BANGKO SENTRAL NG PILIPINAS

OFFICE OF THE GOVERNOR

CIRCULAR NO. 706
Series of 2011

Subject: **UPDATED ANTI-MONEY LAUNDERING RULES AND REGULATIONS**

By the authority vested to the Bangko Sentral ng Pilipinas (BSP) to issue guidelines and circulars on anti-money laundering (AML) in order to effectively implement the provisions of Republic Act No. 9160, otherwise known as the "Anti-Money Laundering Act of 2001", as amended by Republic Act No. 9194 (AMLA, as amended), under Rule 17.1 (b) of the Revised Implementing Rules and Regulations (RIRR), the Monetary Board, in its Resolution No. 1801 dated 16 December 2010, approved the adoption of this Updated Anti-Money Laundering Rules and Regulations and the amendment of Part Eight of the Manual of Regulations as well as the repeal of other BSP Circulars that are inconsistent herewith.

Section X801. Declaration of Policy- The BSP adopts the policy of the State to protect the integrity and confidentiality of bank accounts and to ensure that the Philippines in general and the covered institutions herein described in particular shall not be used respectively as a money laundering site and conduit for the proceeds of an unlawful activity as hereto defined.

Section X802. Scope of Regulations- These regulations shall apply to all covered institutions supervised and regulated by the BSP. The term "covered institution" shall refer to Banks, Offshore 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 as herein defined wherever they may be located:

(a) A subsidiary means an entity more than fifty percent (50%) of the outstanding voting stock of which is owned by a bank, quasi-bank, trust entity or any other institution supervised and/or regulated by the BSP.

(b) An affiliate means an entity the voting stock of which, to the extent of fifty percent (50%) or less, is owned by a bank, quasi-bank, trust entity, or any other institution supervised and/or regulated by the BSP.

Pursuant to Section 20 of the General Banking Law of 2000, a bank authorized by BSP to establish branches or other offices within or outside the

Philippines shall be responsible for all business conducted in such branches and offices to the same extent and in the same manner as though such business had all been conducted in the head office. A bank and its branches and offices shall be treated as one unit.

Whenever local applicable laws and regulations of a branch, office, subsidiary or affiliate based outside the Philippines prohibit the implementation of these Rules or any of the provisions of the AMLA, as amended, its RIRR, and the supervising authority in that foreign country issues a directive forbidding said branch, office, subsidiary or affiliate, the covered institution shall notify the BSP of this situation and furnish a copy of the supervising authority's directive.

Section X803. Definition of terms- Except as otherwise defined herein, all terms used shall have the same meaning as those terms that are defined in the AMLA, as amended, and its RIRR.

(A) Money laundering is a crime whereby the proceeds of an unlawful activity as herein defined are transacted, thereby making them appear to have originated from legitimate sources. It is committed by the following:

(1) Any person knowing that any monetary instrument or property represents, involves, or relates to, the proceeds of any unlawful activity, transacts or attempts to transact said monetary instrument or property.

(2) Any person knowing that any monetary instrument or property involves the proceeds of any unlawful activity, performs or fails to perform any act as a result of which he facilitates the offense of money laundering referred to in paragraph (1) above.

(3) Any person knowing that any monetary instrument or property is required under the act to be disclosed and filed with the Anti-Money Laundering Council, fails to do so.

(B) Covered transaction (CT) is a transaction in cash or other equivalent monetary instrument involving a total amount in excess of five hundred thousand pesos (₱500,000) within one banking day.

(C) Suspicious transactions (ST) are transactions with covered institutions, regardless of the amount involved, where any of the following circumstances exist:

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 the AMLA, as amended;

5. Any circumstance relating to the transaction which is observed to deviate from the profile of the client and/or client's past transactions with the covered institution;
6. The transaction is in any way related to an unlawful activity or any money laundering activity or offense under the AMLA, as amended, that is about to be, is being or has been committed; or
7. Any transaction that is similar or analogous to any of the foregoing.

(D) Monetary instrument refers to:

(1) Coins or currency of legal tender of the Philippines, or of any other country;
(2) Drafts, checks, and notes;
(3) 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;
(4) Contracts or policies of insurance, life or non-life, and contracts of suretyship; and
(5) Other similar instruments where title thereto passes to another by endorsement assignment or delivery.

(E) Transaction refers to any act establishing any right or obligation or giving rise to any contractual or legal relationship between the parties thereto. It also includes any movement of funds by any means with a covered institution.

(F) 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, 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 Anti-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 310 of the Revised Penal Code, as amended;
(10) Smuggling under Republic Act Nos. 455 and 1937;
(11) Violations under 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, including those perpetrated by terrorists against non-combatant persons and similar targets;
(13) Fraudulent practices and other violations under Republic Act No. 8799, otherwise known as the Securities Regulation Code of 2000;
(14) Felonies or offenses of a similar nature that are punishable under the penal laws of other countries.

(G) Customer- refers to any person or entity that keeps an account, or otherwise transacts business, with a covered institution and any person or entity on whose behalf an account is maintained or a transaction is conducted, as well as the beneficiary of said transactions. A customer also includes the beneficiary of a trust, an investment fund, a pension fund or a company or person whose assets are managed by an asset manager, or a grantor of a trust.

(H) Shell Company- Legal entities which have no business substance in their own right but through which financial transactions may be conducted.

(I) Shell Bank- 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 also be a bank that (a) does not conduct business at a fixed address in a 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.

(J) Beneficial Owner- refers to natural person(s) who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement.

(K) Politically Exposed Person or PEP- an individual who is or has been entrusted with prominent public positions in the Philippines or in a foreign state, including heads of state or of government, senior politicians, senior national or local government, judicial or military officials, senior executives of government or state owned or controlled corporations and important political party officials.

(L) Correspondent banking refers to activities of one bank (the correspondent bank) having direct connection or friendly service relations with another bank (the respondent bank).

(M) 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 the beneficiary person may be the same person.

(N) Cross border transfers- any wire transfer where the originating and beneficiary institutions are located in different countries. It shall also refer to any chain of wire transfers that has at least one cross-border element.

(O) Domestic Transfer- any wire transfer where the originating and beneficiary institutions are located in the same country. It shall 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.

(P) Originating institution- refers to the entity utilized by the originator to transfer funds to the beneficiary and can either be (a) a covered institution as specifically defined by these Rules and as generally defined by the AMLA, as amended, and its RIRR, or (b) a financial institution operating outside the Philippines that is other than covered institutions referred to in (a) but conducts business operations and activities similar to them.

(Q) 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 these Rules and as generally defined by the AMLA, as amended, and its RIRR, or (b) a financial institution operating outside the Philippines that is other than covered institutions referred to in (a) but conducts business operations and activities similar to them.

(R) Intermediary institution- refers to 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 these Rules and as generally defined by the AMLA, as amended, and its RIRR, or (b) a financial institution operating outside the Philippines that is other than covered institutions referred to in (a) but conducts business operations and activities similar to them.

Section X804. Basic Principles and Policies to Combat Money Laundering - In line with the declaration of policy, covered institutions shall apply the following principles:

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

2. Know sufficiently your customer 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 covered institution by himself or otherwise;

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

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

5. Fully cooperate with the Anti-Money Laundering Council (AMLC) for the effective implementation and enforcement of the AMLA, as amended, and its RIRR.

A. RISK MANAGEMENT

§ X805. Risk Management – All covered institutions shall develop sound risk management policies and practices to ensure that risks 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 these regulations, to the end that covered institutions shall not be used as a vehicle to legitimize proceeds of unlawful activity or to facilitate or finance terrorism.

The four areas of sound risk management practices are adequate and active Board and Senior Management oversight, acceptable policies and procedures embodied in a money laundering and terrorist financing prevention compliance program, appropriate monitoring and Management Information System and comprehensive internal controls and audit.

§ X805.1. Board and Senior Management Oversight – Notwithstanding the provisions specifying the duties and responsibilities of the Compliance Office and Internal Audit, it shall be the ultimate responsibility of the Board of Directors to fully comply with the provisions of these rules, the AMLA, as amended, and its RIRR. For this reason, it shall ensure that oversight on the institution's compliance management is adequate.

§ X805.1.a. Compliance Office- Management of the implementation of the covered institution's Money Laundering and Terrorist Financing Prevention Program (MLPP) shall be a primary task of the Compliance Office. To ensure the independence of the Office, it shall have a direct reporting line to the Board of Directors or any Board-level or approved committee on all

matters related to AML and terrorist financing compliance and their risk management. It shall be principally responsible for the following functions among other functions that may be delegated by Senior Management and the Board, to wit:

1. Ensure compliance by all responsible officers and employees with these Rules, the AMLA, as amended, the RIRR and its own MLPP. It shall conduct periodic compliance checking which covers, among others, evaluation of existing processes, policies and procedures including on-going monitoring of performance by staff and officers involved in money laundering and terrorist financing prevention, reporting channels, effectivity of the electronic money laundering transaction monitoring system and record retention system through sample testing and review of audit or examination reports. It shall also report compliance findings to the Board or any Board-level 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 board of directors, or the Board-level or approved committee if it believes that the institution 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 as stated in **Section X809**.

§ X805.2. Money Laundering and Terrorist Financing Prevention Program- All covered institutions shall adopt a comprehensive and risk-based MLPP geared toward the promotion of high ethical and professional standards and the prevention of the bank being used, intentionally or unintentionally, for money laundering and terrorism financing. The MLPP shall be consistent with the AMLA, as amended, and the provisions set out in these rules and designed according to the covered institution's corporate structure and risk profile. It shall be in writing, approved by the Board of Directors or by the country/regional head or its equivalent for local branches of foreign banks, and well disseminated to all officers and staff who are obligated by law and by their program to implement the same. Where a covered institution has branches, subsidiaries, affiliates or offices located within and/or outside the Philippines, it shall adopt an institution-wide MLPP that shall be implemented on a consolidated basis.

The MLPP shall also be readily available in user-friendly form, whether in hard or soft copy. The Covered institution must put up a procedure to ensure an audit trail evidencing dissemination process for new and amended policies and procedures. The program shall embody the following at a minimum:

1) Detailed procedures of the covered institution's compliance and implementation of the following major requirements of the AMLA, as amended, its RIRR, and these Rules, to wit:

a) Customer identification process including acceptance policies and on-going monitoring processes;

b) Record keeping and retention;

c) Covered transaction reporting; and

d) Suspicious transaction reporting including the adoption of a system, electronic or manual, of flagging, monitoring and reporting of transactions that qualify as suspicious transactions, regardless of amount or that will raise a "red flag" for purposes of conducting further verification or investigation, or transactions involving amounts below the threshold to facilitate the process of aggregating them for purposes of future reporting of such transactions to the AMLC when their aggregated amounts breach the threshold. The ST reporting shall include a reporting chain under which a suspicious transaction will be processed and the designation of a Board level or approved Committee who will ultimately decide whether or not the covered institution should file a report to the AMLC. If the resources of the covered institution do not permit the designation of a Committee, it may designate the compliance officer to perform this function instead provided that the Board of Directors is informed of his decision.

2) An effective and continuous anti-money laundering and countering of terrorist financing training program for all directors, and responsible officers and employees, to enable them to fully comply with their obligations and responsibilities under these rules, the AMLA, as amended, its RIRR and their internal policies and procedures as embodied in the MLPP. The training program shall also include refresher trainings to remind these individuals of their obligations and responsibilities as well as update them of any changes in AML laws, rules and internal policies and procedures.

3) An adequate screening and recruitment process to ensure that only qualified personnel who have no criminal record/s are employed to assume sensitive banking functions;

4) An internal audit system in accordance with **§ X805.4**;

5) An independent audit program with written scope of audit that will ensure the completeness and accuracy of the information and identification documents obtained from clients, the covered and

suspicious transaction reports submitted to the AMLC, and the records retained in compliance with these rules as well as adequacy and effectiveness of the training program on the prevention of money laundering and terrorism financing;

6) A mechanism that ensures all deficiencies noted during the audit and/or BSP regular or special examination are immediately corrected and acted upon;

7) Cooperation with the AMLC; and

8) Designation of an AML compliance officer, who shall at least be at senior officer level, as the lead implementor of the program within an adequately staffed Compliance Office. The AML compliance officer may also be the liaison between the covered institution, the BSP and the AMLC in matters relating to the covered institution's AML compliance. Where resources of the covered institution do not permit the hiring of an AML compliance officer, the Compliance Officer shall also assume the responsibility of the former.

§ X805.2.a. Submission of the Revised and Updated MLPP. Approval by the Board of Directors or Country Head - Within one hundred eighty days (180) days from effectivity of these Rules, all covered institutions shall prepare and have available for inspection an updated MLPP embodying the principles and provisions stated in these rules. The Compliance Officer shall submit to the Anti-Money Laundering Specialist Group, Supervision and Examination Subsector I of the BSP a sworn certification that the revised MLPP had been prepared, duly noted and approved by the Board of Directors or the Country Head or its equivalent for local branches of foreign banks.

Henceforth, each MLPP shall be regularly updated at least once every two years to 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 MLPP shall likewise be approved by Board of Directors or the country/regional head or its equivalent for local branches of foreign banks.

§ X805.3. Monitoring and Reporting Tools – All covered institutions shall adopt an AML and terrorist financing monitoring system that is appropriate for their risk-profile and business complexity and in accordance with these Rules. The system should be capable of generating timely, accurate and complete reports to lessen the likelihood of any reputational and compliance risks, and to regularly apprise the Board of Directors and Senior Management on anti-money laundering and terrorist financing compliance.

§ X805.3.a. Electronic Monitoring and Reporting Systems for Money Laundering- Universal Banks (UBs) and Commercial Banks (KBs) shall adopt an electronic AML system capable of monitoring risks associated with money-laundering and terrorist financing as well as generating timely reports for the guidance and information of its Board of Directors and Senior Management in addition to the functionalities mentioned in **§ X807.2.**

§ X805.3.b. Manual monitoring- For covered institutions other than UBs and KBs, it need not have an electronic system but must ensure that it has the means of complying with **§ X805.3.**

§ X805.4. Internal Audit - The Internal Audit function associated with money laundering and terrorist financing should 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 a direct reporting line to the Board or a Board level Audit Committee.

The Internal Audit shall, in addition to those specified by these rules, be responsible for the periodic and independent evaluation of the risk management, degree of adherence to internal control mechanisms related to the customer identification process, such as the determination of the existence of customers and the 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, CT and ST reporting and record keeping and retention,as well as the adequacy and effectiveness of other existing internal controls associated with money laundering and terrorist financing.

For UBs and KBs with electronic money laundering transaction monitoring system, in addition to the above, the internal audit shall include determination of the efficiency of the system's functionalities as required by **§ X805.3** and **§ X807.2.**

The results of the internal audit shall be timely communicated to the Board of Directors and shall be open for scrutiny by BSP examiners in the course of the regular or special examination without prejudice to the conduct of its own evaluation whenever necessary. Results of the audit shall likewise be promptly communicated to the Compliance Office for its appropriate corrective action. The Compliance Office shall regularly submit reports to the Board to inform them of management's action to address deficiencies noted in the audit.

B. CUSTOMER IDENTIFICATION PROCESS

Section X806. A covered institution shall maintain a system of verifying the true identity of their customers and, in case of corporate and juridical entities, require a system of verifying their legal existence and organizational structure as well as the authority and identification of all persons purporting to act on their behalf. Along this line, it shall formulate a risk-based and tiered customer acceptance policy, customer retention policy and customer identification process that involves reduced Customer Due Diligence (CDD) for potentially low risk clients and enhanced CDD for higher risk accounts.

§ X806.1. Customer acceptance policy- Every covered institution shall develop clear, written and graduated acceptance policies and

procedures that will ensure that the financially or socially disadvantaged are not denied access to financial services while at the same time prevent suspicious individuals or entities from opening an account.

§ X806.1.a. Criteria for type of customers: low, normal and high risk; Standards for applying reduced, average and enhanced due diligence- Covered institutions shall specify the criteria and description of the types of customers that are likely to pose low, normal or high risk to their operations as well as the standards in applying reduced, average and enhanced due diligence including a set of conditions for the denial of account opening.

Enhanced due diligence shall be applied to customers that are assessed by the covered institution or by these Rules as high risk for money laundering and terrorist financing.

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 covered institution's office or branch, the covered institutions may apply reduced due diligence. Some entities may likewise be considered as low risk clients, these are: Banking institutions, trust entities and quasi-banks authorized by the BSP to operate as such, publicly listed companies subject to regulatory disclosure requirements, government agencies including government owned and controlled corporations (GOCCs).

In designing a customer acceptance policy, the following factors shall be taken into account:

1. Background and source of funds;
2. Country of origin and residence or operations;
3. Public or high profile position of the customer or its directors/trustees, stockholders, officers and/or authorized signatory;
4. Linked accounts;
5. Watch list of individuals and entities engaged in illegal activities or terrorist related activities as circularized by BSP, AMLC, and other international entities or organizations such as the Office of Foreign Assets Control (OFAC) of the U.S. Department of the Treasury and United Nations Sanctions List;
6. Business activities; and
7. Type of services/products/transactions to be entered with the covered institution.

In all instances, the covered institution shall document how a specific customer was profiled (low, normal or high) and what standard of CDD (reduced, average or enhanced) was applied.

§ X806.1.b. Enhanced Due Diligence- Whenever enhanced due diligence is applied as required by these Rules or by the covered institution's customer acceptance policy, the covered institution shall, in addition to profiling of customers and monitoring of their transactions, do the following:

1. Obtain additional information other than the minimum information and/or documents required for the conduct of average due diligence as enumerated under **§ X806.2.a and § X806.2.b**;

(a) In cases of individual customers, obtain a list of banks where the individual has maintained or is maintaining an account, list of companies where he is a director, officer or stockholder, and banking services to be availed of.

(b) For entities assessed as high risk customers, such as shell companies, covered institutions shall, in addition to the minimum information and/or documents enumerated above, obtain additional information including but not limited to prior or existing bank references, the Name, present address, date and place of birth, nature of work, nationality and source of funds of each of the primary officers (President, Treasurer and authorized signatory/ies), stockholders owning at least 2% of the voting stock, and directors/trustees/partners as well as their respective identification documents.

2. Conduct validation procedures on any or all of the information provided in accordance with **§ X806.1.c**.

3. Obtain senior management approval for establishing business relationship.

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

§ X806.1.c. Minimum Validation Procedures- Validation procedures for individual customers shall include but is not limited to the following:

1. Confirming the date of birth from a duly authenticated official document;
2. Verifying the permanent address through evaluation of utility bills, bank or credit card statement or other documents showing permanent address or through on-site visitation;
3. Contacting the customer by phone, email or letter (such as sending of "thank you letters"); and
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 means.

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

1. Requiring the submission of audited financial statements conducted by a reputable accounting/auditing firm;
2. Inquiring from the supervising authority the status of the entity;
3. Obtaining bank references;
4. On-site visitation of the company; and
5. Contacting the entity by phone, email or letter (such as "thank you letters").

§ X806.1.d. Reduced Due Diligence. Whenever reduced due diligence is applied in accordance with the covered institution's customer acceptance policy, the following rules shall apply:

a. For individual customers, a covered institution may open an account under the true and full name of the account owner or owners and defer acceptance of the minimum information. Deferred acceptance of minimum information shall mean obtaining information numbers 1 to 7 of **§ X806.2.a** at the time of account opening while the rest, numbers 8 to 11, may be obtained within a reasonable time but not exceeding ninety (90) days from account opening.

b. For corporate, partnership, and sole proprietorship entities, and other entities such as banking institutions, trust entities and quasi-banks authorized by the BSP to operate as such, publicly listed companies subject to regulatory disclosure requirements, government agencies including GOCCs, a covered institution may open an account under the official name of these entities with only no. 4 of those required under **§ X806.2.b** (Board Resolution duly certified by the Corporate Secretary authorizing the signatory to sign on behalf of the entity)- obtained at the time of account opening.

§ X806.1.e. Face-to-face contact- No new accounts shall be opened and created without face-to-face contact and personal interview between the covered institution's duly authorized personnel and the potential customer except under the following arrangements:

§ X806.1.e.1. Account opened through a trustee, agent, nominee, or intermediary- Where the account is opened through a trustee, agent, nominee or intermediary, the covered institution 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 is being opened. The covered institution 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 criteria 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 are being opened 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 covered institution shall, at the minimum, obtain the true and full name, place and date of birth or date of

registration, as the case may be, present address, nature of work or business, and source of funds as if the account was opened by them separately. Where the covered institution is required to report a CT or circumstances warrant the filing of an ST, it shall obtain such other information on every trustor, principal, beneficial owner, or person on whose behalf the account is being opened in order that a complete and accurate report may be filed with the AMLC.

In case a covered institution 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 in accordance with **§ X806.1.b.**

§ X806.1.e.2. Outsourcing arrangement- Subject to existing rules on outsourcing of specified banking activities, a covered institution, without prior Monetary Board approval, may outsource to a counter-party the conduct of the requisite face-to-face contact provided that such arrangement is formally documented and provided further that the conditions under **§ X806.2.d.** are met.

If the counter party is an entity other than a covered institution as herein defined, covered institutions shall ensure that the employees or representatives of the counter-party conducting the face-to-face contact undergo equivalent training program as that of its front-liners undertaking a similar activity. Covered institutions shall likewise monitor and review annually the performance of the counter-party to assist it in determining whether or not to continue with the arrangement.

§ X806.1.e.3. Third party reliance- Where a third party as defined under **§ X806.2.e.1.** has already conducted the requisite face-to-face contact on its own customer who was referred to a covered institution, the latter may rely on the representation of the third party that it has already conducted face-to-face contact provided that the pertinent requirements in **§ X806.2.e.1.** are also met.

§ X806.2. Customer Identification- Covered institutions shall establish and record the true identity of its customers based on valid identification document/s specified in **§ X806.2.c.**

§ X806.2.a. New Individual Customers- Covered institutions shall develop a systematic procedure for establishing the true and full identity of new individual customers and shall open and maintain the account only in the true and full name of the account owner or owners.

Unless otherwise stated in these Rules, average due diligence requires that the covered institution obtain at the time of account opening all the following minimum information and confirming these information with the valid identification documents stated in **§ X806.2.c.** from individual customers and authorized signatory/ies of corporate and juridical entities:

1. Name;
2. Present address;

3. Date and place of birth;
4. Nature of work, name of employer or nature of self-employment/business;
5. Contact details;
6. Specimen signature;
7. Source of funds.
8. Permanent address;
9. Nationality;
10. Tax identification number, Social Security System number or Government Service Insurance Number, if any; and
11. Name, present address, date and place of birth, nature of work and source of funds of beneficial owner or beneficiary, whenever applicable.

§ X806.2.b. New Corporate and Juridical Entities- Covered institutions shall develop a systematic procedure for identifying corporate, partnership and sole proprietorship entities as well as the stockholders/partners/owners, directors, officers and authorized signatory of these entities. It shall open and maintain accounts only in the true and full name of the entity and shall have primary responsibility to ensure that the entity has not been, or is not in the process of being, dissolved, struck-off, wound-up, terminated, or otherwise placed under receivership or liquidation.

Unless otherwise stated in these Rules, average due diligence requires that the covered institution obtain the following minimum information and/or documents before establishing business relationships:

1. Certificates of Registration issued by the Department of Trade and Industry for single proprietors, or by the Securities and Exchange Commission, for corporations and partnerships, and by the BSP, for money changers/foreign exchange dealers and remittance agents;
2. Articles of Incorporation or Association and By-Laws;
3. Principal business address;
4. Board or Partners' Resolution duly certified by the Corporate/Partners' Secretary authorizing the signatory to sign on behalf of the entity;
5. 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;
6. Contact numbers of the entity and authorized signatory/ies;
7. Source of funds and nature of business;
8. Name, present address, date and place of birth, nature of work and source of funds of beneficial owner or beneficiary, if applicable; and
9. For entities registered outside the Philippines, similar documents and/or information shall be obtained duly authenticated by the Philippine Consulate where said entities are registered.

§ X806.2.c. Valid Identification documents- The following guidelines govern the acceptance of valid ID cards for all types of financial transaction by a customer and the authorized signatory/ies of a corporate or juridical entity, including financial transactions involving Overseas Filipino

Workers (OFWs), in order to promote access of Filipinos to services offered by formal financial institutions, particularly those residing in the remote areas, as well as to encourage and facilitate remittances of OFWs through the banking system:

(1) Customers and the authorized signatory/ies of a corporate or juridical entity who engage in a financial transaction with covered institutions for the first time shall be required to present the original and submit a clear copy of at least one (1) valid photo-bearing ID document issued by an official authority.

For this purpose, the term *official authority* shall refer to any of the following:

a. Government of the Republic of the Philippines;
b. Its political subdivisions and instrumentalities;
c. GOCCs; and
d. Private entities or institutions registered with or supervised or regulated either by the BSP, SEC or IC.

Valid IDs include the following:

1. Passport including those issued by foreign governments
2. Driver's license
3. PRC ID
4. NBI clearance
5. Police clearance
6. Postal ID
7. Voter's ID
8. Tax Identification Number
9. Barangay certification
10. GSIS e-Card
11. SSS card
12. Senior Citizen card
13. OWWA ID
14. OFW ID
15. Seaman's book
16. Alien Certification of Registration/Immigrant Certificate of Registration
17. Government office and GOCC ID (e.g., AFP, HDMF IDs)
18. Certification from the NCWDP
19. DSWD certification
20. IBP ID; and
21. Company IDs issued by private entities or institutions registered with or supervised or regulated either by the BSP, SEC or IC.

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

(3) Where the customer or authorized signatory is a non-Philippine resident, similar IDs duly issued by the foreign government where the customer is a resident or a citizen may be presented.

(4) A covered institution shall require their customers or authorized signatory to submit a clear copy of one (1) valid ID on a one-time basis only at the commencement of business relationship. They shall require their clients to submit an updated photo and other relevant information on the basis of risk and materiality.

(5) A covered institution may classify identification documents based on its reliability and ability to validate the information indicated in the identification document with that provided by the customer.

(6) Whenever it deems necessary, a covered institution may accept other IDs not enumerated above provided that it shall not be the sole means of identification.

(7) In case the identification documents mentioned above or other identification documents acceptable to the covered institution 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, a covered institution may utilize its own technology to take the photo of the customer or authorized signatory.

§ X806.2.d. Outsourcing of the gathering of minimum information and/or documents- Except for deposit taking, which is an inherent banking function that cannot be outsourced and subject to existing rules on outsourcing of specified banking activities, a covered institution may, without prior Monetary Board approval, outsource to a counter-party, which may or may not be a covered institution as herein defined, the gathering of the minimum information and/or documents required to be obtained by these Rules provided that the ultimate responsibility for knowing the customer and for keeping the identification documents shall lie with the covered institution and compliance with the following conditions:

For covered institution counter-party:

1. There is a written service level agreement approved by the board of directors of both covered institutions;
2. The counter-party has a reliable and acceptable customer identification system and training program in place; and
3. In line with requirement no. 1, all identification information and/or documents shall be turned over within a period not exceeding ninety days (90) calendar days to the covered institution, which shall carefully review the documents and conduct the necessary risk assessment of the customer.

For non-covered institution counter-party:

1. All conditions required for covered institution counter-party;

2. The covered institution outsourcing the activity shall likewise ensure that the employees or representatives of the counter-party establishing the true and full identity of the customer undergo equivalent training program as that of the covered institution's own employees undertaking a similar activity.

3. Annual monitoring and review by the covered institution of the performance of the counter-party to assist it in determining whether or not to continue with the arrangement.

§ X806.2.e. Trustee, Nominee, Agent or Intermediary account- Where any transaction is conducted by a trustee, nominee, agent or intermediary, either as an individual or through a fiduciary relationship, a corporate vehicle or partnership, on behalf of a trustor, principal, beneficial owner or person on whose behalf a transaction is being conducted, covered institutions shall establish and record the true and full identity and existence of both the (1) trustee, nominee, agent or intermediary and the (2) trustor, principal, beneficial owner or person on whose behalf the transaction is being conducted. The covered institution 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 it entertains doubts as to whether the trustee, nominee, agent, or intermediary is being used as a dummy in circumvention of existing laws, it shall apply enhanced due diligence in accordance with **§ X806.1.b.**

§ X806.2.e.1. Where the Customer Transacts Through a Trustee, Nominee, Agent or Intermediary which is a Third Party as herein defined (Third Party Reliance)- A covered institution may rely on the customer identification process undertaken by a third party. For purposes of this Subsection, the "third party" shall refer to a (1) covered institution as herein specifically defined and as generally defined by AMLA, as amended, and its RIRR, or (2) a financial institution operating outside the Philippines that is covered by equivalent customer identification requirements. A BSP-accredited custodian may likewise rely in accordance with these Rules on the face-to-face contact and gathering of minimum information to establish the existence and full identity of the customer conducted by the seller or issuer of securities or by the global custodian provided the latter has an equivalent customer identification requirements.

§ X806.2.e.1.a. Third Party is a covered institution specifically defined by these Rules and as generally defined by AMLA, as amended, and its RIRR - A covered institution may rely on the identification process conducted by this third party provided that the covered institution shall obtain from the third party a written sworn certification containing the following:

1. The Third Party has conducted the requisite customer identification requirements in accordance with these Rules and its own MLPP including the face-to-face contact requirement to establish the existence of the

ultimate customer and has in its custody all the minimum information and/or documents required to be obtained from the customer; and

2. The relying covered institution shall have the ability to obtain identification documents from the Third Party upon request without delay.

§ X806.2.e.1.b. Third Party is a financial institution operating outside the Philippines that is other than covered institutions referred to in § X806.2.e.1.a. but conducts business operations and activities similar to them - All the contents required in the sworn certification mentioned in **§ X806.2.e.1.a.** 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 to determine from publicly available information the reputation of the institution and the quality of supervision, including whether it has been subject to money laundering or terrorist financing 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.

§ X806.2.f. Private banking/ Wealth Management operations- These services, which by their nature involve high measure of client confidentiality, are more open to the elements of reputational risk especially if the customer identification process is not diligently followed. Covered institutions therefore shall endeavor to establish and record the true and full identity of these customers and establish a policy on what standard of due diligence will apply to them. They shall also require approval by a senior officer other than the private banking/ wealth management/ similar activity relationship officer or the like for acceptance of customers of private banking, wealth management and similar activities.

§ X806.2.g. Politically Exposed Person- A covered institution shall endeavor to establish and record the true and full identity of PEPs as well as their immediate family members and the entities related to them and establish a policy on what standard of due diligence will apply to them taking into consideration their position and the risks attendant thereto.

§ X806.2.h. Correspondent banking- Because of the risk associated with dealing with correspondent accounts where it may unknowingly facilitate the transmission, or holding and management of proceeds of unlawful activities or funds intended to finance terrorist activities, covered institutions shall adopt policies and procedures for correspondent banking activities and designate an officer responsible in ensuring compliance with these policies and procedures. A covered institution may rely on the

customer identification process undertaken by the respondent bank. In such case, it shall apply the rules on Third Party reliance under **§ X806.2.e.1.**, treating the respondent bank as the Third Party as defined therein. In addition, the correspondent bank shall:

(a) Gather sufficient information about the respondent institution to understand fully the nature of the respondent's business and to determine from publicly available information the reputation of the institution and the quality of supervision, including whether it has been subject to money laundering or terrorist financing investigation or regulatory action.

(b) Assess the respondent institution's anti-money laundering and terrorist financing controls.

(c) Obtain approval from senior management before establishing correspondent relationships.

(d) Document the respective responsibilities of each institution.

(e) With respect to "payable-through accounts", be satisfied that the respondent bank has verified the identity of, and performed on-going due diligence on, the customers having direct access accounts of the correspondent and that it is able to provide relevant customer identification data upon request by the correspondent bank.

Correspondent banking customers presenting greater risk, including shell companies, shall be subject to enhanced due diligence.

§ X806.2.i. Fund/Wire transfer- Because of the risk associated with dealing with fund/wire transfers, where a covered institution may unknowingly transmit proceeds of unlawful activities or funds intended to finance terrorist activities, it shall establish policies and procedures designed to prevent it from being utilized for that purpose which shall include, but not limited to, the following:

(a) The beneficiary institution shall not accept instructions to pay-out fund transfers to non-customer beneficiary, unless it has conducted the necessary customer due diligence to establish the true and full identity and existence of said beneficiary. Should the originator and beneficiary be the same person, the beneficiary institution may rely on the customer due diligence conducted by the originating institution provided the rules on Third Party reliance under **§ X806.2.e.1.** are met, treating the originating institution as Third Party as therein defined;

(b) The originating institution 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 said originator;

(c) In cross border transfers, if the originator is a high risk customer as herein described, the beneficiary institution shall conduct enhanced due

diligence on the beneficiary and the originator. 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 beneficiary institution shall refuse to effect the fund/wire transfer or the pay-out of funds without prejudice to the reporting of a suspicious transaction to the AMLC when circumstances warrant;

(d) Whenever possible, manually initiated fund transfer (MIFT) instructions should not be the primary delivery method. Every effort shall be made to provide client with an electronic banking solution. However, where MIFT is utilized, the existing rules on validation procedures as prescribed by Circular No. 436 dated 18 June 2004 shall apply;

(e) Cross border and domestic fund/wire transfers and related message amounting to P50,000 or more or its equivalent shall include accurate and meaningful originator information. The following are the originator information that shall remain with the transfer or related message through the payment chain:

1. Name of the originator;
2. Address or in its absence the national identity number or date and place of birth of the originator; and
3. Account number of the originator or in its absence, a unique reference number must be included.

(f) Should any wire transfer amounting to P50,000 or more or its equivalent be unaccompanied by the required originator information, the beneficiary institution shall exert all efforts to establish the true and full identity and existence of the originator by requiring additional information from the originating institution or intermediary institution. It shall likewise apply enhanced due diligence to establish the true and full identity and existence of the beneficiary. 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 beneficiary institution shall refuse to effect the fund/wire transfer or the pay-out of funds without prejudice to the reporting of a suspicious transaction to the AMLC when circumstances warrant.

§ X806.2.j. Buyers of Cashier's, Manager's or Certified Checks- A covered institution may sell Cashier'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 and the number of the check;
4. Name of the payee;
5. Amount; and
6. Purpose of such transaction.