



BANGKO SENTRAL NG PILIPINAS

OFFICE OF THE DEPUTY GOVERNOR | FINANCIAL SUPERVISION SECTOR

CIRCULAR LETTER NO. CL-2022-078

To : **All BSP-Supervised Financial Institutions (BSFIs)**

Subject : **Anti-Money Laundering Council (AMLC) Regulatory Issuance No. 4, Series of 2022 - Rules and Regulations Implementing (RRI) Section 9(d) of Republic Act (RA) No. 9208, as amended by RA No. 11862, otherwise known as the Expanded Anti-Trafficking in Persons Act of 2022 (ATIP)**

This is to disseminate the AMLC Rules and Regulations Implementing (RRI) Section 9(d) of the Expanded ATIP of 2022¹ which took effect on 28 October 2022.

The RRI focuses on two major items, namely the (1) reporting of suspicious activities and transactions, and (2) bank inquiry and access to non-bank financial records. As to the reportorial requirements section, it covers (a) reporting of suspicious activities to law enforcement agencies, (b) reporting of suspicious transaction reports to the AMLC, and (c) suspicious circumstances and red flag indicators. On the other hand, the access to financial records covers bank inquiry and financial records not covered by the bank deposit secrecy laws.

All BSFIs are enjoined to comply with the obligations of covered persons under the RRI within the timelines prescribed therein.

For implementation and strict compliance.


CHUCHI G. FONACIER
Deputy Governor

Digitally signed by Chuchi G.
Fonacier
Date: 2022.11.16 14:31:27
+08'00'

16 November 2022

¹ www.amlc.gov.ph/news-and-announcements/16-news-and-announcements/410-rules-and-regulations-implementing-section-9-d-of-republic-act-no-9208-as-amended-by-republic-act-no-11862-otherwise-known-as-the-expanded-anti-trafficking-in-persons-act-of-2022?tmpl=component&print=1&page= The set of rules was published in Business World and filed in the Office of the National Administrative Register on 13 October 2022.



ANTI-MONEY LAUNDERING COUNCIL

REGULATORY ISSUANCE NO. 4 Series of 2022

RULES AND REGULATIONS IMPLEMENTING SECTION 9(D) OF REPUBLIC ACT NO. 9208, AS AMENDED BY REPUBLIC ACT NO. 11862, OTHERWISE KNOWN AS THE EXPANDED ANTI-TRAFFICKING IN PERSONS ACT OF 2022

Pursuant to Section 9(d) of Republic Act No. 9208, as amended by Republic Act No. 11862, otherwise known as the *Expanded Anti-Trafficking in Persons Act of 2022*, the Anti-Money Laundering Council (AMLAC) issues and promulgates the following set of rules and regulations:

Chapter I. General Provisions

- Rule 1 – Title, Purpose, Coverage, and Policies
- Rule 2 – Definition of Terms

Chapter II. Reporting Suspicious Activities and Transactions

- Rule 3 – Reporting to Law Enforcement Agencies
- Rule 4 – Reporting to the Anti-Money Laundering Council
- Rule 5 – Suspicious Transactions and Activities

Chapter III. Bank Inquiry and Access to Other Financial Information

- Rule 6 – Bank Inquiry
- Rule 7 – Access to Other Financial Information

Chapter IV. Miscellaneous Provisions

- Rule 8 – Compliance and Administrative Sanctions
- Rule 9 – Transitory, Separability, and Effectivity Clauses

**CHAPTER I
GENERAL PROVISIONS**

RULE 1 – TITLE, PURPOSE, COVERAGE, AND POLICIES

Section 1. Title.

This set of rules and regulations shall be known as the “Rules and Regulations Implementing Section 9(d) of Republic Act No. 9208, as amended by Republic Act No. 11862, otherwise known as the Expanded Anti-Trafficking in Persons Act of 2022”.

Section 2. Purpose and Coverage.

2.1. These set of rules and regulations is promulgated to provide the details of implementation of Section 9(d) of Republic Act No. 11862.

2.2. This set of rules and guidelines covers the following:

- (a) Reporting of any suspected trafficking in persons-related activity or transaction; and
- (b) Procedure for conducting bank inquiry, or requiring financial intermediaries, internet payment system providers, and other financial facilitators to provide financial documents and information.

Section 3. State Policies

The provisions of this set of rules and regulations in line with the following State Policies:

- (a) Give the highest priority to the enactment of measures and development of programs that will promote human dignity, protect the people from any threat of violence and exploitation, and eliminate trafficking in persons.
- (b) Ensure that the Philippines shall not be used as a money laundering site for the proceeds of any unlawful activity.

RULE 2 – DEFINITION OF TERMS

Section 1. Definitions.

For purposes of this set of rules and regulations, the following terms are hereby defined as follows:

- (a) **“Account”** refers to a bank account, electronic money account, investment account, insurance policy, membership account, and other similar contract or service agreement, or business relationship between a covered person and its customers where funds or any monetary instrument of the latter are held by the former.
- (b) **“Anti-Money Laundering Act”** (AMLA) refers to Republic Act No. 9160, otherwise known as the Anti-Money Laundering Act of 2001, as amended by Republic Act No. 9194, 10167, 10365, 10927, and 11521.
- (c) **“Beneficiary”** refers to:
 - (1) *General*: any person for whose benefit an account was created or transaction was made.
 - (2) *For trust agreements*: any person for whose benefit the trust has been created.
 - (3) *For life insurance or investment-linked insurance policies*: any person who will be paid the policy proceeds.
 - (4) *For wire transfers*: refers to a person or legal arrangement who is identified by the originator as the receiver of the requested wire transfer.
- (d) **“Child Sexual Abuse and Exploitation Material or Child Sexual Abuse Material”** (CSAEM or CSAM) refers to photos, images, videos, recordings, streams, or any other representation or form of media, depicting acts of sexual abuse and exploitation of a child or representation of a child as a sexual object whether or not digitally or by, through, and with the use of information and communications technology. It shall also include materials that focus on real or simulated genitalia or other private body parts of a child.
- (e) **“Covered Persons”** refer to the covered persons under Section 3(a) of the AMLA.
- (f) **“Customer/Client”** refers to any person who keeps or maintains an account, or

otherwise transacts business with a covered person. It includes the following:

- (1) 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;
- (2) Transactors, agents and other authorized representatives of beneficial owners;
- (3) Beneficiaries of trusts, investment and pension funds, insurance policies, and remittance of transactions;
- (4) Persons whose assets are managed by an asset manager;
- (5) Trustors/grantors/settlors of a trust;
- (6) Insurance policy holders, whether actual or prospective; and
- (7) Juridical persons.

For purposes of this set of rules and regulations, the term juridical person shall refer to an entity other than a natural person as defined under the Civil Code of the Philippines, including corporate clients who keep or maintain an account with a covered person.

- (g) **“Customer Due Diligence”** (CDD) refers to the procedure of identifying and verifying the true identity, of customers, and their agents and beneficial owners, including understanding and monitoring of their transactions and activities.
- (h) **“Electronic Money”** (E-money) refers to a monetary value represented by a claim on its issuer that is:
 - (1) Electronically stored in an instrument or device;
 - (2) Issued against receipt of funds of an amount not lesser in value than the monetary value issued;
 - (3) Accepted as means of payment by persons or entities other than the issuer; and
 - (4) Withdrawable in cash or cash equivalent
- (i) **“Electronic Money Issuers”** (EMI) refer to entities accepting e-money as a retail payment medium such as banks, non-banking financial institutions, and non-bank

institutions registered with the Bangko Sentral ng Pilipinas as a monetary transfer agent.

- (j) **“Expanded Anti-Trafficking in Persons Act”** (Expanded Act) refers to Republic Act No. 11862 otherwise known as the Expanded Anti-Trafficking in Persons Act of 2022 (ATIP).
- (k) **“Financial Intermediary”** refers to a person or entity whose principal functions include lending, investing or placement of funds or evidence of indebtedness or equity deposited with them, acquired by them, or otherwise coursed through them either for their own account or for the account of others.

For purposes of this set of rules and regulations, this term shall be interchangeably used with the term “covered persons” under the supervision or regulation of the Bangko Sentral ng Pilipinas, Securities and Exchange Commission, and Insurance Commission, as defined under Section 3(a) of the AMLA.

- (l) **“Information and Communications Technology”** (ICT) refers to the totality of electronic means to access, create, collect, store, process, receive, transmit, present, and disseminate information.
- (m) **“Inter-Agency Council Against Trafficking”** (IACAT) refers to the government body mandated by law to coordinate and oversee the implementation of Republic Act No. 9208, or the Anti-Trafficking in Persons Act of 2003, as amended.
- (n) **“Internet-based Payment System Provider”** refers to a person or entity that provides mechanisms for customers to access, via the Internet, pre-funded accounts which can be used to transfer the electronic money or value held in those accounts to other individuals or businesses which also hold accounts with the same provider.
- (o) **“Law Enforcement Agency”** (LEA) refers to Philippine National Police, National Bureau of Investigation, and other government agencies that are responsible for the prevention, investigation, apprehension and/or detention of individuals suspected of, or convicted for, violation of the Expanded Act.
- (p) **“Money Laundering”** (ML) refers to the crime defined under Section 4 of the AMLA.
- (q) **“Money or Value Transfer Service”** (MVTs) refers to the financial services that involve the acceptance of cash, checks, other monetary instruments or other stores of value, and the payment of a corresponding sum in cash or other form to a beneficiary by means of a communication, message, transfer, or through a clearing network to which the service provider belongs.

- (r) **“Money Service Business”** (MSB) refer to entities engages in remittance, money changing and/or foreign exchange dealing
- (s) **“Occurrence”** refers to the date of establishment of suspicion or determination of the suspicious nature of the transaction.
- (t) **“Online Sexual Abuse and Exploitation”** (OSAEC) refers to the use of digital or analog communication and ICT as means to abuse and exploit children sexually, which includes cases in which contact child abuse or exploitation offline is combined with an online component. This can also include the production, dissemination, and possession of CSAEM or CSAM; online grooming of children for sexual purposes; sexual extortion of children; sharing image-based sexual abuse; commercial sexual exploitation of children; exploitation of children through online prostitution; and live-streaming of sexual abuse, with or without the consent of the victim.
- (u) **“Other Financial Facilitators”** refers to other persons or entities that facilitate financial transactions between parties.
- (v) **“Person”** refers to any natural or juridical person.
- (w) **“Persons Related to a Financial Intermediary”** refer to other persons, including outsourced personnel and service providers, providing services to support the operations of the Financial Intermediary but falls outside the scope of Person Working for the Financial Intermediary
- (x) **“Persons Working for a Financial Intermediary”** refer to the employees of the Financial Intermediary.
- (y) **“Qualified Trafficking in Persons”** (Qualified Trafficking) refers to Section 6 of the Expanded Act.
- (z) **“Related Account”** refers to an account, the funds and sources of which directly originated from and/or are materially-linked to the monetary instruments or properties subject of the freeze order or an order of inquiry.
- (aa) **“Suspicious Circumstance”** refers to any of the following circumstances, the existence of which makes a transaction suspicious:
 - (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;
 - (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 covered person;
 - (6) The transaction is in any way related to ML/TF or TIP that is about to be committed, is being or has been committed; or
 - (7) Any transaction that is similar, analogous or identical to any of the foregoing, such as the relevant transactions in related and materially-linked accounts.
- (bb) **"Suspicion"** refers to a person's state of mind – based on his skills, experience, and/or understanding of the customer profile – which considers that there is a possibility that any of the suspicious circumstances exist.
- (cc) **"Suspicious Transaction"** refers to a transaction, regardless of amount, where any of the suspicious circumstances, as herein defined, is determined, based on suspicion or, if available, reasonable grounds, to be existing.
- (dd) **"Suspicious Transaction Report"** (STR) refers to a report on a suspicious transaction, as herein defined, filed by a covered person before the AMLC.
- (ee) **"Terrorism Financing"** (TF) refers to the crime defined under Sections 4 of RA No. 10168 otherwise known as the Terrorism Financing Prevention and Suppression Act (TFPSA).
- (ff) **"Trafficking in Persons"** (TIP) refers to any of the acts as enumerated in Sections 4 and 5 of the Expanded Act.
- (gg) **"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.

- (hh) **“Virtual Asset”** (VA) refers to a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes.
- (ii) **“Virtual Asset Service Provider”** (VASP) refers to any person who, as a business, conducts one or more of the following activities or operations for or on behalf of another person:
 - (a) Exchange between virtual assets and fiat currencies;
 - (b) Exchange between one or more forms of virtual assets;
 - (c) Transfer (the conduct of a transaction on behalf of another person that moves a virtual asset from one virtual asset address or account to another) of virtual assets;
 - (d) Safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and
 - (e) Participation in and provision of financial services related to an issuer’s offer and/or sale of a virtual asset.
- (jj) **“Wire Transfer”** refers to any transaction carried out on behalf of an originator, through an originating/ordering financial institution, by electronic means, with a view to making an amount of funds available to a beneficiary at a beneficiary financial institution, irrespective of whether the originator and the beneficiary are the same person.

CHAPTER II

REPORTING SUSPICIOUS ACTIVITIES AND TRANSACTIONS

RULE 3

REPORTING TO LAW ENFORCEMENT AGENCIES

Section 1. Reporting of TIP-related Financial Activity or Transaction to the LEAs.

1.1. Reporting to LEAs.

The following persons or entity shall have the duty to report any suspected trafficking in persons-related activity or transaction to the concerned LEAs:

- a. Financial intermediary;
- b. Person working for a financial intermediary;
- c. Person related to a financial intermediary; or
- d. Person who has direct knowledge of any TIP-related financial activity or transaction conducted through a financial intermediary.

1.2. *Creation of a Reporting Portal.*

To facilitate the reporting of any TIP-related financial activity or transaction conducted through a financial intermediary and avoid duplication of reporting to multiple LEAs, the concerned LEAs, through the IACAT, shall create a centralized reporting portal accessible to all concerned the LEAs and financial intermediaries. It shall also have a mechanism to accept reports from any person working for, related to, or who has direct knowledge of any TIP-related financial activity or transaction conducted through a financial intermediary.

Pending the creation of a reporting portal, reports shall be filed manually or electronically to the LEA offices or e-mail addresses to be determined by the concerned LEAs and to be announced by the IACAT and AMLC, through their respective advisories.

Section 2. Safe Harbor Provision.

No administrative, criminal, or civil proceedings shall lie against any person for having made a report on TIP-related financial activity or transaction conducted through a financial intermediary in the regular performance of his duties (for financial intermediaries) and in good faith (for financial intermediaries and other reporting persons), whether or not such reporting results in any criminal prosecution under the AMLA or the Expanded Act.

RULE 4
REPORTING TO THE ANTI-MONEY LAUNDERING COUNCIL

Section 1. Suspicious Transaction Reporting Framework.

When reporting TIP-related STRs to the AMLC, covered persons shall follow the suspicious transaction reporting framework under the AMLA and the registration and reporting guidelines of the AMLC.

Section 2. Reporting of Suspicious Transactions to the AMLC.

Rules and Regulations Implementing Section 9(d) of Republic Act No. 9208, as amended by Republic Act No. 11862, otherwise known as the Expanded Trafficking in Persons Act of 2022

2.1. *Filing of STRs.*

Covered persons shall file all STRs, in accordance with the registration and reporting guidelines of the AMLC. STRs shall cover all transactions, whether completed or attempted.

2.2. *Timing of Reporting*

STRs shall be promptly filed within the next working day from occurrence thereof, which for purposes of this Rule, shall be the date of establishment of suspicion or determination of the suspicious nature of the transaction.

2.3. *Quality and Form of Reports*

- (a) Covered persons shall ensure the completeness, accuracy, and timeliness of the STRs.
- (b) STRs shall be filed in such form as may be prescribed by the AMLC and shall be submitted in a secured manner to the AMLC in electronic form.

Section 3. Registration with the AMLC.

Covered persons shall register with the AMLC's electronic reporting system in accordance with the registration and reporting guidelines.

Section 4. TIP Monitoring System

4.1. *Establishing and Maintaining TIP Monitoring System*

All covered persons shall adopt a TIP monitoring system that is appropriate for their risk profile and business complexity. 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 compliance with the Expanded Act.

For this purpose, covered persons may use their existing anti-money laundering/counter-terrorism financing (AML/CTF) monitoring system to monitor TIP-related risks and transactions, *Provided*, that it is recalibrated to specifically monitor TIP-related transactions and activities.

4.2. *Electronic Monitoring*

- (a) Complex covered persons, as determined by their supervising authorities, shall adopt an electronic TIP system for monitoring risks as well as generating timely reports for the guidance and information of its board of directors and senior management.
- (b) The system must have, at least, the following automated functionalities:
 - (1) STR Monitoring – performs statistical analysis, profiling and able to detect unusual patterns of account activity;
 - (2) Watchlist Monitoring – checks transfer parties (originator, beneficiary, and narrative fields) and the existing customer database for any listed undesirable individual or corporation;
 - (3) Investigation – checks for given names throughout the history of payment stored in the system;
 - (4) Provides a complete audit trail;
 - (5) Capable of aggregating activities of a customer with multiple accounts on a consolidated basis for monitoring and reporting purposes; and
 - (6) Capable of recording all suspicious transactions and support the investigation of alerts generated by the system and brought to the attention of senior management whether or not a report was filed with the AMLC.
- (c) Covered persons with an existing electronic system of flagging and monitoring transactions in place shall ensure that their existing system is updated.

4.3. *Manual Monitoring*

Covered persons not required to have an electronic system of flagging and monitoring transactions, as determined by their Supervising Authorities, shall ensure that they have the means of flagging and monitoring the TIP-related transactions. They shall be maintain a register of all transactions that have been brought to the attention of senior management, whether or not the same was reported to the AMLC.

Section 5. Confidentiality Clause.

All STRs are considered as confidential information. Covered persons, their officers and employees are prohibited from communicating, directly or indirectly, in any manner or by any means, to any person or entity, the media, the fact that a suspicious transaction has been or is about to be reported, the contents of the report or any information related thereto.

Section 6. Safe Harbor Provision.

No administrative, criminal, or civil proceedings shall lie against any person for having made an STR in the regular performance of one's duties and in good faith, whether or not such reporting results in any criminal prosecution under the AMLA or the Expanded Act.

Section 7. AMLC Registration and Reporting Guidelines.

Covered persons shall ensure compliance with the registration and reporting guidelines issued by the AMLC in complying with their obligations under Chapter II hereof.

RULE 5 – SUSPICIOUS TRANSACTIONS AND ACTIVITIES

Section 1. Suspicious Transactions.

Any transaction, regardless of amount, where any of the following suspicious circumstances, is determined, based on suspicion or, if available, reasonable grounds, to be existing shall be reported to the AMLC:

- (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 structured in order to avoid being the subject of reporting requirements under the AMLA;

- (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 with the covered person;
- (f) The transaction is in any way related to ML/TF or TIP that is about to be committed, is being or has been committed; or
- (g) Any transaction that is similar, analogous or identical to any of the foregoing, such as the relevant transactions in related and materially-linked accounts.

Section 2. Red Flag Indicators.

Covered persons shall consider the red flag indicators in determining the existence of suspicious circumstances, which shall warrant the filing of STRs before the AMLC. By using a combination of broad primary indicators, followed by specific secondary indicators, and combined with the institutional knowledge about AMLA regulations and issuances, covered persons shall identify reportable financial transactions and activities related to TIP and report it to AMLC.

Section 3. Primary Financial Transaction Indicators.

3.1 *Financial Transaction Indicators for Possible Victims of TIP.*

The covered person shall recognize the following financial transaction indicators for its clients:

- (a) The client incurs and declares a number of excessive continued expenses over an extended period of time such as, but not limited to bookings for airline tickets, payments transport network vehicle services, tickets for land or sea transportation, lodging expenses of a property, sustenance allowance, or maintenance of a rented location.
- (b) The client receives third party cash deposits or wire transfers from various individuals that are excessive and do not appear to be commensurate client's business or financial capacity.
- (c) The staff of the financial institution observes and detects coercive or forced behavior from their client. Unusual behaviors such as, but not limited to, another person accompanying the client and exerting control by checking deposits/statements, paying in high volumes of cash, or using automated machines to avoid the counters.

- (d) Client receives transactions from an identified suspect for TIP.
- (e) Beneficiary and/or sender is under investigation by LEAs for being a suspected facilitator of TIP/OSAEC, in possession of CSAEM, or with known association or transactions with TIP/OSAEC offenders.

3.2 Financial Transaction Indicators for Probable Perpetrators or Offenders.

The covered person shall recognize the following financial transaction indicators for perpetrators or offenders:

- (a) The sender is a foreigner and makes relatively low-value international or domestic remittances to a large number of beneficiaries with unjustified purpose and unknown relationship.
- (b) Inconsistencies between the client's purpose and the beneficiary do not match such as but not limited to, declaring the purpose for gifts to friends but beneficiaries claim that the purpose is for allowance, business, miscellaneous fees from a friend or an older individual.
- (c) The client sends to individuals, notably minors, located in identified hotspots in the Philippines particularly in mostly rural or depressed areas.
- (d) The client spends money on websites linked to TIP activities.

Section 4. Secondary Indicators.

Any or a combination of the following secondary indicators shall be combined with the primary indicators to identify and report suspicious transactions:

- (a) There is a swift or abrupt increase in the volume and amount of transactions overtime.
- (b) Frequent account transfers between the client's bank accounts and credit card, frequent purchases at online gaming sites, Bitcoin transactions/exchanges, payment processors, sports collectable stores, and money transfers with various individuals with unknown source and purpose.
- (c) Beneficiary is unemployed and relies on remittances as sources of income.

Rules and Regulations Implementing Section 9(d) of Republic Act No. 9208, as amended by Republic Act No. 11862, otherwise known as the Expanded Trafficking in Persons Act of 2022

- (d) There is a significant turnover/frequency of transactions in the account despite the client status is unemployed.
- (e) Remittances come from wire transfers or the use of money service businesses (MSB).
- (f) The money transfers through e-money issuers (EMIs) are made through mobile applications/online.
- (g) Remittances come from different branches of an MSB or EMI within the same province or city.
- (h) Beneficiaries claim remittances at least four times a month or at least twice a week from the same MSB.
- (i) Automatic Teller Machine (ATM) usage often occurred at the same machine at the same time suggesting that a third party is in control of their card.
- (j) The account is made as a pass-through account when the source of fund is immediately remitted to another individual with unknown source and purpose.
- (k) Multiple beneficiaries (victims) sharing bank account information, such as address and phone number.
- (l) Use of multiple bank accounts and credit cards, as well as multiple alias identities and addresses.
- (m) Use of ATM and credit cards and fund transfer at times inconsistent with normal operating hours for the business.
- (n) Client receives multiple international remittances from foreign nationals who appear to have sent multiple transactions to different Filipino individuals.
- (o) Other similar or analogous circumstances that would lead a person to a suspicion that its client committed, is committing, or about to commit TIP or other violations of the Extended Act.

Section 5. Other Transactional/Financial Red Flags.

Covered persons may also consider the following TIP-related behaviors observable during account activity:

- (a) A business customer does not exhibit normal payroll expenditures (e.g., wages, payroll taxes, social security contributions). Payroll costs can be non-existent or extremely low for the size of the customer's alleged operations, workforce and/or business line/model.
- (b) Substantial deductions to wages. To the extent a financial institution is able to observe, a customer with a business may deduct large amounts from the wages of its employees alleging extensive charges (e.g., housing and food costs), where the employees only receive a small fraction of their wages; this may occur before or after the payment of wages.
- (c) Cashing of payroll checks where the majority of the funds are kept by the employer or are deposited back into the employer's account. This activity may be detected by those financial institutions that have access to paystubs and other payroll records.
- (d) The following two red flags may signal anomalous customer activity; however, they should be applied in tandem with other indicators when determining whether transactions are linked to human trafficking.
 - (1) Transactional activity (credits and/or debits) inconsistent with a customer's alleged employment, business or expected activity, or where transactions lack a business or apparent lawful purpose.
 - (2) Cash deposits or wire transfers are in the amount of PHP500,000.00 (or its equivalent in foreign currency) or below in apparent efforts to avoid the filing of Covered Transaction Reports (CTRs) with the AMLC.
- (e) Frequent outbound wire transfers, with no business or apparent lawful purpose, directed to countries at higher risk for human trafficking¹ or to countries that are inconsistent with the customer's expected activity
- (f) A customer's account appears to function as a funnel account, where cash deposits occur in cities/states where the customer does not reside or conduct business. Frequently, in the case of funnel accounts, the funds are quickly withdrawn (same day) after the deposits are made.

Rules and Regulations Implementing Section 9(d) of Republic Act No. 9208, as amended by Republic Act No. 11862, otherwise known as the Expanded Trafficking in Persons Act of 2022

- (g) Multiple, apparently unrelated, customers sending wire transfers to the same beneficiary. These wire senders may also use similar transactional information including but not limited to a common address and phone number. When questioned to the extent circumstances allow, the wire senders may have no apparent relation to the recipient of the funds or know the purpose of the wire transfers
- (h) Transactions conducted by individuals, escorted by a third party (e.g., under the pretext of requiring an interpreter), to transfer funds (that may seem to be their salaries) to other countries.
- (i) Frequent payments to online escort services for advertising, including small posting fees to companies of online classifieds as well as more expensive, higher-end advertising and website hosting companies.
- (j) Frequent transactions, inconsistent with expected activity and/or line of business, carried out by a business customer in apparent efforts to provide sustenance to individuals (e.g., payment for housing, lodging, regular vehicle rentals, purchases of large amounts of food).
- (k) Payments to employment or student recruitment agencies that are not licensed/registered or that have labor violations.
- (l) Customers frequently appear to move through, and transact from, different geographic locations in the Philippines. These transactions can be combined with travel and transactions in and to foreign countries that are significant conduits for human trafficking.
- (m) Transactions are inconsistent with a customer's expected activity and/or line of business in an apparent effort to cover trafficking victims' living costs, including housing (e.g., hotel, motel, short-term rentals, or residential accommodations), transportation (e.g., airplane, taxi, limousine, or rideshare services), medical expenses, pharmacies, clothing, grocery stores, and restaurants, to include fast food eateries.
- (n) Transactional activity largely occurs outside of normal business operating hours (e.g., an establishment that operates during the day has a large number of transactions at night), is almost always made in cash, and deposits are larger than what is expected for the business and the size of its operations.

- (o) A customer frequently makes cash deposits with no Automated Clearing House (ACH) payments.
- (p) An individual frequently purchases and uses prepaid access cards.
- (q) A customer's account shares common identifiers, such as a telephone number, email, and social media handle, or address, associated with escort agency websites and commercial sex advertisements.
- (r) Frequent transactions with online classified sites that are based in foreign jurisdictions.
- (s) A customer frequently sends or receives funds via cryptocurrency to or from darknet markets or services known to be associated with illicit activity. This may include services that host advertising content for illicit services, sell illicit content, or financial institutions that allow prepaid cards to pay for cryptocurrencies without appropriate risk mitigation controls.
- (t) Frequent transactions using third-party payment processors that conceal the originators and/ or beneficiaries of the transactions.
- (u) A customer avoids transactions that require identification documents or that trigger reporting requirements.

Section 6. Other Customer Interaction/Behavioral Red Flags.

Covered persons may also consider the following TIP-related behaviors observed while interacting with the public:

- (a) A customer establishes an account or visits a branch to conduct transactions while always escorted by a third party (e.g., under the pretext of requiring an interpreter). Correspondingly, the third party escorting the customer may always have possession of the customer's ID.
- (b) Common signer(s)/custodian(s) in apparently unrelated business and/or personal accounts. Similarly, common information (e.g., address, phone number, employment information) used to open multiple accounts in different names.

Rules and Regulations Implementing Section 9(d) of Republic Act No. 9208, as amended by Republic Act No. 11862, otherwise known as the Expanded Trafficking in Persons Act of 2022

- (c) Accounts of foreign workers or students where the employer or employment agency serves as a custodian.
- (d) Unexplained/unjustified lifestyle incommensurate with employment or business line. Profits/deposits significantly greater than that of peers in similar professions/business lines.
- (e) Inflows are largely received in cash where substantial cash receipts are inconsistent with the customer's line of business. Extensive use of cash to purchase assets and to conduct transactions.
- (f) A third party speaks on behalf of the customer (a third party may insist on being present and/ or translating).
- (g) A third party insists on being present for every aspect of the transaction.
- (h) A third party attempts to fill out paperwork without consulting the customer.
- (i) A third party maintains possession and/or control of all documents or money.
- (j) A third party claims to be related to the customer, but does not know critical details.
- (k) A prospective customer uses, or attempts to use, third-party identification (of someone who is not present) to open an account.
- (l) A third party attempts to open an account for a minor who is not under parental authority, guardianship, or the person exercising authority over the minor.
- (m) A third party commits acts of physical aggression or intimidation toward the customer.
- (n) A customer shows signs of poor hygiene, malnourishment, fatigue, signs of physical and/or sexual abuse, physical restraint, confinement, or torture.
- (o) A customer shows lack of knowledge of their whereabouts, cannot clarify where they live or where they are staying, or provides scripted, confusing, or inconsistent stories in response to inquiry.

CHAPTER III
BANK INQUIRY AND ACCESS TO OTHER FINANCIAL INFORMATION

RULE 6
BANK INQUIRY

Section 1. Application for Issuance of Bank Inquiry Order.

By authority of the agency heads, the concerned LEA shall file before the competent Regional Trial Court, through the Office of the Solicitor General, a verified *Ex Parte* Application for the Issuance of Bank Inquiry Order to examine or inquire into any particular bank deposit or investment account that is related to TIP or other violations of the Expanded Act.

Section 2. Inquiry Into or Examination of Related Accounts.

A court order *ex parte* must be obtained before any LEA can inquire into the related accounts. The procedure for the *ex parte* application for issuance of bank inquiry order into the principal account shall be the same for that of the related accounts.

Section 3. No Prior Criminal Charge, Pendency of a Case, or Conviction Necessary.

No prior criminal charge, pendency of a case, or conviction for any TIP-related offense is necessary for the filing of an application for issuance of bank inquiry order.

Section 4. Bank Inquiry Order.

Notwithstanding the provisions of Republic Act No. 1405, as amended, Republic Act No. 6426 as amended, Republic Act No. 8791 and other pertinent laws, the LEAs investigating cases of trafficking in persons may inquire into or examine any particular deposit or investment, including related accounts, with any banking institution or non-bank financial institution, upon order of the competent Regional Trial Court based on an *ex parte* application, when it has been established that there is reasonable ground to believe that the bank deposit or investment account, including related accounts involved, are related to TIP or other violations of the Expanded Act.

Section 5. Rule of Procedure for Bank Inquiry under the Expanded Act.

The “Court of Appeals Rule of Procedure in Cases of Bank Inquiry Into or Examination of Deposit or Investment Account Relating to an Unlawful Activity or Money Laundering Offense

under Republic Act No. 9160, as Amended” (A.M. No. 21-03-05-CA) and other relevant provisions of the Rules of Court shall apply suppletorily to the proceedings for the *ex parte* issuance of bank inquiry order under the Expanded Act until the Supreme Court promulgates the specific rule that would apply thereto.

Section 6. Duties of the Covered Persons.

Covered persons shall have the following duties in relation to bank inquiry orders:

- (a) The concerned covered persons shall immediately, upon receipt of the bank inquiry order, give the concerned LEA full access to all information, documents or objects pertaining to the deposit, investment, account and/or transaction.
- (b) Certified true copies of the documents pertaining to deposit, investment, account and/or transaction subject of the bank inquiry shall be submitted to the concerned LEA, within five (5) working days from receipt of the bank inquiry order. Extension of the period of compliance may be allowed upon good causes, *Provided*, that a request to the concerned LEA is submitted before the expiration of the original five (5) working days.
- (c) 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.

RULE 7

ACCESS TO OTHER FINANCIAL INFORMATION

Section 1. Application for Access to Other Financial Information.

By authority of the agency heads, the concerned LEA shall file before the competent Regional Trial Court, a verified *Ex Parte* Application for the Issuance of an Order Allowing Access to Financial Documents and Information not covered by *bank deposit secrecy laws* that are related to TIP or other violations of the Expanded Act.

Section 2. Inquiry Into or Examination of Related Accounts.

A court order *ex parte* must be obtained before any LEA can inquire into the related accounts. The procedure for the *ex parte* application allowing access to the document and information on the principal account shall be the same for that of the related accounts.

Section 3. No Prior Criminal Charge, Pendency of a Case, or Conviction Necessary.

No prior criminal charge, pendency of a case, or conviction for any TIP-related offense is necessary for the filing of an application for issuance of an order allowing access to financial documents and information not covered by *bank deposit secrecy laws*.

Section 4. Order Allowing Access to Financial Information.

The LEAs investigating cases of TIP may require financial intermediaries, internet payment system providers, and other financial facilitators to provide financial documents and information not covered by *bank deposit secrecy laws*, upon order of the competent Regional Trial Court, based on an *ex parte* application, when it has been established that there is reasonable ground to believe that the financial account, including related accounts involved, are related to TIP or other violations of this Act.

Section 5. Rule of Procedure for Accessing Financial Information under the Expanded Act.

The other relevant provisions of the Rules of Court shall apply suppletorily to the proceedings for the issuance of an *ex parte* order allowing access to financial documents and information not covered by *bank deposit secrecy laws* under the Expanded Act until the Supreme Court promulgates the specific rule that would apply thereto.

**CHAPTER 4
MISCELLANEOUS PROVISIONS**

**RULE 8
COMPLIANCE AND ADMINISTRATIVE SANCTIONS**

Section 1. Compliance.

All covered persons shall have written procedures for cooperating and complying with investigations, assessments, directives and orders of the IACAT, the AMLC, the appropriate government agencies and the courts, as the case may be. When the covered person receives a request for information from any competent authority regarding inquiries into potential TIP-related activities, the covered person shall promptly inform the requestor in writing.

Section 2. Administrative Sanctions by the AMLC.

Violations or non-compliance with the suspicious transaction and activity reporting requirements prescribed herein shall subject the erring covered person, its responsible directors, officers, and employees, and other responsible persons to administrative sanctions under the *Rules of Procedure in Administrative Cases under Republic Act No. 9160, as Amended*.

Section 3. Administrative Sanctions by the IACAT. The imposition of the administrative sanctions by the AMLC shall be without prejudice to the imposition of administrative sanctions by the IACAT against the persons responsible for the violations of the requirements of the Expanded Act.

RULE 9 TRANSITORY, SEPARABILITY, AND EFFECTIVITY CLAUSES

Section 1. Transitory Provision.

- 1.1 *For the reporting requirements to the LEAs under Rule 3 hereof:* The AMLC shall, within thirty (30) days from the effectivity of this set of rules and regulations, prescribe the standard reporting template for manual reporting pending the adoption and implementation of a centralized reporting portal.
- 1.2 *For covered persons and entities required to report to the AMLC under Rule 4 hereof:* STRs shall be reported using the procedure, codes, and other reporting requirements for TIP-related transactions prescribed under the *2021 AMLC Registration and Reporting Guidelines*, until the unlawful activities under the Expanded Act are expressly included in the future amendments thereof.
- 1.3 Within one (1) year from the effectivity of this set of rules and regulations, the LEAs, in coordination with the IACAT and the AMLC, shall adopt a central database for the receiving and maintenance of reports to the LEAs.
- 1.4 All covered persons shall adopt or update their TIP-monitoring system within one (1) year from the effectivity of this set of rules and regulations.

Rules and Regulations Implementing Section 9(d) of Republic Act No. 9208, as amended by Republic Act No. 11862, otherwise known as the Expanded Trafficking in Persons Act of 2022

Section 2. Separability Clause.

If any provision of this set of rules and regulations or the application thereof to any person or circumstance is held to be invalid, the other provisions, and the application of such provision to other persons or circumstances, shall not be affected.

Section 3. Effectivity.

This set of rules and regulations shall take effect fifteen (15) days after the completion of its publication in the Official Gazette or a newspaper of general circulation, and filing before the Office of the National Administrative Register (ONAR), University of the Philippines, Diliman, Quezon City.

BY AUTHORITY OF THE AMLC:

(SGD) MATTHEW M. DAVID

Executive Director
Anti-Money Laundering Council

12 October 2022