



**DEPARTMENT OF INTERIOR AND LOCAL GOVERNMENT
AND
ANTI-MONEY LAUNDERING COUNCIL**

**JOINT CIRCULAR NO. ____
Series of ____**

**RULES AND REGULATIONS IMPLEMENTING SECTION 9(C) OF REPUBLIC ACT NO. 11930,
OTHERWISE KNOWN AS THE ANTI-ONLINE SEXUAL ABUSE OR EXPLOITATION OF CHILDREN
(OSAEC) AND ANTI-CHILD SEXUAL ABUSE OR EXPLOITATION MATERIALS (CSAEM) ACT**

Pursuant to Section 9(c) of Republic Act No. 11930, otherwise known as the *Anti-Online Sexual Abuse or Exploitation of Children (OSAEC) and Anti-Child Sexual Abuse or Exploitation Materials (CSAEM) Act*, the Anti-Money Laundering Council (AMLC) 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 Transactions and Activities

- Rule 3 – Reporting to the Department of Justice-Office of Cybercrime
- 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 – Amendments to the Anti-Money Laundering Act
- Rule 9 – Compliance and Administrative Sanctions
- Rule 10 – Transitory, Separability, and Effectivity Clauses

Rules and Regulations Implementing Section 9(c) of Republic Act No. 11930, otherwise known as the Anti-Online Sexual Abuse or Exploitation of Children (OSAEC) and Anti-Child Sexual Abuse or Exploitation Materials (CSAEM) Act

**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(c) of Republic Act No. 11930, otherwise known as the Anti-Online Sexual Abuse or Exploitation of Children (OSAEC) and Anti-Child Sexual Abuse or Exploitation Materials (CSAEM) Act”.

Section 2. Purpose and Coverage.

- 2.1. This set of rules and regulations is promulgated to provide the details of implementation of Section 9(c) of Republic Act No. 11930.
- 2.2. This set of rules and guidelines covers the following:
 - (a) Reporting of any suspected OSAEC and CSAEM related activity or suspicious transaction; and
 - (b) Procedure for conducting bank inquiry, or requiring 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 are in line with the following State Policies:

- (a) To provide special protection to children from all forms of sexual violence, abuse, and exploitation especially those committed with the use of information and communications technology (ICT), provide sanctions for their commission and carry out programs for the prevention, deterrence, and intervention in all situations of online sexual abuse and exploitation of children in the digital and non-digital production, distribution or possession of child sexual abuse or exploitation material.
- (b) Ensure that the Philippines shall not be used as a money laundering site for the proceeds of any unlawful activity.

Rules and Regulations Implementing Section 9(c) of Republic Act No. 11930, otherwise known as the Anti-Online Sexual Abuse or Exploitation of Children (OSAEC) and Anti-Child Sexual Abuse or Exploitation Materials (CSAEM) Act

**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) **“Anti-OSAEC-CSAEM Act”** refers to Republic Act No. 11930, otherwise known as the Anti-Online Sexual Abuse or Exploitation of Children (OSAEC) and Anti-Child Sexual Abuse or Exploitation Materials (CSAEM) Act.
- (d) **“Beneficiary”** refers to any person for whose benefit an account was created or transaction was made. For trust agreements: any person for whose benefit the trust has been created. For life insurance or investment-linked insurance policies: any person who will be paid the policy proceeds. For wire transfers, a beneficiary is a person or a legal arrangement who is identified by the originator as the receiver of the requested wire transfer.
- (e) **“Child”** refers to a person below eighteen (18) years of age or those over but are unable to fully take care of themselves or protect themselves from abuse, neglect, cruelty, exploitation or discrimination because of physical, mental, intellectual or sensory disability or condition. For purposes of this Rule, a child shall also refer to:
 - (1) A person regardless of age who is presented, depicted or portrayed as a child as defined herein; and
 - (2) Computer-generated, digitally or manually crafted images, or graphics of a person who is represented or who is made to appear to be a child as defined herein.

Rules and Regulations Implementing Section 9(c) of Republic Act No. 11930, otherwise known as the Anti-Online Sexual Abuse or Exploitation of Children (OSAEC) and Anti-Child Sexual Abuse or Exploitation Materials (CSAEM) Act

- (f) **“Child Sexual Abuse”** refers to any form of communication through any platform or format, or any physical interaction between a child and any person when the child is being used for any act or activity inducing sexual stimulation or for the purpose of sexual gratification or in pursuit of the desire to have carnal knowledge of the child, regardless of the gender of the perpetrator or the victim, or the consent of the victim;
- (g) **“Child Sexual Abuse and Exploitation Material or Child Sexual Abuse Material”** (CSAEM or CSAM) refers to any representation, whether offline, or by, through or with the use of ICT, by means of visual, video, audio, written, or any combination thereof, by electronic, mechanical, digital, optical, magnetic or any other means, of a child engaged or involved in real or simulated sexual activities, or depicting acts of sexual abuse or exploitation of a child as a sexual object. It shall also include materials that focus on the genitalia or other private body parts of a child.
- (h) **“Child Sexual Exploitation”** refers to any of the following acts even if consent appears to have been granted by the child:
- (1) Child sexual abuse with consideration whether monetary or nonmonetary consideration, favor, or benefit in exchange for the opportunity to perform such abusive or exploitative act;
 - (2) Actual sexual intercourse with a child or children with or without consideration;
 - (3) Employing fraud, machination, undue influence, intimidation, threat or deception by any person to commit sexual abuse of or sexual intercourse with a child or children; or
 - (4) Any other similar or analogous acts related to child abuse, cruelty or exploitation or to be responsible for other conditions prejudicial to the development of the child;
- (i) **“Covered Persons”** refer to any natural or juridical persons supervised or regulated by the Bangko Sentral ng Pilipinas, Securities and Exchange Commission, and Insurance Commission, and other persons and entities defined under Section 3(a) of the AMLA, as amended.
- (j) **“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;

Rules and Regulations Implementing Section 9(c) of Republic Act No. 11930, otherwise known as the Anti-Online Sexual Abuse or Exploitation of Children (OSAEC) and Anti-Child Sexual Abuse or Exploitation Materials (CSAEM) Act

- (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.

- (k) **“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.
- (l) **“Direct Knowledge”** refers to the knowledge acquired through directly perceiving something in the moment¹; directly acquired information.
- (m) **“Discovery”** refers to the date of establishment of suspicion or determination of the suspicious nature of the transaction.
- (n) **“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

¹ https://www.diamondapproach.org/glossary/refinery_phrases/direct-knowledge

Rules and Regulations Implementing Section 9(c) of Republic Act No. 11930, otherwise known as the Anti-Online Sexual Abuse or Exploitation of Children (OSAEC) and Anti-Child Sexual Abuse or Exploitation Materials (CSAEM) Act

- (o) **“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.
- (p) **“Financial Documents and Information”** refers to the following documents and information:
 - (1) *Transaction Records*. These pertain to customer’s records of transaction with the covered person.
 - (2) *Account Records*. These pertain to all other customer account information and documents, not technically considered as Information Data or Transaction Records.²
- (q) **“Information and Communications Technology”** (ICT) refers to the totality of electronic means to access, create, collect, store, process, receive, transmit, present, and disseminate information.
- (r) **“Inter-Agency Council Against Trafficking”** (IACAT) refers to the government body formed under Republic Act No. 9208, or the Anti-Trafficking in Persons Act of 2003, as amended, with additional mandate of addressing cases falling under the Anti-OSAEC-CSAEM Act.
- (s) **“Internet-based Payment System Provider”** (IPSP) 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.
- (t) **“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 Anti-OSAEC-CSAEM Act.
- (u) **“Money Laundering”** (ML) refers to the crime defined under Section 4 of the AMLA.
- (v) **“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.

² Chapter 2, Section 6.2, Items (a), (b), (c), 2022 Information Guideline on the Exchange, Sharing, Dissemination of Financial Intelligence and Other Information.

Rules and Regulations Implementing Section 9(c) of Republic Act No. 11930, otherwise known as the Anti-Online Sexual Abuse or Exploitation of Children (OSAEC) and Anti-Child Sexual Abuse or Exploitation Materials (CSAEM) Act

- (w) **“Money Service Business”** (MSB) refer to entities engages in remittance, money changing and/or foreign exchange dealing.
- (x) **“National Coordination Center Against OSAEC and CSAEM”** (NCC-OSAEC-CSAEM) refers to the center under the direction of the IACAT, mandated by law to develop and implement necessary programs that will prevent the commission of OSAEC and CSAEM, as well as to protect, heal, and reintegrate the child into the mainstream of society.
- (y) **“Online Sexual Abuse or Exploitation of Children”** (OSAEC) refers to the use of ICT as a means to abuse and/or exploit children sexually, which includes cases in which offline child abuse and/or exploitation is combined with an online component. This can also include, but is not limited to, the production, dissemination, and possession of CSAEM; 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. Provided, that OSAEC may be used interchangeably with the online child sexual exploitation or abuse (OCSEA);
- (z) **“OSAEC/CSAEM Activity”** refers to any of the acts as enumerated in Section 4 of the Anti-OSAEC-CSAEM Act.
- (aa) **“Payment System Provider”** (PSP) refers to an entity engaged in any monetary transaction which includes banks, fiat or digital money service businesses including cryptocurrencies, credit card companies and other financial institutions.

For purposes of this set of rules and regulations, this term shall be interchangeably used with the term “covered persons” under item (i) of this Section. 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.
- (bb) **“Person”** refers to any natural or juridical person.
- (cc) **“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;

Rules and Regulations Implementing Section 9(c) of Republic Act No. 11930, otherwise known as the Anti-Online Sexual Abuse or Exploitation of Children (OSAEC) and Anti-Child Sexual Abuse or Exploitation Materials (CSAEM) Act

- (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 OSAEC/CSAEM activity 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.
- (dd) **"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.
- (ee) **"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.
- (ff) **"Suspicious Transaction Report"** (STR) refers to a report on a suspicious transaction, as herein defined, filed by a covered person before the AMLC.
- (gg) **"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).
- (hh) **"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.
- (ii) **"Virtual Asset"** refers to a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes.
- (jj) **"Virtual Asset Provider"** 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:
- (1) Exchange between virtual assets and fiat currencies;
 - (2) Exchange between one or more forms of virtual assets;

Rules and Regulations Implementing Section 9(c) of Republic Act No. 11930, otherwise known as the Anti-Online Sexual Abuse or Exploitation of Children (OSAEC) and Anti-Child Sexual Abuse or Exploitation Materials (CSAEM) Act

- (3) 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;
 - (4) Safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and
 - (5) Participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.
- (kk) **"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 TRANSACTIONS AND ACTIVITIES**

**RULE 3
REPORTING TO THE DEPARTMENT OF JUSTICE-OFFICE OF CYBERCRIME**

Section 1. Reporting of OSAEC and CSAEM-related Financial Activity or Transaction to the DOJ-OOC.

1.1. Reporting to DOJ-OOC.

The following persons or entity shall have the duty to report any suspected OSAEC/CSAEM-related activity or transaction to the DOJ-OCC:

- (a) Payment System Provider; and
- (b) Any person who has direct knowledge of any OSAEC/CSAEM-related financial activity or transaction.

1.2. Period of Reporting.

All reports on suspected OSAEC/CSAEM-related activity or transaction shall be filed with the DOJ-OOC within twenty-four (24) hours from the date of transaction or knowledge thereof, whichever comes first.

Rules and Regulations Implementing Section 9(c) of Republic Act No. 11930, otherwise known as the Anti-Online Sexual Abuse or Exploitation of Children (OSAEC) and Anti-Child Sexual Abuse or Exploitation Materials (CSAEM) Act

1.3. *Creation of a Reporting Portal.*

To facilitate the reporting of any OSAEC/CSAEM-related financial activity or transaction the DOJ-OOC shall create a centralized reporting portal accessible to all PSPs. It shall also have a mechanism to accept reports from any person who has direct knowledge of any OSAEC/CSAEM-related financial activity or transaction.

Pending the creation of a reporting portal, reports shall be filed manually or electronically to the e-mail address to be determined by the DOJ-OOC and to be announced by the DILG 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 OSAEC/CSAEM-related financial activity or transaction in good faith, whether or not such reporting results in any criminal prosecution under the AMLA or the Anti-OSAEC-CSAEM Act.

RULE 4

REPORTING TO THE ANTI-MONEY LAUNDERING COUNCIL

Section 1. Suspicious Transaction Reporting Framework.

When reporting OSAEC/CSAEM-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.

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 discovery thereof, which for purposes of this Rule, shall be the date of establishment of suspicion or

Rules and Regulations Implementing Section 9(c) of Republic Act No. 11930, otherwise known as the Anti-Online Sexual Abuse or Exploitation of Children (OSAEC) and Anti-Child Sexual Abuse or Exploitation Materials (CSAEM) Act

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. OSAEC and CSAEM Monitoring System

4.1. Establishing and Maintaining OSAEC and CSAEM Monitoring System

All covered persons shall adopt an OSAEC/CSAEM 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 Anti-OSAEC-CSAEM Act.

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

4.2. Electronic Monitoring

- (a) Complex covered persons, as determined by their supervising authorities, shall adopt an electronic OSAEC/CSAEM 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;

Rules and Regulations Implementing Section 9(c) of Republic Act No. 11930, otherwise known as the Anti-Online Sexual Abuse or Exploitation of Children (OSAEC) and Anti-Child Sexual Abuse or Exploitation Materials (CSAEM) Act

- (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 OSAEC/CSAEM-related transactions. They shall 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 confidential. Covered persons, their officers, and employees are prohibited from communicating, directly or indirectly, in any manner or by any means, to any person, entity, or the media, the fact that a suspicious transaction has been or is about to be reported, including 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 Anti-OSAEC-CSAEM Act.

Rules and Regulations Implementing Section 9(c) of Republic Act No. 11930, otherwise known as the Anti-Online Sexual Abuse or Exploitation of Children (OSAEC) and Anti-Child Sexual Abuse or Exploitation Materials (CSAEM) Act

Section 7. AMLC Reporting Guidelines.

Covered persons shall ensure compliance with registration and reporting guidelines issued by the AMLC in performing their obligations under Rule 3 hereof.

RULE 5 SUSPICIOUS TRANSACTIONS AND ACTIVITIES

Section 1. Suspicious Transactions.

Any transactions, 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 subject to reporting obligations 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 OSAEC/CSAEM 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 red flag indicators and institutional knowledge about AMLA regulations and

Rules and Regulations Implementing Section 9(c) of Republic Act No. 11930, otherwise known as the Anti-Online Sexual Abuse or Exploitation of Children (OSAEC) and Anti-Child Sexual Abuse or Exploitation Materials (CSAEM) Act

issuances, covered persons shall identify reportable financial transactions and activities related to OSAEC and CSAEM and report it to the AMLC.

2.1 *Red Flag Indicators for Senders of Funds*

The covered person shall recognize, among others, the following financial transaction indicators for senders of funds:

- (a) Senders are usually advanced in age and are male foreigners from countries considered as high-risk jurisdictions for child pornography.
- (b) Individuals who send multiple remittances to different Filipino recipients located in hotspots for child pornography in the Philippines, mostly rural and depressed areas.
- (c) Senders who remit relatively low-value international or domestic remittances to a large number of beneficiaries with unjustified purpose and relationship, mostly non-familial senders.
- (d) Foreign nationals who are currently residing in the Philippines and have been sending domestic remittances to individuals residing in the same or near the sender's place of residency.
- (e) Senders have transactions with identified suspects for human trafficking who are subjects of investigation for child exploitation.

2.2 *Red Flag Indicators for Beneficiaries of Funds*

The covered person shall recognize, among others, the following financial transaction indicators for beneficiaries of funds:

- (a) Beneficiaries are usually unemployed (e.g. housewife) or belonging to the low-income class of the society (e.g. self-employed, with sari-sari store business, service crew, online seller, sales agent, pub dancer, massage therapist, janitor, municipal staff, nanny/helper) and rely on remittances as source of income.
- (b) Beneficiaries have no declared sources of funds.
- (c) Beneficiaries are residing in hotspots for child pornography in the Philippines, mostly rural and depress areas.
- (d) Beneficiaries who received multiple international remittances from various

Rules and Regulations Implementing Section 9(c) of Republic Act No. 11930, otherwise known as the Anti-Online Sexual Abuse or Exploitation of Children (OSAEC) and Anti-Child Sexual Abuse or Exploitation Materials (CSAEM) Act

individuals abroad/foreign nationals or multiple domestic remittances from large number of remitters, with unjustified purpose and relationship, mostly non-familial senders.

- (e) Beneficiaries receiving multiple international remittances from foreign nationals who appear to have sent multiple transactions to different Filipino individuals.
- (f) Beneficiaries are usually young adults to adults and are mostly females.
- (g) Some beneficiaries were identified as minors or students.
- (h) Some beneficiaries were identified as openly gay.
- (i) Beneficiaries are related to each other as family members or relatives or who received remittances from same senders.
- (j) Beneficiaries are transacting with individuals who are known to be sex offenders from another country.
- (k) Beneficiaries are under investigation by law enforcement agencies for being suspected facilitators of online sexual exploitation of children.
- (l) Beneficiaries of funds who have been identified as receiving payments for selling pornographic videos through social media.

Section 3. Other Red Flags.

Covered persons may also consider the following OSAEC and CSAEM – related behaviors observable during account activity:

- (a) The amounts of the remittances are relatively low and below the reporting threshold.
- (b) Remittances were made usually through international and domestic Money Service Businesses (MSBs).
- (c) Beneficiaries claimed remittances from different branches of an MSB within the same province or city.
- (d) Beneficiaries claimed remittances at least four times a month or at least twice a week from same MSB.

Rules and Regulations Implementing Section 9(c) of Republic Act No. 11930, otherwise known as the Anti-Online Sexual Abuse or Exploitation of Children (OSAEC) and Anti-Child Sexual Abuse or Exploitation Materials (CSAEM) Act

- (e) Declared purposes of the remittances are usually for gift, food/food consumption, family needs/daily needs, budget, salary, payment, allowances, fare, business, miscellaneous fee, hospital bills, support/family support, allotment, store stocks/purchase of grocery, expenses/personal expenses/household expenses, payments for bills/internet bills/electric bills, cake, medicine, finances, maintenance, help, school payment, boarding house, transportation and travel.
- (f) Offenders provide financial support to multiple receivers by sending money for purposes as cited above.
- (g) Declared relationships of the senders and beneficiaries are friends, boyfriend, fiancé, husband, girlfriend, brother, brother-in-law, boss, employer, uncle, cousin, sponsor and stepfather.
- (h) Relationships of the beneficiaries and senders are not properly identified.
- (i) Remittances with undisclosed or unknown purpose and relationship.
- (j) The age gap between the sender and the beneficiary is more or less 35 years.
- (k) Beneficiaries disclosed meeting the sender of funds through online or dating app.
- (l) Swift or abrupt increase in the volume and amount of transactions overtime of the offenders as well as the facilitators.
- (m) The beneficiary of remittance, located in the Philippines, receives multiple transactions under \$100.00 within a 30-day period or less.
- (n) Multiple and irregular payments or transactions in a month including same day payments.
- (o) Receives multiple remittances a day or a week from same sender.
- (p) Transactions of beneficiaries deviated during COVID-19 period.
- (q) Payments made through specific account, such as in Electronic Money Issuers (EMI), as advised by social media accounts advertising pornographic photos and videos of children advising that payments should be made to the said specific account.

Rules and Regulations Implementing Section 9(c) of Republic Act No. 11930, otherwise known as the Anti-Online Sexual Abuse or Exploitation of Children (OSAEC) and Anti-Child Sexual Abuse or Exploitation Materials (CSAEM) Act

**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 court, through the Office of the Solicitor General, an *Ex Parte* Application for the Issuance of Bank Inquiry Order to examine or inquire into any particular bank deposit or investment account when it has been established that there is reasonable ground to believe that the deposit or investments are in any way related to OSAEC/CSAEM or other violations of the Anti- OSAEC and Anti-CSAEM 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 OSAEC/CSAEM-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, entitled "An Act Prohibiting Disclosure of or Inquiry into Deposits with any Banking Institution and Providing Penalty Therefor," as amended, Republic Act No.6426, otherwise known as the "Foreign Currency Deposit Act of the Philippines," as amended, Republic Act No. 8791, otherwise known as "The General Banking Law of 2000," as amended, and other pertinent laws, the LEAs investigating cases under the Anti-OSAEC-CSAEM Act 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 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 OSAEC/CSAEM or other violations of the Anti-OSAEC-CSAEM Act.

Rules and Regulations Implementing Section 9(c) of Republic Act No. 11930, otherwise known as the Anti-Online Sexual Abuse or Exploitation of Children (OSAEC) and Anti-Child Sexual Abuse or Exploitation Materials (CSAEM) Act

Section 5. Rule of Procedure for Bank Inquiry under the Anti-OSAEC CSAEM 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 Anti-OSAEC-CSAEM 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 court, an Application for the Issuance of an Order Allowing Access to Financial Documents and Information not covered by *bank deposit and investment secrecy laws* that are related to OSAEC/CSAEM or other violations of the Anti-OSAEC-CSAEM Act.

Rules and Regulations Implementing Section 9(c) of Republic Act No. 11930, otherwise known as the Anti-Online Sexual Abuse or Exploitation of Children (OSAEC) and Anti-Child Sexual Abuse or Exploitation Materials (CSAEM) Act

Section 2. Inquiry Into or Examination of Related Accounts.

A court order must be obtained before any LEA can inquire into the related accounts. The procedure for the 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 OSAEC/CSAEM-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 and investment secrecy laws*.

Section 4. Order Allowing Access to Financial Information.

The LEAs investigating cases of OSAEC/CSAEM may require financial intermediaries, IPSPs, and other financial facilitators to provide financial documents and information not covered by *bank deposit and investment secrecy laws*, upon order of the competent court, based on an application, when it has been established that there is reasonable ground to believe that the transactions, including related accounts involved, are related to OSAEC/CSAEM activity or other violations of the Anti-OSAEC-CSAEM Act.

Section 5. Rule of Procedure for Accessing Financial Information under the Anti-OSAEC-CSAEM Act.

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

**CHAPTER IV
MISCELLANEOUS PROVISIONS**

**RULE 8
AMENDMENTS TO THE ANTI-MONEY LAUNDERING ACT**

Section 1. Associated Unlawful Activity to Money Laundering. Violations under Sections 4 and 5 of the Anti-OSAEC-CSAEM Act shall be considered as "unlawful activity" under Section 3(i) of Republic Act No. 9160, otherwise known as the "Anti-Money Laundering Act of 2001",

Rules and Regulations Implementing Section 9(c) of Republic Act No. 11930, otherwise known as the Anti-Online Sexual Abuse or Exploitation of Children (OSAEC) and Anti-Child Sexual Abuse or Exploitation Materials (CSAEM) Act

as amended:

Section 4. Unlawful or Prohibited Acts. — *Regardless of the consent of the child, it shall be unlawful for any person to commit the following acts through online or offline means or a combination of both:*

- (a) To hire, employ, use, persuade, induce, extort, engage, or coerce a child to perform or participate in whatever way in the creation or production of any form of OSAEC and CSAEM;*
- (b) To produce, direct, manufacture, facilitate, or create any form of CSAEM, or participate in the production, direction, manufacture, facilitation or creation of the same;*
- (c) To offer, sell, distribute, advertise, promote, export, or import, by any means, any form of CSAEM;*
- (d) To knowingly publish, transmit and broadcast, by any means, any form of CSAEM;*
- (e) To permit or influence the child to engage, participate or assist in any form of CSAEM;*
- (f) To produce, direct, create, hire, employ or pay a facilitator to stream or livestream acts of child sexual abuse or exploitation*
- (g) To stream or live-stream acts of, or any form of, child sexual abuse and exploitation;*
- (h) To recruit, transport, transfer, harbor, provide, or receive a child or to induce or influence the same, for the purpose of violating this Act;*
- (i) To introduce or match a child to a foreign national or to any person for the purpose of committing any of the offenses under this Act;*
- (j) For film distributors, theaters and ICT services by themselves or in cooperation with other entities, to distribute any form of CSAEM or to facilitate the commission of any of the offenses under this Act;*
- (k) To knowingly benefit from, financial or otherwise, the commission of any of the offenses of this Act;*
- (l) To provide a venue for the commission of prohibited acts under this section such as dens, private rooms, cubicles, cinemas, houses, private homes, or other establishments;*
- (m) To engage in the luring or grooming of a child: Provided, That grooming taking place offline as a prelude to violations under this Act shall also be penalized;*
- (n) To sexualize children by presenting them as objects of sexual fantasy, or making them conversational subjects of sexual fantasies, in any online or digital platform;*
- (o) To engage in pandering as defined under this Act;*

Rules and Regulations Implementing Section 9(c) of Republic Act No. 11930, otherwise known as the Anti-Online Sexual Abuse or Exploitation of Children (OSAEC) and Anti-Child Sexual Abuse or Exploitation Materials (CSAEM) Act

- (p) *To willfully subscribe, join, donate to, or support an internet site that hosts OSAEC or the streaming or live-streaming of child sexual abuse and exploitation;*
- (q) *To advertise, publish, print, broadcast or distribute, or cause the advertisement, publication, printing, broadcasting or distribution by any means of any brochure, flyer, or any material that promotes OSAEC and child sexual abuse or exploitation*
- (r) *To possess any form of CSAEM: Provided, That possession of three (3) or more CSAEMs is prima facie evidence of the intent to sell, distribute, publish or broadcast;*
- (s) *To willfully access any form of CSAEM; and*
- (t) *To conspire to commit any of the prohibited acts stated in this section: Provided, That the investigation or prosecution of offenses under this Act shall be without prejudice to appropriate investigation and prosecution mechanisms under Republic Act No. 9208, otherwise known as the "Anti-Trafficking in Persons Act of 2003," as amended, and other related laws.*

Section 5. *Effect of Consent of the Victim. — The consent of the victim is not material or relevant and shall not be available as a defense in the prosecution of the unlawful acts prohibited under this Act.*

Section 2. Use of Government Identification Documents in Transactions with Money Transfer and Remittance Centers. Money transfer and remittance centers shall require individuals transacting with them to present valid government identification cards.

RULE 9

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 AMLC, the appropriate government agencies and the courts, as the case may be.

Section 2. Administrative Sanctions by the AMLC.

Violations or non-compliance with the suspicious transaction 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*.

RULE 10
TRANSITORY, SEPARABILITY AND EFFECTIVITY CLAUSES

Section 1. Transitory Provision

- 1.1 *For the reporting requirements to the DOJ-OOC under Rule 3 hereof:* The DOJ-OOC 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 violations of Section 4 of Republic Act No. 9775, otherwise known as the “Anti-Child Pornography Act of 2009”, prescribed under the *2021 AMLC Registration and Reporting Guidelines*, until the unlawful activities under the Anti-OSAEC-CSAEM 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 DOJ-OOC, in coordination with the NCC-OSAEC-CSAEM and the AMLC, shall adopt a central database for the receiving and maintenance of reports to the DOJ-OOC.
- 1.4 All covered persons shall adopt or update their OSAEC/CSAEM-monitoring system within one (1) year from the effectivity of this set of rules and regulations.

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.

Rules and Regulations Implementing Section 9(c) of Republic Act No. 11930, otherwise known as the Anti-Online Sexual Abuse or Exploitation of Children (OSAEC) and Anti-Child Sexual Abuse or Exploitation Materials (CSAEM) Act

JUANITO VICTOR C. REMULLA JR.
Secretary
Department of the Interior and
Local Government

MATTHEW M. DAVID
Executive Director
Anti-Money Laundering Council

_____ 20__

DRAFT ZERO