the account of Mr. Juan dela Cruz under account number CBSSA004. Account CBSSA004 was already closed at the time of receipt of the NFO. Review of the account CBSSA004 revealed that Mr. Juan Palaris through his account number CBSSA031 transferred/deposited funds to Mr. dela Cruz's CBSSA004.

Mr. Palaris' account number CBSSA031 is considered materially linked account if the transfer/deposit of funds does not have an underlying legal or trade obligation, economic justification or purpose.

d. All "In Trust For" accounts where either the trustee or the trustor pertains to a person whose accounts, monetary instruments, or properties are the subject of the freeze order or order of inquiry;

Example:

Mr. Juan dela Cruz's account number CBSSA005 is listed in the NFO. Mr. dela Cruz also maintains accounts under: (1) SA number CBSSA006 in trust for his son, and (2) SA number CBSSA007 for the account of his mother.

Accounts CBSSA006 and CBSSA007 are considered materially linked accounts.

Under this scenario, the person subject of the NFO holds an account(s) in favor of or for the benefits of others.

e. All accounts held for the benefit or in the interest of the person whose accounts, monetary instruments, or properties are the subject of the freeze order or order of inquiry;

Example:

Mr. Juan dela Cruz is listed in the NFO. Mr. Andres Malong maintains account numbers CBSTD203 in trust for Mr. dela Cruz and CBSSA008 for the account of Mr. dela Cruz.

Both accounts of Mr. Malong under CBSTD203 and CBSSA008 are considered materially linked accounts.

Under this scenario, other persons (not listed in the NFO) maintain an account(s) in favor of or for the benefits of a person listed in the NFO.

f. All accounts or monetary instruments under the name of the immediate family or household members of the person whose accounts, monetary instruments or properties are the subject of the freeze order if the amount or value involved is not commensurate with the business or financial capacity of the said family or household member;

Example:

Mr. Juan dela Cruz is listed in the NFO. Mrs. Simeona dela Cruz, wife of Mr. dela Cruz, maintains account with the Bank as follows: (1) Account number CBSTD004, a time deposit with balance of P20M, and (2) SA number CBSSA009 with balance of P20,020.

CBSSA009 transaction movements showed regular transactions are payments of utilities (i.e., Meralco, PLDT, and Maynilad). Mr. Colet dela Cruz, son of Mr. Juan dela Cruz, maintains an account under CBSSA010 for educational expenses with a minimal balance of P2,019. Ms. Andreas Cacuchaba, a household helper of Mr. Juan dela Cruz, maintains a time deposit account under CBSTD005 with a balance of P5M.

Accounts CBSTD004and CBSTD005 are considered materially linked accounts.

Accounts CBSSA009 and CBSSAO10 are not considered materially-linked since the amount or values involved are commensurate with the financial capacity of the family or household members.

g. All accounts of juridical persons or legal arrangements that are owned, controlled or ultimately effectively controlled by the natural person whose accounts, monetary instruments or properties are subject of the freeze order or order of inquiry, or where the latter has ultimate effective control; and

Example:

Mr. Juan dela Cruz's account number CBSTD006 is listed in the NFO. JP Corporation's account number CBSTD007 is controlled (owned by 51% or more) by Mr. Juan dela Cruz. AM Corporation's account number CBSCA102 is 25% owned by Mr. dela Cruz but Mr. dela Cruz is a director and signatory of AM Corporation. JDC Corporation maintains an account under account number CBSSA011. Mr. dela Cruz owns 10% of JDC Corporation and sits as its Chief Operating Officer of the Company.

Account numbers CBSTD007, CBSCA102 and CBSSA011 are considered materially linked accounts.

Under this scenario, the determining factors to report the account as materially-linked are the extent of ownership and influence of the person subject of the freeze order over the corporate entities.

h. All other accounts, shares, units, or monetary instruments that is similar, analogous, or identical to any of the foregoing.

12.2 MONETARY INSTRUMENTS OR PROPERTY

12.2.1 **Monetary Instruments** shall refer, but not limited to the following:

a. Coins or currency of legal tender of the Philippines, or of any other country;

b. Credit instruments, including bank deposits, financial interest, royalties, commissions, and other intangible property;

c. Drafts, checks, and notes;

d. Stocks or shares, participation or interest in a corporation or in a commercial enterprise or profit-making venture and evidenced by a certificate, contract, instrument, whether written or electronic in character, including those enumerated in Section 3 of the Securities Regulation Code;

e. A participation or interest in any non-stock, non-profit corporation;

f. Securities or negotiable instruments, bonds, commercial papers, deposit certificates, trust certificates, custodial receipts, or deposit substitute instruments, trading orders, transaction tickets, and confirmations of sale or investments and money market instruments;

g. Contracts or policies of insurance, life or non-life, contracts of suretyship, pre-need plans, and member certificates issued by mutual benefit association; and

h. Other similar instruments where title thereto passes to another by endorsement, assignment, or delivery.

12.2.2 **Property** refers to anything or item of value, real or personal, tangible or intangible, or any interest therein, or any benefit, privilege, claim, or right with respect thereto, including:

1. Personal property, including proceeds derived therefrom or traceable to any unlawful activity, as herein defined, such as, but not limited to:

    a. Cash;
    b. Jewelry, precious metals and stones, and other similar items;
    c. Works of art, such as paintings, sculptures, antiques, treasures, and other similar precious objects;
    d. Perishable goods; and
    e. Vehicles, vessels, aircraft, or any other similar conveyance.

2. Personal property, used as instrumentalities in the commission of any unlawful activity, as herein defined, such as:

    a. Computers, servers, and other electronic information and communication systems; and
    b. Any conveyance, including any vehicle, vessel, and aircraft.

3. Real estate, improvements constructed or crops growing thereon, or any interest therein, standing upon the record of the registry of deeds or local government unit in the name of the party against whom the freeze order or asset preservation order is issued, or not appearing at all upon such records, or not belonging to the party against whom the freeze order or asset preservation order is issued and held by any other person, or standing on the records of the registry of deeds or local government unit in the name of any other person, but are:

    a. Derived from, or traceable to, any unlawful activity; or
    b. Used as an instrumentality in the commission of any unlawful activity, as herein defined.

12.2.3 **Monetary instrument or property related to unlawful activity** refers to:

a. All proceeds of an unlawful activity;

b. All instrumentalities of an unlawful activity, including all moneys, expenditures, payments, disbursements, costs, outlays, charges, accounts, refunds, and other similar items for the financing, operations, and maintenance of any unlawful activity;

c. All monetary instruments or property, including monetary, financial or economic means, devices, accounts, documents, papers, items, objects or things, used in or having any relation to any unlawful activity or money laundering, regardless of the current owner or possessor, and circumstances of ownership or acquisition; and

d. For purposes of freeze order and bank inquiry order: related and materially-linked accounts.

12.3 HANDLING OF FREEZE ORDER (FO)

Freeze Order refers to a provisional remedy aimed at blocking or restraining monetary instruments or properties in any way related to an unlawful activity, as herein defined, from being transacted, withdrawn, deposited, transferred, removed, converted, concealed, or otherwise moved or disposed without affecting the ownership thereof. FO shall be handled with utmost urgency and shall be prioritized above other tasks/activities handled by the Divisions/Departments/Branches/Units involved in the process.

12.3.1 **Freezing of Accounts or Properties of the Subject of Freeze Order and Readily Identified Related Accounts.** The following procedures shall be strictly observed in handling the accounts or properties of a person who is a subject of freeze order. *"Subject of Freeze Order"* shall refer to the named personalities and entities provided in the order whose accounts or properties are subject to freeze order.

1. Upon receipt of the Freeze Order by the Bank's General Services Department or any appropriate department where the order was served, the forthwith forwarding/delivery of such Freeze Order to the Legal Services Division will be of utmost priority, as the Order requires immediate freezing of the subject accounts. The AML Compliance Department of Compliance Division shall also be provided a copy.

2. The Legal Services Division shall immediately provide the names listed in the Freeze Order and instruct the Branch/Unit, where the accounts/properties are maintained, to immediately freeze without delay, the accounts identified in order to prevent withdrawal or closure prior to the implementation of the Freeze Order.

   The notice and instruction of the Legal Services Division shall also be addressed to all branches/units for the latter to conduct their own search to ensure that other accounts of the subject of freeze order or related/materially linked accounts are identified and accounted for.

Whenever an account or property can be immediately determined as a related account (*as defined in section 11.1 above*) with reasonable certainty, such related account shall be immediately subject to freeze;

3. The Head of the Branch/Unit shall cause the freezing of the accounts or properties immediately upon receipt of the Freeze Order instruction from the Legal Services Division, simultaneously reporting to the latter any/all accounts made subject to the freeze order and the details thereof.

   It should be pointed out that it is the responsibility of the concerned Branch/Unit to preliminary identify, assess and note should there be any 'related web of accounts' to be considered. Likewise, the concerned Branch/Unit shall also make a report if there are **no** accounts identified to be considered as 'related web of account' and the same shall be furnished to Compliance Division and Legal Services Division;

4. The Head of the Branch/Unit concerned shall, without undue delay, cause the furnishing of a copy of the freeze order upon the customer/owner or holder of the monetary instrument or property or related accounts subject thereof.

   In no case shall notice be given to the customer prior to the freezing of accounts or properties.

12.3.2 **Detection and Freezing of Related/Materially-linked Accounts.** A central unit shall be designated by the AML Committee to detect all accounts or properties falling within the definition of related and/or materially-linked account. In the absence of a formal designation by the AML Committee, the Branch Operations Division (BOD) or its equivalent will act as *de facto* central unit and custodian of the documents of accounts subject of freeze order.

Whenever the processing of freeze order and/or determination of related accounts is being handled by a designated central unit, all officers of the Branch/Unit shall extend their full cooperation in the determination of other related or linked accounts. Should the central unit be unreasonably prevented to identify such accounts, the responsible officers of the Branch/Unit shall be personally liable for any loss that may be incurred for failure to detect such other related or linked accounts.

The following procedures shall be strictly observed in handling investigation to detect related and/or materially-linked accounts as defined in *section 11.1*.

1. The designated central unit shall conduct its own investigation of the transactions of the customer who is a subject of freeze order and those whose accounts are readily determined as "related accounts" per *section 11.1*. The investigation shall cover identification of parties whose accounts have material/significant transaction with the subject of the freeze order or the related accounts initially identified, as well as those customers who are known to be directly related to the subject of freeze order or to related accounts already identified.

2. The transaction history of customers subjected to the freeze order shall be retrieved for determination of related accounts. The originator (for credits) and beneficiary (for debits) of each transaction shall be identified based on the information available in the system or available transaction and KYC documents.

3. If the freeze order specifically directs the freezing of related accounts and there are accounts related to the monetary instrument or property subject of the freeze order upon verification, the Branch/Unit Head shall immediately cause the freezing of these related accounts wherever these may be found. (reference: Section 4, Rule 10 of the 2018 RIRR of R.A. 9160, as amended)

4. If the related accounts cannot be determined within twenty-four (24) hours from receipt of the freeze order due to the volume and/or complexity of the transactions, or any other justifiable factors, the Bank shall effect the freezing of the related accounts within a reasonable period and shall submit a supplemental return thereof to the Court of Appeals and the AMLC within twenty-four (24) hours from the freezing of said related accounts. (reference: *Section 4, Rule 10 of the 2018 RIRR of R.A. 9160, as amended*)

5. The Head of the Branch/Unit shall, likewise, notify the owner or holder of a frozen related account on why the monetary instrument or property was considered as such, and furnish a copy of the freeze order, which was used as the basis for the freeze.

   In no case shall notice be given to the customer prior to the freezing of accounts or properties.

6. Relevant transactions of related accounts shall be reported to the AMLC as suspicious transactions. (reference: *Section 4, Rule 10 of the 2018 RIRR of R.A. 9160, as amended*)

7. Upon identification of all related accounts as a result of the investigation conducted, the designated central unit shall prepare a "Related Accounts Report" detailing the relationships of each related accounts identified to the subjects of the Freeze Order. The report shall be immediately provided to the AML Compliance Department of the Compliance Division for further validation.

   The Related Accounts Report of the designated central unit shall include a "Matrix" showing the relationships of the related accounts to the subjects of freeze order.

12.3.3 **Submission of a Detailed Return.** Within twenty-four (24) hours from receipt of the freeze order (*section 11.3.1*) or freezing of the related account (*section 11.3.2*), the Legal Services Division of the Bank shall cause the submission, by personal delivery, to the Court of Appeals and to the AMLC, a written detailed return on the freeze order.

The Bank, through the Legal Services Division, shall also submit to the AMLC, through the internet, an electronic detailed return in a format to be prescribed by the AMLC.

12.3.4 **Contents of the Detailed Return.** The detailed return on the freeze order shall specify all the pertinent and relevant information, which shall include the following:

1. The names of the account holders, personal property owners or possessors, or real property owners or occupants;
2. The value of the monetary instrument, property, or proceeds as of the time the assets were ordered frozen;
3. All relevant information as to the status and nature of the monetary instrument, property, or proceeds;
4. The date and time when the freeze order was served;
5. The basis for the identification as related accounts; and
6. The account numbers and/or description of the monetary instrument, property, or proceeds involved

12.3.5 **Lifting of Freeze Order.** The freeze order shall be deemed *ipso facto* lifted after six (6) months from the date of freezing of the account, unless a money laundering complaint against the person whose monetary instrument or property was frozen, or a petition for civil forfeiture against the frozen monetary instrument or property, has been filed, in which case the freeze order shall remain effective until the money laundering case is terminated or an asset preservation order is issued, respectively.

The lifting of the freeze order to an account is **NOT AUTOMATIC** after the expiration of the 6-month period. Prior to the expiration of the order, the designated central unit shall initiate, through the Legal Services Division, a written request for confirmation to the AMLC as to the lifting of the freeze order.

In no case shall the freeze status of the account subject to the freeze order be lifted without prior written confirmation from the AMLC.

12.3.6 **Handling of Customers Subject of Freeze Orders (FO)**

Filing of STR and Submission of KYC Documents

Branches/ Units shall file STR to all accounts subject of the Freeze Order and relevant transactions of identified Related or Materially-Linked accounts. STRs shall be promptly filed within the next working day from the occurrence thereof, which for purposes of this rule, shall be the date upon receipt of the Freeze Order. If the predicate crime of the freezing is based on any of the following, kidnapping for ransom; drug trafficking; hijacking; destructive arson and murder, including those perpetrated by terrorist against non-combatant persons and similar targets; terrorism and conspiracy to commit terrorism; and financing of terrorism, KYC documents shall be submitted to AMLC.

Individual/Entity Subject of Freeze Order

Names of individuals and entities subject of Freeze Order as well as customers identified to be related and materially-linked to a person subject of Freeze Order shall be included in the Internal Watchlist. The Authorized Personnel of the AML Compliance Department shall maintain a database of customers and accounts subject to Freeze Order. Legal Services Division shall likewise do a regular review of the status of the accounts of the subjects of freeze orders. The regular review shall be done not later than 6 months from the date of last review.

Further, the risk assessment of the customer subject of a freeze order or determined to be related or materially-linked to the subject of freeze order shall be automatically upgraded to high risk and immediate updating of customer's records shall be performed. Opening of additional account shall be automatically denied for those accounts subject to Freeze Order and those identified to be related and materially-linked to the subject of the Freeze Order.

The authorized officer of the AML Department shall conduct a review and validation to check the accuracy and completeness of the execution of the freeze order in the Bank's core banking system. Any findings and deviation from the policy shall be escalated to the AML Committee for appropriate action.

Retention or termination of client relationship for accounts with Freeze Order is dependent upon the approval or recommendation of the AML Committee. Should the AML Committee decided to close the accounts covered by Freeze Order subsequent to its lifting by the court, appropriate and proper approval of the authorized officers shall be secured.

12.4 HANDLING OF BANK INQUIRY (BI)

Notwithstanding the provisions of Republic Act No. 1405, as amended; Republic Act No. 6426, as amended; Republic Act No. 8791, and other laws, the AMLC may inquire into or examine any particular deposit or investment account, including related accounts, with any banking institution or non-bank financial institution, ***upon order by the Court of Appeals*** based on an ex parte application in cases of violation of the AMLA when it has been established that probable cause exists that the deposits or investments involved, including related accounts, are in any way related to an unlawful activity or money laundering offense.

The AMLC shall issue an ex parte order authorizing the AMLC Secretariat to inquire into or examine any particular deposit or investment account, including related accounts, with any banking institution or non-bank financial institution and their subsidiaries and affiliates when it has been established that probable cause exists that the deposits or investments involved, including related accounts, are in any way related to any of the following unlawful activities:

1. Kidnapping for ransom under Article 267 of Act No. 3815, otherwise known as the Revised Penal Code, as amended;

2. Sections 4, 5, 6, 8, 9, 10, 11, 12, 13, 14, 15 and 16 of Republic Act No. 9165, otherwise known as the Comprehensive Dangerous Drugs Act of 2002;

3. Hijacking and other violations under Republic Act No. 6235; destructive arson and murder, as defined under the Revised Penal Code, as amended;

4. Felonies or offenses of a nature similar to those mentioned in Rule 11, Sections 2.1 (a), (b) and (c), which are punishable under the penal laws of other countries;

5. Terrorism and conspiracy to commit terrorism as defined and penalized under Republic Act No. 9372; and

6. Financing of terrorism under Section 4 and offenses punishable under Sections 5, 6, 7 and 8 of the TFPSA.

In the course of a periodic or special examination of covered persons under its supervision and/or regulation, the BSP may inquire into or examine bank accounts, including customer identification, account opening, and transaction documents, for the purpose of checking compliance with the requirements of the Anti-Money Laundering Act and Terrorism Financing Prevention and Suppression Act, their respective IRR, and other AMLC issuances.

The AML/CTF findings that fall within the parameters set by the AMLC shall be referred by the BSP to the AMLC for evaluation and filing of an administrative case, if warranted, against the covered person and its responsible directors, officers and employees.

12.4.1 **Bank Inquiry requesting customer information and documents.** Upon receipt of a Bank Inquiry, the following guidelines shall be strictly observed:

1. The Authorized Personnel of the AML Compliance Department of the Compliance Division shall stamp the received Bank Inquiry to signify the date and exact time of receipt;

   In case the Bank Inquiry is initially received by other units, it shall be forwarded to the AML Compliance Department within twelve (12) hours from the time of actual receipt;

2. The Authorized Personnel shall make an immediate search through the Finacle Core Banking System (FCBS) or the source system to identify the Branch/Unit where the accounts inquired are maintained.

   In extreme circumstances when the Branch/Unit of account cannot be identified, the Authorized Personnel shall forward the unidentified accounts to the BSOMD or other units (for head office units) for determination;

3. The Authorized Personnel of the AML Compliance Department shall obtain the customer records from the DIGICUR system.

   The authorized officer/delegate of BSOMD shall sign the documents as certified true copy. For other business units, CTC are signed by the business unit's designated officers.

4. AML Compliance Department may also request for transaction documents from BSOMD should the need arise.

5. After gathering the necessary documents, the Authorized Personnel of the AML Compliance Department shall prepare a draft reply to the letter of the AMLC. The draft reply shall provide reference to the AMLC letter and previous responses, if any.

6. Certified true copies of the documents pertaining to deposit, investment, account and/or transaction subject of the bank inquiry shall be submitted to the AMLC Secretariat, within five (5) working days from receipt of the court order or notice of AMLC Resolution.

7. The Branch/Unit shall keep the confidentiality of the inquiry, and ensure that the owner of any monetary instrument or property or other unauthorized personnel shall not be informed about the inquiry, to prevent tipping-off.

12.4.2 **Authority of the AMLC to Examine.** The Bank Inquiry or a separate letter by the AMLC may also include authority to personally appear and examine the said records. The AMLC may conduct a visit to the Bank or its branches/units to personally conduct the review. In such case, the AML Compliance Department shall coordinate the assistance and logistics needed for the conduct of the examination by the AMLC.

The Bank/Branch/Unit shall give the authorized personnel of the AMLC, full access to all information, documents or objects pertaining to the account, transaction and/or person subject of the investigation immediately upon receipt of the request or order (reference: *Rule 8 of the 2018 AMLA RIRR*);

The Bank/Branch/Unit shall submit **within five (5) working days** from receipt of the request or order from the AMLC, certified true copies of the documents pertaining to account, transaction and/or person subject of the investigation (reference: *Rule 8 of the 2018 AMLA RIRR*) and;

All Personnel shall keep the confidentiality of the investigation and ensure that the owner of any monetary instrument or property, or other unauthorized personnel, shall not be informed about the investigation, to prevent **tipping-off** (reference: *Rule 8 of the 2018 AMLA RIRR*).

12.5 ASSET PRESERVATION ORDER (APO)

Upon verified petition by the AMLC, with prayer for issuance of asset preservation order, and after determination that probable cause exists that any monetary instrument or property is in any way related to an unlawful activity, the Regional Trial Court may issue an asset preservation order, in accordance with the "Rule of Procedure in Cases of Civil Forfeiture, Asset Preservation, and Freezing of Monetary Instrument, Property, or Proceeds Representing, Involving, or Relating to an Unlawful Activity or Money Laundering Offense under Republic Act No. 9160, as Amended" (A.M. No. 05-11-04-SC), which shall be effective immediately, forbidding any transaction, withdrawal, deposit, transfer, removal, conversion, concealment or other disposition of the subject monetary instrument or property.

(APO) refers to a provisional remedy aimed at preserving monetary instruments or properties in any way related to an unlawful activity or money laundering offense defined herein, during the pendency of civil forfeiture proceedings.

Upon receipt of the APO, the Authorized Personnel of the Branch/Unit shall immediately implement asset preservation order issued by the appropriate Court with regards to the monetary instruments or properties in the Branch/Unit custody. The Branch/Unit, through the Legal Services Division, shall likewise comply with the required detailed returns for the said court orders.

12.6 DATABASE FOR CUSTOMERS SUBJECT TO BANK INQUIRY AND FREEZE ORDER

The Authorized Personnel of the AML Compliance Department shall maintain a database of customers and accounts subject to Bank Inquiry and Freeze Oder. The listing will be used in the updating of internal watchlist. The listing

shall also include the identified related and/or materially-linked accounts, whether or not such determination led to the freezing of such accounts.

12.7 RECORD-KEEPING STANDARD

Original and certified true copies of the order, inquiry, CDD documents and all other correspondences and analysis pertaining to accounts subject to inquiry or freeze order shall be retained upon final resolution of the related case or five (5) years **whichever is later**.

12.8 THE ANTI-FINANCIAL ACCOUNT SCAMMING ACT

On July 20, 2024, President Marcos signed into law R.A. 12010 or the Anti-Financial Account Scamming Act (AFASA). In the Declaration of Policy, the State recognizes the vital role of banks, non-bank financial institutions, other payment service providers, and the general banking public in maintaining a stable financial system. Furthermore, with the increased use of digital financial services, there is a need to promote awareness on the proper use of Financial Accounts, and to protect the public from cybercriminals and criminal syndicates.

Prohibited Acts and their Penalties

Prohibited Act/Offense	Penalties
Money Muling Activities 1. Using, borrowing, or allowing the use of a Financial Account 2. Opening a Financial Account under a fictitious name or using the identity or identification documents of another 3. Buying or renting a Financial Account 4. Selling or lending a Financial Account 5. Recruiting, enlisting, contracting, hiring, utilizing or inducing any person to perform the above acts.	Imprisonment of not less than 6 years, but not more than 8 years, **or** a fine of at least PHP 100,000 but not exceeding PHP 500,000, **or** both at the discretion of the Court. For items #1-4, the court shall also order the closure of the **Financial Account** involved, and forfeiture.
Social Engineering Schemes 1. Misrepresenting oneself as acting on behalf of an Institution or making false representations to solicit another person's sensitive identifying information or 2. Using electronic communications to obtain another person's sensitive identifying information	Imprisonment of not less than 10 years but not more than 12 years, **or** a fine of at least PHP 500,000 but not exceeding PHP 1,000,000, **or** both at the discretion of the court. *Provided,* that the penalty of not less than 12 years but not more than 14 years of imprisonment, **or** a fine of at least PHP 1,000,000 but not exceeding PHP 2,000,000 **or** both at the discretion of the court, shall be imposed if the target is a **senior citizen at the time the offense was committed.**
Economic Sabotage – Money Muling Activities and Social Engineering Schemes shall be considered economic sabotage when it is committed:	**Life imprisonment**, **or** a fine of not less than PHP 1,000,000 but not exceeding PHP 5,000,000 **or** both at the discretion of the court.

1. By a group of three or more persons conspiring or confederating with one another 2. Against 3 or more persons individually or as a group 3. Using a mass mailer (refers to a service or software used to send electronic communications to an aggregate of 50 or more recipients 4. Through human trafficking	
Other Offenses 1. Willfully aiding or abetting in the commission of any of the above offenses (Money Muling Activities, Social Engineering Schemes, Economic Sabotage) 2. Willfully attempting to commit any of the above offenses 3. Opening a Financial Account under a fictitious name or using the identity or identification documents of another 4. Buying or selling a Financial Account.	Imprisonment of not less than 4 years but not more than 6 years **or** a fine of at least PHP 100,000 but not exceeding PHP 200,000 **or** both, at the discretion of the court. The court shall also order the **closure of the financial account** If the prohibited acts falls under #3 and #4

Responsibility of the Bank to Protect Access to Client's Financial Account

Institutions shall ensure that access to their clients' Financial Account is protected by adequate risk management systems that are proportionate and commensurate to the nature, size, and complexity of their operations. Institutions shall be liable for restitution of funds to Account Owners for failure to employ adequate risk management systems or failure to exercise the highest degree of diligence**.** Conviction is not a prerequisite to restitution of funds.

Temporary Holding of Funds Subject of a Disputed Transaction

Institutions have the authority to temporarily hold funds subject of a disputed transaction within the period prescribed by the BSP, which shall not exceed 30 calendar days, unless otherwise extended by a court of competent jurisdiction. *Provided,* Institutions shall also notify BSP whenever it temporarily holds the funds.

The BSP shall issue rules and regulations on the temporary holding of funds. No liability shall be imposed against an Institution or its directors, trustees, officers, and employees for holding funds subject of a disputed transaction, when done in accordance with BSP rules and regulations.

Upon receipt of a complaint, an information from another Institution, or detection through a Fraud Management System, the Institutions and Account Owners shall initiate a **coordinated verification process** to validate the disputed transaction. The provisions of the "Foreign Currency Deposit Act of the Philippines", Revised Non-Stock Savings and Loan Association Act of 1997, and "Data Privacy Act of 2012" shall not apply during this coordinated verification process.

Penalties Related to the Temporary Holding of Funds

If an Institution fails to temporarily hold funds subject of a disputed transaction, it shall be liable for loss or damage, including the restitution of the disputed funds. On the other hand, an Institution that holds funds subject of a disputed transaction beyond the allowable period, or improperly holds funds, shall be subject to administrative action under "The New Central Bank Act." Likewise, any person who, in malice or in bad faith, reports or files unwarranted or false information that results in the temporary holding of funds shall be penalized with imprisonment of not less than 1 year but not more than 5 years, or a fine of not less than PHP 50,000, but not exceeding PHP 200,000, or both, at the discretion of the court.

Investigation and Inquiry into Financial Accounts

The BSP shall have the authority to investigate and inquire into Financial Accounts which may be involved in the commission of Prohibited Acts and Other Offenses. The provisions of RA 1405, as amended, "Foreign Currency Deposit Act of the Philippines," Revised Non-Stock Savings and Loan Association Act of 1997, and "Data Privacy Act of 2012" shall not apply to Financial Accounts subject of BSP's investigation. No court below the Court of Appeals shall have jurisdiction to enjoin the BSP from exercising its authority to investigate and inquire.

Without prejudice to the authority of the cybercrime units of the National Bureau of Investigation and the Philippine National Police, the BSP or its duly authorized officer or body shall have the authority to apply for cybercrime warrants and to issue the orders provided in the "Cybercrime Prevention Act of 2012," with respect to

Civil Liability in case of Conviction and Administrative Sanctions

Independent of a criminal case, all properties, tools, instruments, and/or any other non-liquid assets used for the commission of the acts prohibited in Sections 4 and 5 shall be subject to civil forfeiture, upon finding of probable cause. *Provided,* that in cases of economic sabotage, the rules shall include a summary procedure for the release of a portion of such assets to the Department of Justice upon ex-parte motion for operational support and victim protection, including victims of human trafficking involved in the commission of prohibited acts and other offenses.

Administrative sanctions in RA 7643 shall also be imposed upon the Institution, its directors, officers, trustees, employees, or agents, for violation of this Act or any other regulations of the BSP.

PART XIII
CUSTOMER RECORDS UPDATING AND RECORD KEEPING

PART XIII: CUSTOMER RECORDS UPDATING AND RECORD KEEPING

All customer identification records shall be maintained and safely stored as long as the account exists. Records and files shall contain the full and true identity of the owners or holders of the accounts involved in the transactions such as the ID card and photo of individual customers and the related documents.

All transaction records shall be maintained and safely stored for five (5) years from the date of transaction.

13.1 UPDATING OF CUSTOMER RECORDS

13.1.1 Client account opening documents (Client Information Sheet, Signature Card, and Identification Documents, etc.) of the active accounts shall be updated gradually based on risk materiality:

a) Low Risk Client - At least every 3 years
b) Normal Risk Client - At least every 2 years
c) High Risk Client - At least yearly

13.1.2 Updating of customer records (including ECRAF) shall be immediately performed whenever material information not previously known or provided has become available. The material information may come from the review of daily transactions or the presence of profile or transaction indicators per ECRAF policy.

13.1.3 The risk assessment of the customer shall be automatically upgraded to **high risk**, and immediate updating shall be performed in any of the following:

a. The customer is a subject of a freeze order or determined to be related or materially-linked to the subject of freeze order;
b. The customer is a subject of an AMLC or regulatory inquiry or determined to be related or materially-linked to the subject of the inquiry;
c. The customer is in a way involved in unlawful activity or determined to be related or materially-linked to the person involved in unlawful activity. The source is decision by the court;
d. The customer is the subject of suspicion of an STR previously filed;
e. The customer is a subject of negative news report pertaining to violations of AMLA or any predicate crime;
f. The customer is a subject of negative information that is publicly known or known to the reviewing branch/unit officers;
g. Presence of information relating to the client or representative or future use of the account that may be reasonably received to be detrimental to the Bank's reputation;
h. The account of the customer is expected to be used by the client to service high volume deposits or remittances or fund transfers for a future project/business;
i. The transactions in the account are not consistent with the customer's historical transactions, without official/public/acceptable private document supporting the source of funds and purpose of the transaction;

j. The transactions in the account are not consistent with the profile of the client, without official/public/acceptable private document supporting the source of funds and purpose of the transaction;
k. The transaction is actually or suspected to be related to an unlawful activity;
l. Frequent (*at least 3 transactions of any combination*) outward or inward remittance to/from a High Risk country;
m. Other transactional event that is not normal considering both the history and profile of the customer, without official/public/acceptable private document supporting the source of funds and purpose of the transaction.

13.1.4 Whenever there's investigation for filing of STR and such updating will "tip-off" the customer, the Authorized Personnel of the branch or unit shall refrain from requesting additional documents and/or information, and shall complete the due diligence based on the records of the customer at hand.

13.2 RETENTION OF ORIGINAL RECORDS

13.2.1 All customer identification records of the Bank, which contains the relevant documents that would establish the true and full identity of the account holders, beneficial owners, beneficiaries and authorized representatives, shall be retained for as long as the account exist and for at least five (5) years after closure of the account. The documentation of the nature and complexity of the business, purpose, analysis, correspondences and approval leading to the acceptance, continuance or termination of the business relationship shall likewise be retained as such.

13.2.2 Transaction documents which includes transaction tickets/forms and transaction history, including supporting documents, analysis, correspondences and approvals shall be maintained and safely stored for a minimum of five (5) years from the date of transaction or in accordance with the Bank's retention policy, whichever is longer.

13.2.3 Hard copies of the suspicious transactions report including the supporting documents, analysis, correspondences and approvals shall be maintained and safely stored for a minimum of five (5) years from the date of filing of such report to the Anti-Money Laundering Council (AMLC).

Soft copies of covered and suspicious transactions report shall be retained for at least five (5) years from the date of submission to the AMLC.

13.2.4 Records shall be retained as originals in such forms as are admissible in court pursuant to existing laws and the applicable rules promulgated by the Supreme Court.

13.3 CUSTOMER OR ACCOUNT IS A SUBJECT OF A COURT CASE

If a money laundering case has been filed in court involving the account or customer, records must be retained and safely kept beyond the five (5)-year retention period, until it is officially confirmed by the AMLC Secretariat that the case has been resolved, decided or terminated with finality.

13.4 SAFEKEEPING OF RECORDS AND DOCUMENTS

The Branch Operations Head and Branch Service Head or their equivalent in case of business units & support units shall be jointly responsible and accountable in the safekeeping of all records and documents required to be retained by the AMLA, as amended, its RIRR and this MTPP. They shall have the obligation to make these documents and records readily available without delay during BSP regular or special examinations.

13.5 DIGITIZATION OF CUSTOMER RECORDS

The Bank shall implement the digitization of all customer records on all accounts opened through the eKYC System wherein a central database of customer records is maintained.

The Authorized Personnel of all business units shall ensure that central database retrieval procedures of all customer records are compliant with prevailing laws related to data privacy, data protection and security.

The authorized AML Compliance Officer/s shall have a direct, immediate and unimpeded access to the database for purposes of acting promptly with utmost confidentiality all requests for information and/or documents, as well as orders to provide customer records pursuant to the AMLC's function to investigate or conduct bank inquiry. The AML Compliance Department shall ensure complete, accurate, timely and secure submission of customer records, in accordance with the Implementing Rules and Regulations of the AMLA, as amended and other AMLC issuances.

Further, the digitization of customer records shall be without prejudice to the Bank's compliance with record-keeping and retrieval requirements under AMLA, as amended and its Implementing Rules and Regulations, resolutions, directives and other issuances of the AMLC.

13.6 GUIDELINES ON DIGITIZATION OF CUSTOMER RECORDS

13.6.1 SharePoint locations

The central database of all scanned KYC documents shall be Digicur Project site in SharePoint (https://chinabankph.sharepoint.com/sites/DigicurProject).

Within the site, there are three sub-sites for each category:

1. APD Lending
   https://chinabankph.sharepoint.com/sites/DigicurProject/APD

2. Treasury Operations Division
   https://chinabankph.sharepoint.com/sites/DigicurProject/TOD

3. Branch Banking Group
   https://chinabankph.sharepoint.com/sites/DigicurProject/BBG

13.6.2 File Properties and Drop Off Library

1. The standard file name format of the uploaded KYC documents shall be:
    a. Branches and TOD <CIF ID_CustomerName_DocumentCode>
    b. APD-LOD < CIF ID_Account/PN Number_CustomerName_DocumentCode>

2. The uploaded KYC documents shall be in PDF format. Setting for scanning of documents must be at "100 x 100 dpi" resolution to keep the file at minimum acceptable quality.

3. Drop Off library, located in the SharePoint shall contain folder based on the SOL ID assigned to the user (as a Maker/Checker). The following are the predefined folders inside the SOL ID folder:
    a. Corporate – where KYC documents of business and/or juridical entity are stored and saved.
    b. Retail – where KYC documents of individual customers including signatories of a corporate account are stored and saved.
    c. Identification (ID) Card – where the ID card of the individual customers is stored and saved.

4. A system generated email notification shall be sent to the approver for any request for approval for the uploaded KYC documents.

5. Any request for parameter set-up, issues, and configuration for the central database (SharePoint) shall be documented and course through to BPMD-SDSD.

6. PCCI shall generate and upload all Customer Information and Account File in the SharePoint daily.

13.6.3 Procedures

1. Uploading KYC Documents to the Sync Library
   Maker
   1.1. After scanning the KYC documents, opens the sync folder of the Drop Off Library.
   1.2. Click the assigned SOL ID folder.
   1.3. Open the appropriate folder to upload the scanned KYC documents.
   1.4. Check if the status icon has a green mark.
   1.5. If with green check, rename the uploaded KYC documents based on standard file name format. Otherwise, wait until the green check appear or re-upload the KYC documents.

2. Indexing of KYC documents
   Maker
   2.1. Once the status of uploading of KYC documents is completed, select the file to submit for indexing[10].
   2.2. Clicks the "Submit for Indexing" button[11].
   2.3. Navigates to Indexing from the left sidebar menu in the Group Homepage.
   2.4. Opens the CIF ID Folder of the document for indexing.

[10] Maker can submit the KYC documents for indexing in multiple/bulk.
[11] An alert box will display to notify the user that it was successful.

2.5. Selects the document and click the ellipsis icon.
2.6. Clicks "More" and "Properties" button[12].
2.7. Clicks "Edit all" button[13].
2.8. Populates the index such as Account No., Expiration Date, ID No. etc. and hits "Save" button.
2.9. Selects the files to submit for approval[14].
2.10. Clicks the "Submit for Approval" button[15].

Approver

2.11. Upon receipt of the email notification, accesses "Approval Library" from the left sidebar menu.
2.12. Opens the "CIF ID folder" for the document/s to be approved.
2.13. Selects and opens the documents.
2.14. Checks the correctness and completeness of the uploaded scanned KYC documents.
2.15. If in order, clicks the "Approve" button. Otherwise, clicks the "Reject" button and informs the maker to take necessary actions[16].

Note: Approver can approve the uploaded KYC documents in multiple/bulk.

[12] Properties pane will show up to the right side.
[13] The view will change to the edit form.
[14] Maker can submit the KYC documents for approval in multiple/bulk.
[15] An alert box will display to notify the user that the process is successful. Simultaneously, an email notification shall be sent to the approver for the request of approval.
[16] Approver can approve the uploaded KYC documents in multiple/bulk.

PART XIV
COOPERATION WITH REGULATORS AND GOVERNMENT AUTHORITIES

PART XIV: COOPERATION WITH REGULATORS AND GOVERNMENT AUTHORITIES

The Bank Management hereby enjoins all units of the Bank to extend full cooperation with the Anti-Money Laundering Council (AMLC) in the proper implementation of the UARR under BSP Cir. No. 706 dated January 5, 2011, BSP Cir. No. 950 dated March 15, 2017, and BSP Cir. 1022 dated November 26, 2018, AMLA, as amended, and its RIRR and the Bank's MTPP.

Likewise, to ensure genial relation with the AMLC and the BSP, the Bank shall designate the Chief Compliance Officer as its link with the said institutions.

AMLC AND BSP AUTHORITY TO EXAMINE DEPOSITS AND INVESTMENTS

The authority of AMLC to inquire into or examine the main account and the related accounts shall strictly comply with the requirements of Republic Act No. 9160, as amended by Republic Act No. 9194, 10167, 10365 and 10927, its Revised Implementing Rules and Regulations and the BSP Circular No. 706, 950 and 1022 which are hereby incorporated for reference.

In the course of a periodic or special examination, the BSP may inquire into or examine bank accounts including customer identification, account opening and transaction documents for the purpose of checking compliance with the requirements of the Anti-Money Laundering Act and Terrorist Financing Prevention and Suppression Act, their respective Implementing Rules and Regulations and other AMLC issuances.

PART XV
SANCTIONS AND PENALTIES

PART XV: SANCTIONS AND PENALTIES

15.1 IMPOSITION OF ADMINISTRATIVE SANCTIONS

The Anti-Money Laundering Council "Rules of Procedure in Administrative Sanctions (RPAC) under R.A. 9160 (AMLA), as amended" imposes and/or re-calibrates penalties and other administrative measures such as fines, reprimands, or warnings on specified violations of AMLA.

The violations may be triggered by compliance issues surfaced in the course of money laundering investigation or regular checking functions of the Compliance Unit of the AMLC Secretariat (Report of Compliance), or Supervising Authorities of the BSP (Report of Examination).

Assessments shall be in amounts as may be determined by the AMLC to be appropriate, which shall not be more than Five Hundred Thousand Pesos (Php500,000.00) per violation. In no case shall the aggregate assessment exceed five percent (5%) of the asset size of the respondent based on its audited financial statements as of the year of the compliance testing covered by the sampled data. If the violations were committed over several years, as of the last year of violation covered by the sampled data during the compliance testing will serve as basis. Otherwise, the audited financial statements used by the supervising authorities shall be the basis of the respondent's asset size.

The following is a summary of the types of violation and the corresponding penalties applicable to Covered Persons depending on: (a) gravity of violation as to grave, major, serious, less serious and light serious; (b) other circumstances e.g., concealment, misrepresentation, voluntary disclosure, corrective measure/s taken; and (c) nature of the violation. The following are the specific violations and their corresponding sanctions:

A. The following are the specific violations and their corresponding sanctions based on the entity size and gravity of violations:

TABLE A:

A. GRAVE VIOLATION					
Administrative Sanctions					
	Micro	**Small**	**Medium**	**Large A**	**Large B**
Minimum	₱25,000 per violation, but not exceeding ₱1 Million	₱62,500 per violation, but not exceeding ₱2.5 Million	₱125,000 per violation, but not exceeding ₱5 Million	₱187,500 per violation, but not exceeding ₱7.5 Million	₱250,000 per violation, but not exceeding ₱10 Million
Medium	₱37,500 per violation, but not exceeding ₱1.5 Million	₱93,750 per violation, but not exceeding ₱3.75 Million	₱187,500 per violation, but not exceeding ₱7.5 Million	₱281,250 per violation, but not exceeding ₱11 Million	₱375,000 per violation, but not exceeding ₱15 Million
Maximum	₱50,000 per violation, but not exceeding ₱2 Million	₱125,000 per violation, but not exceeding ₱5 Million	₱250,000 per violation, but not exceeding ₱10 Million	₱375,000 per violation, but not exceeding ₱15 Million	₱500,000 per violation, but not exceeding ₱20 Million
1.	Non-compliance with the requirement to immediately freeze, upon receipt of the notice of the Freeze Order (FO), Provisional Asset Preservation Order (PAPO), and Asset Preservation Order (APO), the			Assessment is on per Resolution (FO) or Order (PAPO, APO) basis, plus restoration, whenever applicable.	

	monetary instrument or property identified in the FO, and related accounts, the PAPO and the APO.	
2.	Lifting the effects of the FO, PAPO, and/or APO during its effectivity.	Assessment is on a per account basis, plus restoration, whenever applicable.
3.	Non-compliance with the requirement to immediately give the AMLC and/or its Secretariat full access to all information, documents or objects pertaining to the deposit, investment, account, transaction, and/or person subject of inquiry or investigation.	Assessment is on a per account basis.
4.	Non-compliance with the Guidelines on Digitization of Customer Records.	Assessment is on a per customer basis.

B. MAJOR VIOLATION

Administrative Sanctions

	Micro	Small	Medium	Large A	Large B
Minimum	₱15,000 per violation, but not exceeding ₱500 Thousand	₱37,500 per violation, but not exceeding ₱ 1.5 Million	₱75,000 per violation, but not exceeding ₱2.5 Million	₱112,500 per violation, but not exceeding ₱3.5 Million	₱150,000 per violation, but not exceeding ₱5 Million
Medium	₱22,500 per violation, but not exceeding ₱750 Thousand	₱56,250 per violation, but not exceeding ₱2 Million	₱112,500 per violation, but not exceeding ₱3.5 Million	₱168,750 per violation, but not exceeding ₱5.5 Million	₱225,000 per violation, but not exceeding ₱7.5 Million
Maximum	₱30,000 per violation, but not exceeding ₱1 Million	₱75,000 per violation, but not exceeding ₱2.5 Million	₱150,000 per violation, but not exceeding ₱5 Million	₱225,000 per violation, but not exceeding ₱7.5 Million	₱300,000 per violation, but not exceeding ₱10 Million

1.	Non-compliance with the requirement to obtain all information to establish and record the true identity of each customer and/or the person on whose behalf the transaction is being conducted.	Assessment is on a per customer basis.
2.	Non-compliance with the requirement to retain and safely keep records beyond the five (5)-year period, where the account is the subject of a case, until it is officially confirmed by the AMLC Secretariat that the case has been resolved, decided or terminated with finality.	Assessment is on a per account basis.
3.	Non-compliance with the requirement to report to the AMLC suspicious transactions.	Assessment is on a per account or suspicious transaction report (STR) basis.

C. SERIOUS VIOLATION

Administrative Sanctions

	Micro	Small	Medium	Large A	Large B
Minimum	₱10,000 per violation, but not exceeding ₱100 Thousand	₱25,000 per violation, but not exceeding ₱250 Thousand	₱50,000 per violation, but not exceeding ₱500 Thousand	₱75,000 per violation, but not exceeding ₱750 Thousand	₱100,000 per violation, but not exceeding ₱1 Million
Medium	₱15,000 per violation, but not exceeding ₱250 Thousand	₱37,500 per violation, but not exceeding ₱750 Thousand	₱75,000 per violation, but not exceeding ₱1.5 Million	₱112,500 per violation, but not exceeding ₱2 Million	₱150,000 per violation, but not exceeding ₱2.5 Million
Maximum	₱20,000 per violation, but not	₱50,000 per violation, but not	₱100,000 per violation, but not	₱150,000 per violation, but not	₱200,000 per violation, but not

		exceeding ₱500 Thousand	exceeding ₱1 Million	exceeding ₱2.5 Million	exceeding ₱3.75 Million	exceeding ₱5 Million
1.	Non-compliance with the requirement to conduct institutional risk assessment.				Assessment is on a per examination basis.	
2.	Non-compliance with the requirement to formulate a Money Laundering / Terrorism Financing Prevention Program (MTPP).				Assessment is on a per examination basis.	
3.	Allowing the opening of anonymous accounts, accounts under fictitious names, and all other similar accounts.				Assessment is on a per account basis.	
4.	Allowing the opening of checking numbered accounts.				Assessment is on a per account basis.	
5.	Non-compliance with the requirements on "Customer Verification Process."				Assessment is on a per customer basis.	
6.	Non-compliance with the requirement to obtain more than three (3) but not all information to establish and record the true identity of each customer and/or the person on whose behalf the transaction is being conducted.				Assessment is on a per customer basis.	
7.	Non-compliance with the requirements on "Identification and Verification of Agents."				Assessment is on a per customer or on a per account basis, as the case may be.	
8.	Non-compliance with the requirements on "Beneficial Ownership Verification."				Assessment is on a per account basis.	
9.	Non-compliance with the requirements on "Determination of the Purpose of Relationship."				Assessment is on a per account basis.	
10.	Non-compliance with the requirements on "Ongoing Monitoring Process."				Assessment is on a per account basis.	
11.	Non-compliance with the requirement to Risk Profile customers.				Assessment is on a per customer basis.	
12.	Non-compliance with the requirements on "Life Insurance and Other Investment-related Insurance Policies."				Assessment is on a per customer basis.	
13.	Non-compliance with the requirements of the provisions on "Politically-Exposed Persons."				Assessment is on a per customer basis.	
14.	Non-compliance with the requirements of the provisions on "Correspondent Banking."				Assessment is on a per transaction basis.	
15.	Non-compliance with the requirements on "New Technologies."				Assessment is on a per examination basis.	
16.	Non-compliance with the requirements of the provisions on "Wire Transfers", including the requirements on "Money or Value Transfer Services Provider" and "Implementation of Targeted Financial Sanctions."				Assessment is on a per transaction basis.	
17.	Non-compliance with the requirements of the provisions on "Shell Bank, Shell Company and Bearer Share Entity."				Assessment is on a per transaction basis.	
18.	Non-compliance with the requirements of the provisions on "High-Risk Jurisdiction or Geographical Location."				Assessment is on a per customer basis.	
19.	Non-compliance with the requirements of the provisions on Foreign Branches and Subsidiaries.				Assessment is on a per examination basis.	
20.	Non-compliance with the requirement to establish a transaction monitoring system.				Assessment is on a per examination basis.	
21.	Non-compliance with the requirement to maintain and safely store for five (5) years from the dates of transactions, or from dates the accounts were closed, all records of transactions, including customer identification documents.				Assessment is on a per account basis.	

22.	Non-compliance with the requirement to register with the AMLC's electronic reporting system within the prescribed period.	Assessment is on a per examination basis.
23.	Non-compliance with the requirement to secure a written confirmation from the AMLC before the expiration of the freeze order.	Assessment is on a per account basis, plus restoration in cases where there is civil forfeiture or money laundering case filed and the monetary instruments were withdrawn, transferred or dissipated.
24.	Non-compliance with the requirement to submit certified true copies of the documents pertaining to deposit, investment, account, transaction, and/or person subject of inquiry or investigation, within five (5) working days from receipt of the court order or AMLC Resolution.	Assessment is on a per account basis.
25.	All other violations of orders, resolutions and other issuances of the AMLC.	Assessment is on a per resolution, rule, regulation, circular, order and guideline basis.

D. LESS SERIOUS VIOLATION

Administrative Sanctions

	Micro	**Small**	**Medium**	**Large A**	**Large B**
Minimum	₱5,000 per violation, but not exceeding ₱50 Thousand	₱12,500 per violation, but not exceeding ₱125 Thousand	₱25,000 per violation, but not exceeding ₱250 Thousand	₱37,500 per violation, but not exceeding ₱375 Thousand	₱50,000 per violation, but not exceeding ₱500 Thousand
Medium	₱7,500 per violation, but not exceeding ₱75 Thousand	₱18,750 per violation, but not exceeding ₱200 Thousand	₱37,500 per violation, but not exceeding ₱375 Thousand	₱56,250 per violation, but not exceeding ₱550 Thousand	₱75,000 per violation, but not exceeding ₱750 Thousand
Maximum	₱10,000 per violation, but not exceeding ₱100 Thousand	₱25,000 per violation, but not exceeding ₱250 Thousand	₱50,000 per violation, but not exceeding ₱500 Thousand	₱75,000 per violation, but not exceeding ₱750 Thousand	₱100,000 per violation, but not exceeding ₱1 Million

1.	Non-compliance with the other requirements on the contents of the MTPP (Insufficient Contents). Where the basis of the Major and Serious Violations are absence of MTPP provisions, in such case, the penalty under such violations will apply.	Assessment is on a per examination basis.
2.	Non-compliance with the requirement on "Continuing Education and Training Program."	Assessment is on a per examination basis.
3.	Non-compliance with less than three (3) of the required information to establish and record the true identity of each customer and/or the person on whose behalf the transaction is being conducted.	Assessment is on a per account basis.
4.	Non-compliance with the requirement to obtain at least three (3) criteria for risk profiling (Deficient Risk Profiling Mechanism).	Assessment is on a per account basis.
5.	Non-compliance with the requirement to indicate the true name of the account holder in covered transaction reports (CTRs) and STRs involving non-checking numbered accounts.	Assessment is on a per transaction basis.
6.	Non-compliance with the requirement on the accuracy and completeness of covered and suspicious transactions reports.	Assessment is on a per transaction basis.
7.	Non-compliance with the requirement to submit to the AMLC within twenty-four (24) hours from receipt of the freeze order a detailed written return on the accounts subject of the freeze order. For related	Assessment is on a per Resolution (FO) basis.

	accounts, the twenty-four (24) hours shall be reckoned from the determination thereof.	

E. LIGHT VIOLATION					
Administrative Sanctions					
	Micro	**Small**	**Medium**	**Large A**	**Large B**
Minimum	₱2,500 per violation, but not exceeding ₱25 Thousand	₱6,250 per violation, but not exceeding ₱50 Thousand	₱12,500 per violation, but not exceeding ₱125 Thousand	₱18,750 per violation, but not exceeding ₱150 Thousand	₱25,000 per violation, but not exceeding ₱250 Thousand
Medium	₱3,750 per violation, but not exceeding ₱37.5 Thousand	₱9,375 per violation, but not exceeding ₱100 Thousand	₱18,750 per violation, but not exceeding ₱150 Thousand	₱28,125 per violation, but not exceeding ₱250 Thousand	₱37,500 per violation, but not exceeding ₱375 Thousand
Maximum	₱5,000 per violation, but not exceeding ₱50 Thousand	₱12,500 per violation, but not exceeding ₱125 Thousand	₱25,000 per violation, but not exceeding ₱250 Thousand	₱37,500 per violation, but not exceeding ₱350 Thousand	₱50,000 per violation, but not exceeding ₱500 Thousand

1.	Non-compliance with the requirement to submit complete information on the detailed return on the FO.	Assessment is on a per account basis.
2.	Non-compliance with the requirement to submit to the AMLC an electronic detailed return of the FO in a format prescribed by the latter.	Assessment is on per Resolution (Freeze Order) basis.
3.	Non-compliance with the requirement to keep electronic copies of all CTRs or STRs for, at least, five (5) years from the dates of submission to the AMLC.	Assessment is on a per violation basis.

B. Assessments involving non-compliance with submission of CTRs within the required period shall be as follows:

TABLE B:

A. MAJOR VIOLATIONS: Non-compliance with the covered transaction reporting requirement representing more than 25% of the total sampled population of CTRs within the examination period.	**Administrative Sanctions**					
		Micro	**Small**	**Medium**	**Large A**	**Large B**
	Minimum	₱1,500.00 per CT, but not exceeding ₱1 Million	₱3,750.00 per CT, but not exceeding ₱2.5 Million	₱7,500.00 per CT, but not exceeding ₱5 Million	₱11,250.00 per CT, but not exceeding ₱7.5 Million	₱15,000.00 per CT, but not exceeding ₱10 Million
	Medium	₱2,250.00 per CT, but not exceeding ₱1.5 Million	₱5,625.00 per CT, but not exceeding ₱3.75 Million	₱11,250.00 per CT, but not exceeding ₱7.5 Million	₱16,875.00 per CT, but not exceeding ₱11 Million	₱22,500.00 per CT, but not exceeding ₱15 Million
	Maximum	₱3,000.00 per CT, but not exceeding ₱2 Million	₱7,500.00 per CT, but not exceeding ₱5 Million	₱5,000.00 per CT, but not exceeding ₱10 Million	22,500.00 per CT, but not exceeding ₱15 Million	₱30,000.00 per CT, but not exceeding ₱20 Million
B. SERIOUS VIOLATIONS:	**Administrative Sanctions**					
		Micro	**Small**	**Medium**	**Large A**	**Large B**

Non-compliance with the covered transaction reporting requirement representing more than 5% but not more than 25% of the total sampled population of CTRs within the examination period.	**Minimum**	₱1,000.00 per CT, but not exceeding ₱500 Thousand	₱2,500.00 per CT, but not exceeding ₱1.25 Million	₱5,000.00 per CT, but not exceeding ₱2.5 Million	₱7,500.00 per CT, but not exceeding ₱3.75 Million	₱10,000.00 per CT, but not exceeding ₱5 Million
	Medium	₱1,500.00 per CT, but not exceeding ₱750 Thousand	₱3,750.00 per CT, but not exceeding ₱1.875 Million	₱7,500.00 per CT, but not exceeding ₱3.75 Million	₱11,250.00 per CT, but not exceeding ₱5.5 Million	₱15,000.00 per CT, but not exceeding ₱7.5 Million
	Maximum	₱2,000.00 per CT, but not exceeding ₱1 Million	₱5,000.00 per CT, but not exceeding ₱2.5 Million	₱10,000.00 per CT, but not exceeding ₱5 Million	₱15,000.00 per CT, but not exceeding ₱7.5 Million	₱20,000.00 per CT, but not exceeding ₱10 Million
C. LESS SERIOUS VIOLATIONS: Non-compliance with the covered transaction reporting representing 5% or less of the total sampled population of CTRs filed within the examination period.	**Administrative Sanctions**					
		Micro	**Small**	**Medium**	**Large A**	**Large B**
	Minimum	₱500.00 per CT, but not exceeding ₱100 Thousand	₱1,250.00 per CT, but not exceeding ₱250 Thousand	₱2,500.00 per CT, but not exceeding ₱500 Thousand	₱3,750.00 per CT, but not exceeding ₱750 Thousand	₱5,000.00 per CT, but not exceeding ₱1 Million
	Medium	₱750.00 per CT, but not exceeding ₱250 Thousand	₱1,875.00 per CT, but not exceeding ₱625 Thousand	₱3,750.00 per CT, but not exceeding ₱1.25 Million	₱5,625.00 per CT, but not exceeding ₱1.875 Million	₱7,500.00 per CT, but not exceeding ₱2.5 Million
	Maximum	₱1,000.00 per CT, but not exceeding ₱500 Thousand	₱2,500.00 per CT, but not exceeding ₱1.250 Million	₱5,000.00 per CT, but not exceeding ₱2.5 Million	₱7,500.00 per CT, but not exceeding ₱3.750 Million	₱10,000.00 per CT, but not exceeding ₱5 Million

15.2 ADMINISTRATIVE SANCTIONS BY THE OTHER REGULATING AGENCIES

Other regulating agencies such as the BSP and the Inter-Agency Council Against Trafficking or IACAT (for trafficking-in-persons cases), to name a few, may likewise impose administrative sanctions on the Bank without prejudice to the imposition of administrative sanctions by the AMLC and vice versa.

15.3 VIOLATIONS OF THE CODE OF ETHICS

Violations enumerated in this Manual and those analogous thereto and acts or omissions committed contrary to R.A. 9160 (AMLA), as amended, Law on Secrecy of Deposits, the General Banking Act and other banking laws shall also be punishable in accordance with the Bank's Code of Ethics.

This Manual covers all China Bank Savings, Inc. employees. Infractions of this Manual shall constitute a major violation of the Company policy. The degrees of offenses on Company and penalties set forth in the Company's Code of Ethics are hereby adopted.

Any loss, fines or penalties arising from violation or non-adherence to this Manual and other existing Bank policies shall be for the account of the erring officers and/or employees. A more severe corrective action or penalty may be imposed on an erring employee even on the first, second or third offense depending on the gravity of the offense and the personal circumstances of the offending employee. Gross negligence coupled with loss to the Bank or a third party amounts to bad faith shall be dealt with as an intentional violation.
Though not a disciplinary penalty per se, restitution or compensation shall be required of a person who by act or omission causes loss or damage to the Bank or another, unless there are equitable considerations for requiring less than full restitution or compensation.

Similarly, adherence to AMLA policies and guidelines shall form part of the performance rating system of employees.

PART XVI
AML TRAINING AND INFORMATION DISSEMINATION

PART XVI: AML TRAINING AND INFORMATION DISSEMINATION

The Compliance Division through the AML Compliance Department shall provide responsible Bank Officers and Employees with efficient, adequate and continuous education program to enable them to fully and consistently comply with all their obligations under the Revised Implementing Rules and Regulations (RIRR) of the Anti-Money Laundering Act (AMLA), as amended.

The AML Compliance Department shall have a close coordination with the Human Resources Division pertaining to the formulation, execution and monitoring of training programs. General and specialized training programs shall be provided either through classroom or internet-based training modules.

16.1 SUBJECT CONTENT

The training module covers the salient provisions of the Anti-Money Laundering Law as amended and the guidelines contained in the MTPP. Additionally, new rules and regulations, such as but not limited to the following shall be covered in training:

- RA No. 9160
- RA No. 9194
- RA No. 10167
- RA No. 10168
- RA No. 10365
- RA No. 10927
- RA No. 11479
- RA No. 11521

The modules shall cover AML policies and procedures and new regulatory issuances to strengthen employees' awareness and knowledge on AML. Specific modules shall be designed taking into account the nature of the function.

16.2 EMPLOYEE COVERAGE

a. Key Personnel and Front-liners
b. Senior Officers and Directors of the Bank
c. Non-key Personnel / Back-office Personnel
d. New Hires

16.3 ATTENDANCE AND FREQUENCY OF TRAINING

a. All employees not categorized as key personnel shall receive AML training every other year.
b. For Key Personnel, refresher training shall be given annually.
c. For Senior Officers, frequency of training will depend on the function of the unit or group.

16.4 MODE OF TRAINING AND VALIDATION

The training shall be facilitated through electronics means and/or classroom training. For e-Training, with the exception of directors, personnel shall be required to take the examination via Moodle (an intranet-based e-learning facility) or through questionnaires. The Senior Officers shall also be required to take the training via Moodle and/or attend AML Training which will be facilitated by Compliance Division.

16.5 AML TRAINING REQUIREMENT

All bank personnel including Senior Officers should have completed AML Training and should have passed the AML examination to be eligible for recommendation to a higher position or for any promotion.

16.6 AML TRAINING POLICIES

1. All Officers and Employees shall undergo trainings and testing on Anti-Money Laundering as programmed by Bank Compliance Division (CD).

   Refresher training on AMLA shall be undertaken by responsible Bank Officers and Employees every year.

   For AMLA updates/developments/directives which require urgent dissemination of information and/or implementation, the AML Compliance Officer shall disseminate such information via email to all bank units and shall monitor proper implementation of responsible unit, as applicable. Such updates/developments/directives shall likewise be incorporated in the AML training modules, and MTPP, as necessary.

2. New Officers and Employees shall attend the formal AML training during their New Orientation (NEO) Program within three (3) months from date of hiring.

3. The training must instill in Officers and Employees awareness of their respective duties and responsibilities under the Money Laundering and Terrorist Financing Prevention Program MTPP particularly in relation to:

   a. Customer identification process;
   b. Client risk assessment process through the use of Enhanced Customer Risk Assessment Form (ECRAF). The ECRAF shall be accomplished for all new and existing accounts and in case of change of client's profile, if any, e.g., from low risk to high risk;
   c. Client shall be profiled and corresponding due diligence shall be applied:
      - Average Due Diligence (ADD) if client is profiled as low/normal risk; or
      - Enhanced Due Diligence (EDD) if Client is profiled as high risk;
   d. Record keeping requirements;
   e. Covered and suspicious transactions reporting;
   f. Understanding of the internal processes including the chain of command for the reporting and investigation of suspicious and money laundering activities.

4. The program shall be designed to suit:

- New hires
- Front-line staff
- Compliance Division staff
- Internal Audit staff
- Supervisors
- Junior Officers
- Senior Management
- Directors
- Stockholders

5. The Anti-Money Laundering Compliance Officer (AMLCO) or duly authorized representative shall handle/conduct the trainings on anti-money laundering in coordination with the HRD.

   The CCO shall recommend external resource persons to conduct the training when necessary.

6. In coordination with CD, designated Compliance Officer shall monitor and ensure that all Bank Employees shall attend all the required AMLA Trainings (NEO and Refresher).

7. HRD shall monitor AML training of each Associate and ensure that Associates are updated and have attended the AML training program arranged by CD. HRD may recommend AML training facilitated by external resources.

16.7 SCOPE OF TRAINING

1. Scope of training shall depend on the work assignment of Officers and Employees.

   1.1. New Hires

   a. General appreciation of the principles and elements of money laundering
   b. Features and requirements of AMLA
   c. Ability to recognize covered and suspicious transactions and reporting requirements
   d. Other provisions of AMLA

   The training shall form part of the NEO Program.

   1.2. Front line Staff (Teller, Senior Teller, Service Associate, Processor, etc.)

   As Employees who directly deal with the Customer and who may be the first point of contact of a potential money-launderer, they must be made aware of the reporting system.

   a. Factors that may give rise to suspicion and the procedures to be adopted when a suspicious or covered transaction is suspected.

b. Vigilance required in dealing with non-regular customers particularly when large cash transactions are involved.

1.3. Sales Associates and Traders

a. Account opening and customer identity verification procedures as they deal with account opening, or acceptance of new customers.
b. The requirements of obtaining the mandatory information of the clients and ensuring that mandatory fields in CIS are filled up.
c. Reporting system as they directly deal with the prospective customer and are the first point of contact of the potential money-launderer.
d. Factors that may give rise to suspicion and on the actions to be taken when a suspicious or covered transaction is detected.
e. Vigilance required in dealing with non-regular customers particularly when large cash transactions are involved.
f. Awareness that the offer of suspicious funds accompanying a request to undertake investment business may need to be reported to the proper authority whether or not the funds are accepted or the transaction pushes through.

1.4. Branch, Business and Lending Unit Officers

High level instructions covering all aspects of money laundering procedures which shall include internal reporting procedures, requirement for verification and retention of records.

1.5. Other Employees

Similar in scope for New Hires

2. The training of Employees shall be included in the HRD Programs (e.g., NEO, Officership Training Program, Management Development Program, etc.)

3. Training programs shall always be updated based on new developments and issuances related to the prevention of money laundering and terrorism financing.

16.8 TRAINING RECORDS

1. All records pertaining to the regular and refresher trainings including copies of AML seminar/training materials conducted shall be maintained and safe kept by designated Custodians of CD and HRD which shall be made available during periodic or special BSP examinations.

2. The records shall contain the following:

a. Names and work assignments of participants

b. Dates and location of the trainings

3. The records shall be:

   a. Stored in designated filing cabinets
   b. Retained for 5 years from date of training, and
   c. The accountability of AML CO or designated Custodian which shall be turned-over to successor upon resignation or transfer to another unit

16.9 TRAINING METHODS AND MATERIALS

The AML Compliance Department of the Compliance Division shall oversee the creation, communication and deployment of AMLA training materials. Separate training materials for special topics or complicated AML-issues shall be prepared by the AML Department for participants approved by the Compliance Division.

The AMLA refresher course and other training modules shall be deployed through an internet-based training module. However, classroom trainings shall be held by the Compliance Division (with closed coordination with the Human Resources Division) to front-liners and personnel handling the monitoring, review or day-to-day approval of transactions to provide a more interactive discussion of AML-related topics and issues.

The classroom training, which will be conducted parallel to the e-Learning AMLA refresher course, shall be held every two (2) years to selected set of participants as determined by the Compliance Division.

16.10 IMPLEMENTING GUIDELINES OF THE AMLA E-LEARNING COURSE

Human Resources Division, in collaboration with Compliance Division aims to provide AMLA accreditation to all employees after successfully completing the online certificate course. All employees of China Bank Savings are required to read and understand the training materials, and pass the examination.

Below are the implementing guidelines in the AMLA e-Learning Course:

1. Human Resources Division shall release an e-mail announcement containing the module of the AMLA e-Learning Course, list of participants and account credentials for the exam.

2. Human Resources Division shall upload the list of participants to Moodle e-Learning Facility for the exam. The employee's Personnel Number or PERNR will be assigned as their username and initial password. The participants will be prompted to personalize their initial password upon first successful log-in.

3. The participants will be given a **10-day access schedule** to study the reference materials, and take the exam. Once the 10-day access schedule has lapsed, the reference materials and exam will no longer be accessible.

4. The online exam and its results will be monitored by Human Resources Division and AML Compliance Department; participants should obtain a **grade equal to or greater than 80%** to be able to pass the course.

5. Only three (3) attempts will be given to the participants for the exam, wherein the highest score attained by the participants will be recorded as their final score. Once finished, the participant will be informed if he / she has passed or failed the exam.

6. The online exam is time-pressured. A maximum of thirty (30) minutes will be given to finish the online exam.

7. Employees who failed the exam after the third attempt will be scheduled by Human Resources Division for retake. Only one attempt will be given for remedial. Failure to retake within the agreed schedule shall be construed to have failed the course.

   If the employee failed to pass the remedial exam, they will have to attend the one-day AML Certificate Course via MS Teams to be scheduled and conducted by the AML Compliance Officer. All participants should pass the exam after the program. Exam results will be considered final.

8. Human Resources Division will record successful completion of the course in SAP - ESS.

9. If the participant failed to access the exam due to server downtime, Human Resources Division will re-schedule the participant's access to the next available access schedule.

10. Any attempt to cheat will result in the disqualification from taking the exam, and will subject the employee to disciplinary action as may be deemed appropriate by the Bank and the same will form part of the 201 File. Some examples of these offences are: a. Any recording of the exam screens, including taking screenshots, pictures or videos; b. Copying the exam questions or answers; c. Searching thru mobile devices, web browsers, software applications, or other computer during the exam.

11. The result of the e-Learning exam including those who failed or failed to take shall be reported to the AML Committee.

12. Reopening of the module shall also be based on the decision of the AML Committee.

13. If the employee didn't take the exam or failed the exam after several attempts and despite the training intervention, the Human Resource Division shall issue a written warning to the erring employees and this will form part of their 201 file.

14. Further, passing the AML exam is included in the Compliance Rating which is one of the criteria for promotion. On the other hand, the Human Resource Division shall include in the PAR form across all employees 5% allocation for Compliance, Audit and Risk where employees must have no major findings from Compliance, Audit and Risk Management. If employee did not take or failed the AML exam, it would have an effect on his/her performance rating or their eligibility for promotion.

15. Repeated non-compliance or violation of the guidelines shall be dealt with more seriously.

16.11 INFORMATION DISSEMINATION

The Unit Compliance Coordinators (UCC) of branches (BSH) and units shall be responsible in the dissemination of information or issuances provided by the Compliance Division or any of its department. The dissemination responsibility requires the Unit Compliance Coordinator to discuss with the affected units of the respective branch/unit the information or issuance from the Compliance Division.

The information or issuance from the Compliance Division shall be printed and kept in a separate folder and shall be made available to all branch/unit personnel.

The discussion performed by the Compliance Coordinator shall be recorded in the minutes of regular branch/unit meeting or shall be recorded in the print-out of the issuance through the signature of the Coordinator and the audience to whom such information or issuance was discussed.

PART XVII
ANNEXES

PART XVII: ANNEXES

Annex A	-	R.A. 9160 as Amended by R.A. 9194, R.A. 10167, R.A. 10365, R.A. 10927, & R.A. 11521
Annex B	-	R.A. 10168 – The Terrorism Financing Prevention and Suppression Act of 2012 and R.A. 11479 – The Anti-Terrorism Act of 2020
Annex C	-	2018 Revised Implementing Rules and Regulations (RIRR) of R.A. 9160
Annex D	-	2021 AMLC Registration and Reporting Guidelines and 2024 AML Guidelines on Transaction Reporting and Compliance Submissions
Annex E	-	2021 AMLC Sanctions Guidelines
Annex F	-	AML Due Diligence Questionnaire for Counterparty Financial Institutions
Annex G	-	Amended Guidelines on Acceptable IDs of Foreign Nationals
Annex H	-	Enhanced Customer Risk Assessment Form (ECRAF) V2.2 – Individual
Annex I	-	Enhanced Customer Risk Assessment Form (ECRAF) V2.3 – Corporate
Annex J	-	ECRAF Implementing Guidelines V2.3 and its Annexes
Annex K	-	Enhanced Due Diligence (EDD) Form
Annex L	-	Guidelines on Post-Transaction Screening for Cash Pick-up Anywhere Service
Annex M	-	Illustration of Direct and Indirect Ownership
Annex N	-	Ultimate Beneficial Owner (UBO) Determination Form
Annex O	-	UBO Determination Form Implementing Guidelines
Annex P	-	List of High Risk Jurisdictions and High Risk Philippine Areas
Annex Q	-	Guidelines on Handling of Deposit Accounts Used for ADA of Loan Clients
Annex R	-	Guidelines in Writing a High Quality Report on Incident of Suspicious Activity (RISA) Narrative
Annex S	-	Report on Incident of Suspicious Activity (RISA) Form – Individual
Annex T	-	Report on Incident of Suspicious Activity (RISA) Form – Corporate
Annex U	-	Sworn Statement of Non-Engagement
Annex V	-	Counterparty Disclosure Form
Annex W	-	Due Diligence Questionnaire (DDQ) Form
Annex X	-	Document Checklist (Gaming and Gaming-related)
Annex Y	-	Enhanced Due Diligence (EDD) Form for Gaming Clients (For Entities Engaged in Gaming or Gaming-Related Activities)

Annex Z - Framework for Gaming and Gaming-related Clients

Annex AA - AML& CTF Questionnaire for Money Service Business Clients (MSBs)

Annex AB - Application for Business Relationship of MSB Clients

Annex AC - Standard Template on Annual Analysis of MSB Clients

Annex AD - Document Checklist (Money Service Business)

Annex AE - Document Checklist (Cash-Intensive Business)

Annex AF - Alerts Management Guidelines for Branches and Business Units

Annex AG - Alerts Management Guidelines for Compliance Investigators and Approvers

Annex AH - Guidelines on Whitelisting of Clients from Alerts Generation

Annex AI - Whitelisting Request Form

Annex AJ - Transaction Enhanced Due Diligence (TEDD) Form

Annex AK - TEDD Form Instruction Manual

Annex AL - Criteria Whether to Retain or Terminate Business Relationship

Annex AM - IRA Parameters in Evaluating the Strength of Controls

Annex AN - Results of the 2023-2024 Institutional Risk Assessment