REVISED NAT RE MONEY LAUNDERING AND TERRORISM FINANCING PREVENTION PROGRAM (MTPP)

Approved by the Board on its meeting on March 26, 2026

The Board approved this revised Nat Re MTPP during its meeting on March 26,2026

Section 1. General Policies to Combat Money Laundering and Financing of Terrorism

National Reinsurance Corporation of the Philippines (Nat Re) is committed in observing its ethical responsibility to the public and to its people. It shall comply with the requirements of the Insurance Commission (IC) for its regulated entities (ICREs) embodied in IC Circular Letter (CL) No. 2018-48, as amended by CL 2018-60, further amended by CL 2019-65, and Anti-Money Laundering Council (AMLC) Regulatory Issuances, particularly the 2018 Revised IRR of RA 9160 and the Regulatory Issuance No. 2, Series of 2024 "Guidelines on Transaction Reporting and Compliance Submissions (GoTRACS)", as well as other applicable issuances of the IC, in revising Nat Re's guidelines and procedures against money-laundering and combating the financing of terrorism.

Nat Re supports the efforts and policies of the AMLC and the IC in combating money laundering and preventing financing of terrorism. Considering that money laundering and financing of terrorism are serious crimes that threaten the competitiveness and openness of the Philippine economy, Nat Re shall observe the following principles throughout its business:

a. Conform with high ethical standards and observe good corporate governance consistent with the subject guidelines to protect the integrity of Nat Re;

b. Know sufficiently our customers to prevent criminal elements and suspicious entities from transacting with, or establishing or maintaining relationship with Nat Re;

c. Adopt and effectively implement an appropriate *anti-money laundering and counter-terrorism financing* (AML/CTF) risk management system that identifies, understands, assesses, monitors, and controls risks associated with *money laundering and terrorism financing* (ML/TF);

d. Comply fully with existing laws and regulations aimed at combating money laundering and terrorism financing by making sure that Nat Re officers and employees are aware of their respective responsibilities and carry them out in accordance with a superior and principled culture of compliance; and

e. Cooperate fully with the IC, AMLC and other competent authorities for the effective implementation of the Anti-Money Laundering and Counter-Terrorism Financing Laws, their respective implementing rules and regulations, and other directives, guidance and issuances from the IC and AMLC.

SECTION 2. Definition of Terms

For purposes of this Guidelines, the following terms are defined as follows:

a) "**Anti-Money Laundering Act**" (AMLA) refers to Republic Act No. 9160, as amended by Republic Act Nos. 9194, 10167,10365, 10927 and 11521.[1]

b) "Anti-Money Laundering Council" (AMLC) refers to the Philippines' central Anti Money Laundering/Counter Terrorism Financing (AML/CTF) authority and financial intelligence unit, which is the government instrumentality mandated to implement the AMLA and R.A. 10168 or the Terrorism Financing Prevention and Suppression Act of 2012 (TFPSA). It also refers to the official name of the Council, which is the governing body of the said government agency.[1]

c) "**Beneficial Owner**" refers to any natural person who:

1. Ultimately owns or controls the customer and/or on whose behalf a transaction or activity is being conducted; or
2. Has ultimate effective control over a legal person or legal arrangement; or
3. Owns, at least, twenty percent (20%) shares, contributions or equity interest in a juridical person or legal arrangement.
4. Control includes whether the control is exerted by means of trusts, agreements, arrangements, understandings, or practices and whether or not the individual can exercise control through making decisions about financial and operating policies. [1]

d) "**Covered Transaction**" refers to a transaction in cash or other equivalent monetary instrument exceeding Five Hundred Thousand Pesos (Php500,000.00)

e) **"Covered Transaction Report" (CTR) refers to a report on a covered transaction, as herein defined, filed by a covered person before the AMLC.** [1]
Please see Annex A on Reporting Covered Transaction Reports,

f) "**Customer/Client**" refers to any person who keeps an account, or otherwise transacts business with Nat Re.[1]

g) "**Financing of Terrorism**" is a crime committed by a person who, directly or indirectly, willfully and without lawful excuse, possesses, provides and collects or uses property or funds or makes available property, funds or financial service or other related services, by any means, with the unlawful and willful intention that they should be used or with the knowledge that they are to be used, in full or in part: (i) carry out or facilitate the commission of any terrorist act; (ii) by a terrorist organization, association or group; or (iii) by an individual terrorist.[2]

h) "**Related Accounts**" 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[1]

[1] AMLC Regulatory Issuance No. 2, Series of 2024

[2] Section 4, R.A. 10168 The Terrorism Financing Prevention and Suppression Act of 2012

i) "**Money Laundering**" – Money laundering is a crime whereby the proceeds of an unlawful activity are transacted, thereby making them appear to have originated from legitimate sources. It is committed by the following:

a. Any person knowing that any monetary instrument or property represents, involves, or relates to, the proceeds of any unlawful activity, transacts or attempts to transact said monetary instrument or property;
b. Any person knowing that any monetary instrument or property involves the proceeds of any unlawful activity, performs or fails to perform any act as a result of which he facilitates the offense of money laundering referred to in paragraph (a) above.;
c. Any person knowing that any monetary instrument or property is required under this Act to be disclosed and filed with the Anti-Money Laundering Council (AMLC), fails to do so.[2]

j) "Juridical Person" refers to any entities other than natural persons created by law and recognized as a legal entity having distinct identity, legal personality and duties and rights that can establish a permanent customer relationship with a financial institution. This can include companies, bodies corporate, foundations, partnerships, or associations and other relevantly similar entities.[3]

k) **"Politically Exposed Person**" (PEP) refers to an individual who is or has been entrusted with prominent public position in (1) the Philippines with substantial authority over policy, operations or the use or allocation of government-owned resources; (2) a foreign State; or (3) an international organization.[4]

a. "**Immediate Family Member of PEPs**" refers to individuals related to the PEP within the second degree of consanguinity or affinity.

b. "**Close Relationship/Associates of PEPs**" refer to persons who are widely and publicly known, socially or professionally, to maintain a particularly close relationship with the PEP and include persons who are in a position to conduct substantial domestic and international financial transactions on behalf of the PEP.

l) "**Suspicious Transaction**" refers to a transaction, regardless of amount, where any of the suspicious circumstances, as defined in the 2024 Guidelines on Transaction Reporting and Compliance Submissions, is determined, based on suspicion or, if available, reasonable grounds, to be existing.[5]
Please see Annex B on Reporting of Suspicious Transactions

m) "Suspicious Circumstances" refers to:

1. any of the following circumstances, the existence of which makes a transaction suspicious:
   a. there is no underlying legal or trade obligation, purpose or economic justification;

[2] Section 4, R.A. 9160 Anti-Money Laundering Act of 2001
[3] AMLC regulatory Issuance No.2 series of 2024 re: Guidelines on Transaction Reporting and Compliance Submissions (GoTRACS)
[4] Rule 3- Definition of Terms, Section 1, 2018 IRR of RA 9160
[5] AMLC Regulatory Issuance No. 2, series of 2024 -Guidelines on Transaction Reporting and Compliance Submissions

b. the client is not properly identified; the amount involved is not commensurate with the business or financial capacity of the client;

c 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;

d. 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;
e. the transaction is in any way related to ML/TF or related unlawful activity that is about to be committed, is being or has been committed; or
f. any transaction that is similar, analogous, or identical to any of the foregoing, such as the relevant transactions in related and materially linked accounts, as herein defined.

2. The presence of the following circumstances under the Rule 3.a.15 of the Implementing Rules and Regulations of R.A. 10168 or the Terrorism Financing Prevention and Suppression Act of 2012 (TFPSA) shall also make transactions suspicious:
    a. Wire transfers between accounts, without visible legal, economic, or business purpose, especially if the wire transfers are effected through countries which are identified or connected with terrorist activities;
    b. Sources and/or beneficiaries of wire transfers are citizens of countries which are identified or connected with terrorist activities;
    c. Repetitive deposits or withdrawals that cannot be satisfactorily explained or do not make economic or business sense;
    d. Value of the transaction is grossly over and above what the client is capable of earning;
    e. Client is conducting a transaction that is out of the ordinary for his known business interests;
    f. Deposits by individuals who have no known connection or relation with the account holder;
    g. Client is receiving remittances from a country where none of his family members is working or residing;
    h. Client was reported and/or mentioned in the news to be involved in terrorist activities;
    i. Client is under investigation by law enforcement agencies for possible involvement in terrorist activities;
    j. Transactions of individuals, companies, or Non-Government Organizations (NGOs)/Non-Profit Organizations (NPOs) that are affiliated or related to people suspected of having connection with a terrorist individual, organization, association, or group of persons;
    k. Transactions of individuals, companies or NGOs/NPOs that are suspected of being used to payor receive funds from a terrorist individual, organization, association, or group of persons;

l. The NGO/NPO does not appear to have expenses normally related to relief or humanitarian efforts;
m. The absence of contributions from donors located within the country of origin of the NGO/NPO;
n. The volume and frequency of transactions of the NGO/NPO are not commensurate with its stated purpose and activity; and
o. Any other transaction that is similar, identical, or analogous to any of the foregoing.[6]

n) "Transaction" refers to any act establishing any right or obligation or giving rise to any contractual or legal relationship between the parties thereto. It also includes any movement of funds by any means with a covered person. [7]

o) "Ultimate Effective Control" - refers to a situation in which ownership/control is exercised through actual or a chain of ownership or by means other than direct control.[8]

p) "Unlawful Activity" refers to the associated unlawful activities, also known as predicate crimes, to money laundering defined under Section 3(i) of the AMLA.[8]

Section 3. Role of the Board of Directors, Senior Management and Compliance Officer

Nat Re's Board of Directors is ultimately responsible for ensuring compliance with the AML/CTF Guidelines, the AML and CTF Laws, the respective implementing rules and regulations, and other directives, guidance and issuances from the IC and AMLC.

Senior management shall oversee the day-to-day management of Nat Re, ensure effective implementation of the AML/CTF policies approved by the board and alignment of activities with the strategic objectives, risk profile and corporate values set by the Board. Senior management shall establish a management structure that promotes accountability and transparency and upholds checks and balances.

A. The Compliance Office shall be mainly responsible for implementing Nat Re's ML/TF prevention program and guidelines. To ensure the independence of the office, it shall have a direct reporting line to the Board's Governance & Related Party Transaction Committee (GRPT) on all matters relating to AML and CTF compliance and risk management. It shall also be responsible for the following:

    1. Ensure compliance by all responsible officers and employees with the AML/CTF Guidelines, the AML and CTF Laws, the respective rules and regulations, other directives, guidance and issuances from the IC and AMLC and this ML/TFPP.

    2. Conduct periodic compliance checking which covers, among others, evaluation of existing processes, policies and procedures including on-going monitoring of performance by staff and officers involved in ML and TF prevention, reporting channels,

[6] AMLC Regulatory Issuance No. 2, series of 2024 -Guidelines on Transaction Reporting and Compliance Submissions
[7] AMLC Regulatory Issuance No. 2, series of 2024 -Guidelines on Transaction Reporting and Compliance Submissions

effectiveness of AML and CTF transaction monitoring system and record retention system through sample testing and review of audit or checking report. Report compliance findings to the board;

3. Ensure that infractions, discovered either by internally initiated audits, or by special or regular compliance checking conducted by the IC and/or AMLC are immediately corrected;

4. Inform all responsible officers and employees of all resolutions, circulars and other issuances by the IC and/or the AMLC in relation to matters aimed at preventing ML and TF;

5. Alert senior management and the board of directors if it believes that Nat Re is failing to appropriately address AML/CTF issues; and

6. Organize the timing and content of AML/CTF training of officers and employees including regular refreshers training.

B. Designation of a Compliance Officer

The designated Compliance Officer shall be of management level with authority and mandate to ensure day-to-day compliance with its AML/CTF obligations. Another official may also be designated to be responsible and accountable for all record keeping requirements such as making records of customer identification and transaction documents readily available during compliance checking and investigation.[8]

C. Implementation of a comprehensive MTPP

Nat Re's Board of Directors shall approve and the Compliance Officer shall implement a comprehensive and risk-based Money Laundering and Terrorism Financing Prevention Program (MTPP) geared towards the promotion of high ethical and professional standards and the prevention of ML and TF. This ML/TFPP shall be updated once every two years or whenever necessary to reflect relevant changes. [9]

D. Reporting to the Insurance Commission

The Compliance Officer shall submit to the IC not later than fifteen (15) days from the approval of the Board the new/updated MTPP a sworn certification that a new/updated MTPP has been prepared, duly noted and approved by the Board. [10]

[8] Section 2, 2018 revised IRR of RA 9160

[9] Section 3, IC CL 2019-65

Section 4. Risk Management Policy and Procedures

Nat Re shall develop sound risk management policies and procedures to ensure that risks associated with money laundering and terrorism financing such as counterparty, reputational, operational and compliance risks are identified, assessed, monitored, mitigated and controlled, as well as ensure effective implementation of this Guidelines.

The four (4) areas of effective risk management are (a) *adequate and active board and senior management oversight, (b) acceptable policies and procedures embodied in the MTPP, (c) appropriate monitoring and Management Information System and (d) comprehensive internal control and audits.*

Section 5. Guidelines on Anti- Money Laundering and Counter Terrorism Financing (AML/CTF)

To combat money laundering and terrorism financing, Nat Re shall adopt the following guidelines, procedures and controls:

A. Customer Due Diligence

Before a business relationship is established, Nat Re shall take steps to establish and record the identity of the customer based on official documents. Nat Re shall maintain a system of verifying the customer's legal existence and organizational structure, as well as the authority and identification of all persons purporting to act on their behalf. Nat Re shall establish appropriate system and methods, and adequate internal controls, compliant with the AMLA, 2018 Revised Implementing Rules and Regulations, other AMLC issuances, guidelines issued by the IC and internationally accepted anti-money laundering standards, for verifying and recording the true and full identity of the clients.

In conducting customer due diligence, a risk-based approach shall be undertaken depending on the type of customer, business relationship and nature of the transaction.[10]

1. Customer Identification –

a. For minimum customer information and identification of documents, the designated Reinsurance Operations team shall gather Identification information as follows:

   a. Full Name of entity;
   b. Name of authorized representative/transactor/signer;
   c. Current Office address;
   d. Contact number or information;
   e. Nature of business;
   f. Source of fund
   g. Specimen signature or biometrics of the of authorized representative/transactor/signer; and
   h. Name, address, date and place of birth, contact number or information, sex, and citizenship or nationality of beneficiary and/or beneficial owner, if applicable.
   i. Beneficial Ownership
   j. Politically Exposed Persons

[10] Rule 18, 2018 revised IRR of RA 9160

and obtain all the following identification documents:

a. Certificates of Incorporation issued by the Securities and Exchange Commission (SEC);
b. Articles of Incorporation;
c. Registration Data Sheet/Latest General Information Sheet (GIS);
d. Secretary's Certificate citing the pertinent portion of the Board or Partners' Resolution authorizing the signatory to sign on behalf of the entity;
e. For entities registered outside of the Philippines, similar documents and/or information duly authenticated by a senior officer of the covered person assigned in the country of registration; in the absence of said officer, the documents should be authenticated by the Philippine Consulate, company register or notary public, where said entities are registered.

The company shall understand the nature of the customer's business, its ownership and control structure.[11]

b. Verification of beneficial ownership –

Nat Re shall identify and take reasonable measures to verify the identity of beneficial owners through the following information:

a. the identity of the natural persons, if any, who ultimately have controlling ownership interest in the corporation;

b. to the extent that there is doubt under (a) above, as to whether the persons with controlling ownership interest are the beneficial owners or where no natural person exerts control through ownership interests, the identity of the natural persons, if any, exercising control over the corporation through other means; and

c. where no natural person is identified under items (a) and (b) above, the identity of the relevant natural persons who hold senior management positions.

c. Undertake additional verification measures if there is reason to doubt the accuracy of the data given or the veracity of the identification documents presented. Check further on any significant change in the client company's structure or ownership. Details of additional checking made should be recorded.[12]

2. Sanction Screening

Under the AMLC 2021 Sanction Guidelines, Financial Sanctions and restrictions put in place by the United Nations and its Security Council, a supra-national jurisdiction (e.g. European Union), another jurisdiction or by the Philippine government to:
• limit the provision of certain financial services; and
• restrict access to financial markets, funds and economic resources

At a minimum customers should be screened against the following sanctions list:

[11] Section 6, IC CL 2019-65)

[12] Section 7, IC CL 2019-65

(1) UN Consolidated Sanction List
(2) US Office of Asset Foreign Control (OFAC)
(3) European Union Sanction List
(4) AMLC Sanction List

3. Risk Assessment

Nat Re shall:

i. Identify, assess and understand the AML/CTF risks in relation to its customers, its business, products and services, geographical exposures, transactions, delivery channels, and size, among others; and appropriately define and document its risk-based approach. The risk assessment shall include both quantitative and qualitative factors.

ii. Institute the following processes in assessing the ML/TF risks:
   a. Document risk assessments and findings;
   b. Consider all the relevant risk factors, including the results of national and sectoral risk assessment, before determining what is the level of overall risk and the appropriate level and type of mitigation to be applied;
   c. Keep the assessment up-to-date through periodic review; and
   d. Ensure submission of the risk assessment information as may be required by the IC.

iii. Conduct Institutional Risk Assessment
Under IC-CL 2024-16, the Insurance Commission issues guidelines in the conduct of Institutional Risk Assessment to ensure that the AML/CFT institutional risk assessment by all IC Regulated Entities is conducted comprehensively and uniformly. [13]

Nat Re transactions are considered as "low risk' transactions due to the following:
i. Transactions are mostly with the local/domestic insurance companies /professional reinsurers/intermediaries duly licensed by the Insurance Commission and are also vetted through their respective MTPPs.
ii. Foreign incoming/outgoing treaty arrangements are reported to the Insurance Commission, as required, for good order.[14]

4. On-going Monitoring of Customers, Accounts and Transactions

Nat Re shall on the basis of materiality and risk, ensure that pertinent identification information and documents collected under the CDD process are kept up-to-date and relevant.

It shall secure the consent of its customers to be bound by obligations set out in the relevant United Nations Security Council Resolutions relating to the prevention and suppression of proliferation of financing of weapons of mass destruction, including the freezing and unfreezing actions as well as prohibitions from conducting transactions with designated persons and entities.[15]

[13] Section 2, IC CL 2019-65
[14] Section 7.5, AMLC Regulatory Issuance No. 2, series of 2024
[15] Section 15, IC CL 2019-65

5. Monitoring and Reporting System

Nat Re maintains a system that allows it to report regularly and consistently the prescribed CTR and/or STR as applicable on a timely basis. While no fully electronic monitoring system is in place for flagging and monitoring subject transactions, a manual process is in place to monitor exceptions and report any Suspicious Transactions (STs) accordingly. This monitoring system is 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 AML/CTF compliance. Depending on the development of our risk–profile and growing business complexity, there is a continuous assessment of the need to have a reasonable electronic monitoring system to be in place.

B. Record Keeping and Retention

The departments concerned must ensure that robust record-keeping is maintained and that, as a minimum, documents listed shall be maintained and safely stored for five (5) years from the date of transactions for all records of customer identification and transaction documents:

- Documentation regarding identifying and knowing your customers (*Life and Non-Life Reinsurance Operations*);
- Reports submitted to the authorities concerning the suspicious activities of a customer in connection with potential money laundering and/or terrorism financing, along with any supporting documentation (*Finance*);
- Registers of training on money laundering and terrorism financing (*Compliance*); and any other documents or registers that must be kept per applicable legislation of anti-money laundering or counter-terrorism financing. [16]

If a case has been filed in court involving the account, records must be retained and safely kept beyond the five (5)-year period, until it is officially confirmed by the AMLC Secretariat that the case has been resolved, decided or terminated with finality. [17]

C. Reporting of Covered and Suspicious Transactions

Nat Re's Finance department shall be responsible in regularly reporting to the AMLC the Covered Transaction Report (CTR) within five (5) working days, unless the AMLC prescribes a different period not exceeding fifteen (15) working days, from the occurrence thereof.

For suspicious transactions, it shall be filed within the next working day from the occurrence thereof, which shall be the date of establishment of suspicion or determination of the suspicious nature of the transaction.

[16] Section 48, IC CL2018-48

[17] Refer to Nat Re's Document Retention and Storage Policy

Should a transaction be determined to be both a covered and suspicious transaction, it shall be reported as a suspicious transaction. In this regard, it shall be reported first as a CTR, subject to updating if it is finally confirmed to be reportable as STR.

Nat Re's directors, officers and employees are prohibited from communicating, directly or indirectly, in any manner or by any means, to any person or entity, or the media, the fact that a covered or suspicious transaction has been or about to be reported, or any other information in relation thereto.

The due diligence process shall flag any suspicious transaction and this shall be reported to the Finance team for proper reporting to AMLC.

Procedures and formats in mandatory reporting of CTRs and STRS should follow AMLC Regulatory Issuance No. 2, series of 2024, Please see Annexes A & B

Relative to AMLC Section 7.5 of Regulatory Issuance No. 2, series of 2024 where Deferred reporting shall be applicable to low-risk covered transactions only. The responsibility of Covered Persons to report suspicious transactions, where applicable, remains, should there be further adjustments or modifications in the application thereof; the foregoing policy shall be prospective.

For IC-Supervised Financial Institutions, the following are considered low-risk transactions

a. *Transactions between domestic insurance companies / professional reinsurers/intermediaries licensed by the Insurance Commission;*
b. *Renewal of non-life insurance policies under the same terms and conditions provided that a CTR has been previously filed;*
c. *Collection of premium payments from telemarketing, or direct marketing or through SMS and/or by way of salary deductions, where the bulk settlement exceeds Php500,000.00 but the individual transactions are below the reporting threshold amount;*
d. *Group Life Insurance and Hospitalization Insurance;*
e. *Transactions of members of Mutual Benefit Associations pertaining to basic benefits;*
f. *Bulk settlement of claims on death and disability benefits of a policy where individual claim does not exceed Php500,000.00;*
g. *Transactions coursed through brokers, agents and other intermediaries, in which case, however, the insurance company (principal) shall report the said transactions;*
h. *IC-initiated or system generated transactions, which are proprietary in nature; provided, that it shall be limited to the following transactions:*
    1. *Internal operating expenses and capital expenditures that are booked as such in the books of the covered persons; and*
    2. *Adjusting entries or reclassification of accounts.* [18].

[18] AMLC Regulatory Issuance No. 2, series of 2024

D. Training and Awareness

Nat Re through its Compliance Office shall provide training to all responsible directors, officers and employees to enable them to fully comply with their obligations and responsibilities. This must be facilitated through:

1. Developing or creating opportunities for, continuing education and training programs for responsible directors, officers and employees to promote AML/CTF awareness and strong compliance culture.

2. Training programs shall include relevant topics, such as: *a) Overview on ML/TF, and the AMLA and TFPSA; b) Roles of directors, officers and employees in ML/TF prevention; c) Risk Management; d) Preventive measures; e) Compliance with freeze, bank inquiry and asset preservation orders, and all directives of the AMLC; f) Cooperation with the AMLC and the IC; and f) International standards and best practices.*

3. Attendance by directors, officers and employees in all education and training programs, whether internally or externally organized, shall be documented.

4. Provide refresher training program at least every three (3) years. If there are new developments brought about by new legislations, rules and regulations, and other IC and/or AMLC issuances, immediately cascade this information to the responsible officials and employees and document accordingly.[19]

E. Employee Screening

Nat Re's Human Resource department will conduct an adequate screening and recruitment process to ensure, that only qualified personnel who have no criminal record(s) or adverse circumstances in their background that would entail a risk of involvement in money-laundering or terrorism financing, are employed to assume sensitive functions in Nat Re. [20]

F. Implementation of a Money Laundering and Terrorism Financing Prevention Program (MTPP)

Nat Re's Board of Directors (BOD) shall approve, and the compliance officer shall implement, a comprehensive, risk-based MTPP geared towards the promotion of high ethical and professional standards and the prevention of Money Laundering and Terrorism Financing.

The MTPP shall be regularly updated at least once every two (2) years to incorporate changes in AML policies and procedures, latest trends in ML and TF typologies, and latest pertinent IC and/or AMLC issuances.

Any revision or update in the MTPP shall likewise be approved by the BOD. The compliance officer shall submit to the IC not later than fifteen (15) days from the approval of the Board of Director of the new/updated MTPP a sworn certification that a new/updated MTPP has been prepared, duly noted and approved by the BOD. [21]

[19] Section 4, IC CL 2019-65

[20] Section 3, IC CL 2019-65

G. Independent Review of the Money Laundering and Terrorism Financing Prevention Program (MTPP)

The Internal Audit will include in the audit program the review of the completeness and accuracy of information obtained from customers, the covered and suspicious transaction reports submitted to AMLC, and all other records and internal control pertaining to compliance with AML/CTF obligations. Internal audit shall be conducted at least once a year. [21]

I. Scope of Internal Audit

The internal audit function shall be responsible to perform an independent review on a regular basis or at least every once a year and establish an audit program to obtain reasonable assurance on Nat Re's compliance with the applicable AML/CTF laws and regulations.

The internal audit program, at a minimum, shall include the following:

a. Verify the existence and implementation of the duly approved AML/TFPP;
b. Perform independent evaluation of the risk assessment and management to prevent and detect potential ML/TF activities;
c. Review the internal control mechanisms related to the customer due diligence such as:
    1. the determination of the existence of customers, and
    2. the accuracy and completeness of the minimum customer information and documents from reliable independent sources;

d. Check the establishment and effectiveness of a monitoring system for AML/CTF with a name screening mechanism, whether electronic or manual, that is capable of generating timely report;

e. Verify whether a duly authorized compliance officer of a senior management status is designated to monitor day to day compliance of Nat Re with AML/CTF obligations;

f. Evaluate whether all responsible directors, officers and employees have:
    1. Adequate training and continuing education program,
    2. Unrestricted access to AML/CTF guidelines, and
    3. Undergone systematic employee screening before onboarding;

g. Assess the compliance with the other AML/CTF requirements as follows:
    1. to keep and retain records of the customers' transactions and documents for at least five (5) years,
    2. to identify, monitor and report CT and ST to the competent authorities,
    3. to cooperate and comply with investigations, assessments, directives and orders of the Insurance Commission and other competent authorities,
    4. to obtain appropriate level of approval for new products and business practices,
    5. to monitor and update the required information and identification documents of existing customers,

6. to formulate or update the AML/TFPP in accordance with the applicable AML/CTF laws and their respective implementing rules and regulations, and other directives, guidance and issuances from the IC and AMLC.[21]

II. Reporting of Internal Audit Results

The internal audit function shall have the support of the board of directors and senior management to effectively perform its responsibilities and shall report directly to the board's audit committee.

The results of the internal audit shall be timely communicated to the senior management, compliance officer and board of directors and shall be available to the Insurance Commission and other competent authorities upon request for compliance checking.

The internal audit function shall be assisted by the risk and compliance function on monitoring the corrective actions taken by the concerned business unit and shall report to the board's risk oversight committee on management's action to address deficiencies noted in the internal audit report.

Section 6: Administrative Actions

The IC shall impose administrative sanctions upon Nat Re, including its board of directors, senior management and officers, for violations of these Guidelines, or for failure or refusal to comply with the orders, resolutions and other issuances of the IC.

Violation of the regulatory guidelines for AML/CTF shall be subject to the following enforcement actions against the board of directors, senior management and officers by the IC, not necessarily according to priority and whenever applicable:

a. Written reprimand;
b. Suspension or removal from the office they are currently holding; or
c. Disqualification from holding any position in any covered institution.

Further, failure to comply with the requirements under AML/CTF Guidelines shall be taken into account in the renewal of Nat Re's Certificate of Authority.

In addition to the non-monetary sanctions stated above, the IC shall also impose monetary penalties against Nat Re *(classified under Large A entity, with total asset base of Php 1.0 B to Php 50.0 B)* based on the following specific violations and their corresponding fines:

GRAVE VIOLATIONS	FINE
1. **Full access of the Compliance checker**. Non-compliance with the requirement to immediately make available, give full access and submit to the compliance checker any and all information and documents, including customer record and transaction documents, as he or she may require and/or to allow the officers and staffs of Nat Re be interviewed during compliance checking.	Computation of fine is on per customer or violation basis. P150,000.00 per violation, but not exceeding P3.750 Million

[21] Section 5, 2018 revised IRR of RA 9160; Sections 3 & 11, IC CL 2019-65

2. **Digitization of customer records.** Non-compliance with the Guidelines on Digitation of Customer Records	Computation of fine is on per account or customer basis. P150,000.00 per violation, but not exceeding P3.750 Million
MAJOR VIOLATIONS	**FINES**
1. **Customer Identity.** Non-compliance with the requirement to establish and record the true identity of each customer and/or person on whose behalf the transaction is being conducted.	Computation of fine is on per customer basis. P 75,000.00 per violation but not exceeding P750,000.00
2. **Record retention.** Non-compliance with the requirement to retain and safely keep records beyond the five (5)-year period, where the account is the subject of a case, until it is officially confirmed by the AMLC Secretariat that the case has been resolved, decided or terminated with finality.	Computation of fine is on per account basis. P75,000.00 per violation, but not exceeding P750,000.00
3. **Reporting of suspicious transactions.** Non-compliance with the requirement to report to the AMLC suspicious transactions. Reporting of suspicious transactions to the AMLC beyond the prescribed period shall constitute non-compliance with the requirement to report	Computation of fine is on per transaction basis. P75,000.00 per violation, but not exceeding P750,000.00
SERIOUS VIOLATIONS	**FINES**
1. **Reporting of covered transactions.** Non-compliance with the requirement to report to the AMLC covered transactions. Reporting of covered transactions to the AMLC beyond the prescribed period shall constitute non-compliance with the requirement to report.	Computation of fine is on per transaction basis P 37,500.00 per violation but not exceeding P375,000.00
2. **Customer verification.** Non-compliance with the requirements on Customer Verification.	Computation of fine is on per customer basis P 37,500.00 per violation but not exceeding P375,000.00
3. **Customer risk profiling.** Non-compliance with the requirements on Customer Risk Profiling	Computation of fine is on per account basis P 37,500.00 per violation but not exceeding P375,000.00
4. **Institutional risk assessment.** Non-compliance with the requirements to conduct institutional risk assessment	Computation of fine is on per compliance checking or monitoring basis P 37,500.00 per violation but not exceeding P375,000.00
5. **Risk assessment.** Non-compliance with the requirements on new product, new business practice or new technology risk assessment.	Computation of fine is on per new product, new business practice or new technology basis P 37,500.00 per violation but not exceeding P375,000.00
6. **Politically-exposed persons (PEPs).** Non-compliance with the requirements of the provisions on Politically-Exposed Persons	Computation of fine is on per customer basis P 37,500.00 per violation but not exceeding P375,000.00
7. **High-risk jurisdiction.** Non-compliance with the requirements of the provisions on High-Risk Jurisdiction or Geographical Location [22]	Computation of fine is on per customer basis P 37,500.00 per violation but not exceeding P375,000.00

[22] FATF website, high risk jurisdiction are countries identified by the Financial Action Task Force (FATF) as having significant strategic deficiencies in combating money laundering, terrorism financing, and proliferation financing. e.g. "grey list"

8. **Update customer information.** Non-compliance with the requirement to monitor and update all information and identification documents of existing customers	Computation of fine is on per customer basis P 37,500.00 per violation but not exceeding P375,000.00
9. **Transaction monitoring system.** Non-compliance with the requirement to establish a transaction monitoring system	Computation of fine is on per compliance checking or inspection basis P 37,500.00 per violation but not exceeding P375,000.00
10. **Anonymous accounts.** Allowing the opening of anonymous accounts, accounts under fictitious names, and all other similar accounts.	Computation of fine is on per account basis P 37,500.00 per violation but not exceeding P375,000.00
11. **Record retention.** Non-compliance with the requirement to maintain and safely store for at least five (5) years from the dates of transactions, or from dates the accounts were closed, all records of transactions, including customer identification documents.	Computation of fine is on per account basis P 37,500.00 per violation but not exceeding P375,000.00
12. **AMLC Registration**. Non-compliance with the requirement to register with the AMLC's electronic reporting system within the prescribed period.	Computation of fine is on per compliance checking or monitoring basis P 37,500.00 per violation but not exceeding P375,000.00
13. **Update AMLC Registration.** Non-compliance with the requirement to update registration with the AMLC's electronic reporting system as required under the ARRG.	Computation of fine is on per compliance checking or monitoring basis P 37,500.00 per violation but not exceeding P375,000.00
14. **Update the MTPP.** Non-compliance with the requirement to formulate or update the MTPP in accordance with the provisions of the AML and CTF Laws, their respective implementing rules and regulations, AML/CTF Guidelines and applicable IC and AMLC issuances	Computation of fine is on per compliance checking or monitoring basis P 37,500.00 per violation but not exceeding P375,000.00
15. **Verification of beneficial ownership.** Non-compliance with the requirement on Verification of Beneficial Ownership	Computation of fine is on per account basis P 37,500.00 per violation but not exceeding P375,000.00
16. **Purpose of relationship.** Non-compliance with the requirement on Determination of the Purpose of Relationship	Computation of fine is on per account basis P 37,500.00 per violation but not exceeding P375,000.00
17. **Ongoing monitoring.** Non-compliance with the requirement on Ongoing Monitoring	Computation of fine is on per account basis P 37,500.00 per violation but not exceeding P375,000.00
18. **Targeted financial sanctions.** Non-compliance with the requirements on Implementation of Targeted Financial Sanctions	Computation of fine is on per transaction basis P 37,500.00 per violation but not exceeding P375,000.00
19. **Shell company.** Non-compliance with the requirements on Shell Company	Computation of fine is on per transaction basis P 37,500.00 per violation but not exceeding P375,000.00

LESS SERIOUS VIOLATIONS	FINES
1. **Minimum customer information.** Non-compliance with the requirement to obtain all the minimum customer information and/or identification documents required from juridical entities	Computation of fine is on per account or customer basis P 18,750.00 per violation but not exceeding P187,500.00
2. **Continuing education**. Non-compliance with the requirement on Continuing Education and Training Program	Computation of fine is on per compliance checking or monitoring basis P18,750.00 per violation but not exceeding P187,500.
3. **MTPP requirements.** Non-compliance with the requirements on the contents of the MTPP (Insufficient Contents)	Computation of fine is on per compliance checking or monitoring basis P18,750.00 per violation but not exceeding P187,500
LIGHT VIOLATIONS	**FINES**
1. **No electronic copies**. Non-compliance with the requirement to keep electronic copies of all CTRs or STRs for at least five (5) years from the dates of submission to the AMLC.	Computation of fine is on per violation basis P 7,500.00 per violation but not exceeding P75,000.00
2. **Non-submission of required Sworn Certification on board approval.** Non-compliance with the requirement to submit to the IC not later than fifteen (15) days from the approval of the BOD of the new/updated MTPP a sworn certification that a new/updated MTPP has been prepared, duly noted and approved by Nat Re's BOD.	Computation of fine is on per violation basis P 7,500.00 per violation but not exceeding P75,000.00
3. **No MTPP.** Non-submission of an acceptable BOD-approved plan within the deadline and/or failure to implement its action plan.	Computation of fine is on per violation basis P 7,500.00 per violation but not exceeding P75,000.00

The monetary penalties on the foregoing specific violations shall not be imposed in case the specific acts or omissions constituting the violations have already been penalized by the AMLC.

Non-payment of the penalty imposed for violating the Guidelines shall be taken into account in the renewal of the Certificate of Authority.

ANNEXES

ANNEX A – Reporting Covered Transaction Reports
ANNEX B –Reporting Suspicious Transaction Reports

RECOMMENDED BY:

original signed

JACQUELINE MICHELLE C. DY
Head, Risk and Compliance

APPROVED BY:

(original signed)

ALLAN R. SANTOS
President & CEO

Date approved: March 26, 2026

(original signed)

REX MARIA A. MENDOZA
Chairman, Governance & Related Party Transaction Committee (GRPT)

Date approved: March 26, 2026

(original signed)

EVELINA G. ESCUDERO
Chairperson of the Board

Date approved: March 26, 2026

Electronic Record Format X - for IC Supervised Covered Persons

HEADER RECORD

FIELD NO.	FIELD NAME	TYPE	LENGTH	FORMAT	VALUE/REMARKS	DESCRIPTION
H-1	Header Record Indicator	Text	1	H	**H** - for Header	This field should contain "H" to indicate the beginning of the Header record.
H-2	Supervising Agency	Number	1	9(1)	**3**-IC	This field represents the supervising agency (for IC) of the reporting covered person.
H-3	Institution Code	Number	18	9(18)	AMLC Library	This refers to the 18-digit code of the reporting covered person.
H-4	Report Type/STR Type	Text	5	X (5)	**CTR, STRA, STRR, STRHU, STRHP**	Identifies whether report is CTR, STRA, STRR, STRHU, STRHP
H-5	Format Code	Text	1	X (1)	**X -** GoTRACS Format (Format X)	Identifies the version of the CTR/STR's Format Structure
H-6	Submission Type	Text	1	X (1)	**A**- add, **E**- edit/correction, **D**- delete, **T**-test	Indicates whether the report being submitted is new, correction of previously submitted report, for deletion and test file.

DETAIL RECORD

Transaction Data

FIELD NO.	FIELD NAME	TYPE	LENGTH	FORMAT	VALUE/REMARKS	DESCRIPTION
D-TD-1	Detail Record Indicator	Text	1	D	**D** - for Detail	Contains "D" indicating start of detail record for each transaction.
D-TD-2	Transaction Date	Number	8/14	9(8)/ 9(14)	Year Month Date Format (**YYYYMMDD**)	Date when transaction occurred in year, month, and day format (YYYYMMDD).
D-TD-3	Transaction Code	Text	10	X (10)	AMLC Transaction Codes	Refers to the type of transaction based on AMLC Transaction Codes. (Please refer to AMLC System Codes.)
D-TD-4	Transaction Reference No.	Text	100	X (100)		Refers to the unique reference number assigned by the covered person to its individual transaction.
D-TD-5	Mode of Transaction	Number	2	9(2)	**1** – OTC - Cash xxxxxx **0** – Others Please refer to **Annex F** (MOT Table) for the complete list of MOT and its mandatory fields/ parties.	Indicates the mode of transaction used by the involved party in the transaction.
D-TD-6	Official/ Provisional Receipt no.	Text	40	X (40)		Refers to the Issued Official/Provisional Receipt Number
D-TD-7	Php Premium Payment/ Php Amount of Claim/ Dividend/ CSV	Number	20	9(18).99	Php Amount	Peso Amount for: For Premiums, this should be limited to the premium amount based on the policy

FIELD NO.	FIELD NAME	TYPE	LENGTH	FORMAT	VALUE/REMARKS	DESCRIPTION
	Php Policy Loan/ Loan Release Amount Php Amount of Capital Infusion Php Amount of Collateral PHP amount of reinsurance Php amount paid under OPEX					owner schedule of payment, any excess or top-ups should be indicated in D-TD-15. Field is also for Amount of Claim, Dividend, Policy Loan, Loan release amount, Capital Infusion and Collateral.
D-TD-8	Php Annualized Premium/ Php Loan Availment Amount	Number	20	9(18).99	Php Amount	Refers to the Philippine Peso amount of annual premium received by the insurance company or its equivalent if transaction is in foreign currency. Amount of Approved Loan. Amount should be greater than 0.
D-TD-9	Php Policy Amount/ Face Value/ Php Contract Value/Sum Insured/ Php Loan Availment Amount	Number	20	9(18).99	Php Amount	Amount in Philippine peso for which the policy is purchased from the insurance company or its agents.
D-TD-10	Policy Effectivity Date	Number	8	9(8)	Year Month Date Format **(YYYYMMDD)**	The date when the policy contract becomes effective, or the date specified on the certificate of insurance as the beginning of coverage. It should not be less than 1900.
D-TD-11	Maturity Date/ Expiry Date	Number	8	9(8)	Year Month Date Format **(YYYYMMDD)** Date should be between the transaction date and the policy date +100 years. For HMO – 1 year from effectivity date	Date when the financial obligation/services/benefits become due or when the policy matures, or the contract expires. It should be between the transaction date and the policy date +100 years.
D-TD-12	Policy/ Insurance/ Product Type	Text	30	X (30)	Life, variable, non-life, pre-need, MBA, HMO, etc.	Refers to the policy/insurance/product type.
D-TD-13	Terms of Insurance Policy (in years)	Number	3	9(3)		Refers to the coverage (in years) of the insurance policy.
D-TD-14	Policy No./ Certificate No	Text	40	X (40)		Refers to the assigned Insurance Policy No.
D-TD-15	Php Excess/ Premium/ Payment/ Top-ups/	Number	20	9(18).99	Php Amount	Refers to the Philippine Peso amount of excess, advance premiums or payments, and top-ups received by the insurance company or its equivalent if transaction is in foreign currency. Amount should be greater than 0.
D-TD-16	Promissory Note	Text	40	X (40)		Refers to the associated promissory note/account number of the loan

FIELD NO.	FIELD NAME	TYPE	LENGTH	FORMAT	VALUE/REMARKS	DESCRIPTION
D-TD-17	Old Policy No./ Old Certificate No.	Text	40	X (40)		For reinvestment of matured policies. Refers to the old policy/certificate no.
D-TD-18	Nature/ Purpose of Transaction	Text	200	X (200)		Explains the nature or purpose of transaction or any additional information on the transaction.
D-TD-19	FX amount/ equivalent If the transaction under **D-TD-7** is a foreign currency transaction.	Number	20	9(18).99	FX Amount	
D-TD-20	FX Currency code of **D-TD-19**	Text	3	X (3)	Please see **Annex L** for the complete list of Currency Codes.	
D-TD-21	FX amount/ equivalent If the transaction under **D-TD-8** is a foreign currency transaction.	Number	20	9(18).99	FX Amount	
D-TD-22	FX Currency code of **D-TD-21**	Text	3	X (3)	Please see **Annex L** for the complete list of Currency Codes.	
D-TD-23	FX amount/ equivalent If the transaction under **D-TD-9** is a foreign currency transaction.	Number	20	9(18).99	FX Amount	
D-TD-24	FX Currency code of **D-TD-23**	Text	3	X (3)	Please see **Annex L** for the complete list of Currency Codes.	

Subject Party Data: Other Participant Bank

FIELD NO.	FIELD NAME	TYPE	LENGTH	FORMAT	VALUE/REMARKS	DESCRIPTION
D-OPB-1	OPB Flag	Text	3	OPB	**OPB**-Other Participant Bank	This should contain "OPB" indicating start of the other participant bank data. For multiple participant banks involved, each name shall be preceded by its corresponding party flag "OPB".
D-OPB-2	Other Participant Bank Type	Text	2	X (2)	**CB**-Correspondent Bank (International remittances) **IB** – Intermediary Bank/Pass Thru Bank **DB**-Drawee Bank/Issuing Bank **OB** – Originating Bank (Inward Remittances) **OP**-Other CP/Partner Bank/Credit Card **RB** – Receiving Bank (Outward Remittances) **RT**-Remittance Tie-up **PB** – Presenting Bank **VA** – Virtual Asset Service Provider	
D-OPB-3	Name of Other Participant Bank	Text	90	X (90)		Name of: Correspondent Bank/ Partner Bank/ Remittance Tie-Up/ Issuing Bank/ Drawee Bank

FIELD NO.	FIELD NAME	TYPE	LENGTH	FORMAT	VALUE/REMARKS	DESCRIPTION
D-OPB-4	Amount	Number	20	9(18).99	Amount	Amount involved
D-OPB-5	Check Number or Account Number/ Credit Card No.	Text	50	X (50)		Indicate the check number for Check transactions. Account number for Debit or credit transactions
D-OBP-6	Currency Code	Text	3	X (3)	Please see **Annex L** for the complete list of Currency Codes.	Indicates the currency of the FX transaction derived from AMLC's currency codes. Mandatory if D-OPB-5 is mandatory and is an FX amount.
D-OPB-7	City or Country	Text	200	X (200)	City Code or Country Code **Annex N** for City Codes **Annex M** for Country Codes	City Codes if within the Philippines Country Code if outside the Philippines
D-OPB-8	Swift Code	Text	50	X (50)	Swift Code of the Other Participant Bank	For international banks, if field is tagged as mandatory as per table of transaction code and swift is not available, please use a unique reference number/code.

Subject Party Data: Policy Owner

FIELD NO.	FIELD NAME	TYPE	LENGTH	FORMAT	VALUE/REMARKS	DESCRIPTION
D-O-1	Party Type Flag	Text	1	X	**O – Policy Owner/Customer**	This should contain "O" to indicate that the subject is a Policy Owner/Customer. For multiple Policy Owner/Customers, each Policy Owner/Customer information shall be preceded by its corresponding party flag "O".
D-O-2	Customer Reference Number	Text	50	X (50)		Refers to the covered person's reference number of their Policy Owner/Customer. This will serve as reference for the static data to be submitted by the reporting institution
D-O-3	Name Flag	Text	2	X (2)	**J** – if Policy Owner/Customer is a Juridical person	Use Name Flag "J" if Policy Owner/Customer is a Juridical Person (ie. Corporation, Partnership)
					CP - if Policy Owner/Customer is a Covered Person	Use Name Flag "CP" if the Policy Owner/Customer is a Covered person.
					CO - if Policy Owner/Customer is a Cooperative	Use Name Flag "CO" if the Policy Owner/Customer is a Cooperative
					S – if Policy Owner/ Customer is a Sole Proprietor	Use Name Flag "S" if Policy Owner/Customer is a Sole Proprietor
					O – if Policy Owner/ Customer is a One Person Corporation	If Policy Owner/Customer is a One Person Corporation
					N – if Policy Owner/Customer is a Natural Person	Use Name Flag "N" if Policy Owner/Customer is a Natural Person (i.e.. individual)
D-O-4	**Name of Policy Owner/ Customer**	Text				**Last Name Field Only –** for Corporation, Partnership, Sole Proprietorship, One Party Corporation, Cooperative, or Other CP, and Unknown Name Flag. (Name Flag J, CP, CO, S, O & U)
	Last Name		150	X (150)	Last name of policy owner/customer or name of entity or Unknown if Name flag is **U.**	

FIELD NO.	FIELD NAME	TYPE	LENGTH	FORMAT	VALUE/REMARKS	DESCRIPTION
	First Name		150	X (150)	First name of policy owner/customer	For Unknown, the word "Unknown" should be indicated in the last name field. Last Name, First Name, Middle Name (if available) – for Natural Person (Name Flag I) For foreign nationals with one (1) name only, the following should be observed: • Complete Name should be placed in Last Name field • There should be five (5) dots (.....)in the first name Nationality will be mandatory (use country code)
	Middle Name		150	X (150)	Middle name of policy owner/customer	
D-O-5	Complete Address	Text	600	X (600)	Complete Address	Gives the detailed address of the Policy Owner/ Customer, specifying the: Room No./ Office Name, building/house no., Street, District, Town, City, Province
D-O-6	Country Code Address	Number	10	9(10)	Please see **Annex M** for the complete list of Country Codes.	Country Code of the Policy Owner/Customer's complete address
D-O-7	City code	Text	200	X(200)	Please refer to **Annex N** for the list of City codes)	City Code of the Policy Holder's complete address Mandatory if Address is Philippines (Country Code 608) For City Codes not included in the list, the covered persons shall use the "**0000000000**" followed by a semi-colon and the name of the region, province, and city, separated by dash (-). • Example: 0000000000;[Region ABC-Province XYZ-Brgy123]
D-O-8	Birthdate/ Registration Date	Number	8	9(8)	Year Month Date Format (YYYYMMDD)	For Natural Persons: The Date of Birth of the Policy Owner/Customer For Juridical persons: The Registration Date of the Company
D-O-9	Place of Birth/ Registration	Text	90	X (90)	City Code or Country Code **Annex N** for City Codes **Annex M** for Country Codes	City Codes for Filipino and Filipino Entities Country Code for Foreign Nationals and Entities
D-O-10	Nationality	Text	40	X (40)	City Code or Country Code **Annex N** for City Codes **Annex M** for Country Codes	City Codes for Filipino and Filipino Entities Country Code for Foreign Nationals and Entities
D-O-11	ID Type	Text	4	X (4)	**ID1** – Passport xxxxx **ID27** – Others Please refer to **Annex I** for the list of valid ID Types.	Type of ID presented by the Policy Owner/ Customer (whether Natural or Legal in Nature) For ID Type 0 – Others – the ID no. should be preceded by the ID Type. Please make sure that the ID type indicated does not fall in any one of the ID types before using ID0.
D-O-12	Identification No.	Text	30	X (30)		Identification No. of the Policy Owner/Customer For ID Type 0 – Others – the ID no. should be preceded by the ID Type.

FIELD NO.	FIELD NAME	TYPE	LENGTH	FORMAT	VALUE/REMARKS	DESCRIPTION
						Details should contain the complete ID type and ID number, separated by dash (-). • Example: ID0;[other ID not listed- 12345] The Identification Number must match when uploading the mandatory KYC documents and/or STR attachment and can be clearly identified.
D-O-13	Source of Fund	Text	35	X (35)	**SF1** – Employed **SF2** - Business **Xxxxxxx** **SF13** – Covered Services under the AMLA **SF0** – Others Please refer to **Annex J** for the list of Source of Fund.	Specifies the occupation of the Account Holder/Customer, or nature of the business of the Company For Source of Fund Details should contain the specific Source of Fund. SF1 – Employed; (Name of Company) SF2 – Business; (Name of Business) SF13-Covered Service;(Specific covered service as enumerated in Annex J) SF0; [other Source of Fund not listed] For SF0, please ensure that source of funds does not fall in any one of the listed.
D-O-14	Contact No.	Text	15	X (15)		Contact number of the Policy Owner/Customer, whether in Landline/Fax/Mobile Number.

Subject Party Data: Other Parties

FIELD NO.	FIELD NAME	TYPE	LENGTH	FORMAT	VALUE/REMARKS	DESCRIPTION
D-OP-1	Party Type Flag	Text	1	X (1)	**B – Beneficiary** **I – Insured** **E – Trustee** **R – Payor/Trustor** **T – Transactor** **P – Other Participant**	· The party flag "B" refers to the beneficiary/recipient. · The party flag "I" refers to the insured. · The party flag "E" refers to the trustee. · The party flag "R" refers to the payor/trustor. · The party flag "T" is for the transactor. This is the person executing the transaction. · For transactions involving parties other than the policy owner/customer, beneficiary, insured, trustee, payor/trustor, the party flag "P" for other party shall be used. For multiple parties, each party information shall be preceded by their corresponding party flags.
D-OP-2	Customer Reference Number	Text	50	X (50)		Refers to the covered person's reference number of the subject party. This will serve as reference for the static data to be submitted by the reporting institution.
D-OP-3	Name Flag	Text	2	X (2)	**J** –Juridical person	Use Name Flag "J" if Other Party is a Juridical Person (ie. Corporation, Partnership)
					CP - Covered Person	Use Name Flag "CP" if Other Party is a Covered Person
					CO –Cooperative	Use Name Flag "CO" if Other Party is a Cooperative

FIELD NO.	FIELD NAME	TYPE	LENGTH	FORMAT	VALUE/REMARKS	DESCRIPTION
					S –Sole Proprietor	Use Name Flag "S" if Other Party is a Sole Proprietor
					O – One Person Corporation	Use Name Flag "O" if Other Party is a One Person Corporation
					N– Natural Person	Use Name Flag "N" if Other Party is a Natural Person (i.e. individual)
					U – Unknown subject	The name flag "U" indicates that the subject party is unidentified, and shall be applicable only on the following: • Subject of Suspicion – perpetrator is unknown (i.e. hacking incidents, etc.)
D-OP-4	Name of Subject	Text				Last Name Field Only – for Corporation, Partnership, Sole Proprietorship, One Party Corporation, Cooperative, or Other CP, and Unknown Name Flag. (Name Flag J, CP, CO, S, O & U) For Unknown, the word "Unknown" should be indicated in the last name field. Last Name, First Name, Middle Name (if available) – for Natural Person (Name Flag I) For foreign nationals with one (1) name only, the following should be observed: Complete Name should be placed in Last Name field There should be five (5) dots (.....)in the first name Nationality will be mandatory (use country code)
	Last Name		150	X (150)	Last name or name of entity or Unknown if Name flag is **U.**	
	First Name		150	X (150)	First name of subject data	
	Middle Name		150	X (150)	Middle name of subject data	
D-OP-5	Complete Address	Text	600	X (600)	Complete Address	Gives the detailed address of the subject of suspicion, specifying the: Room No./Office Name, building/house no., Street, District, Town, City, Province
D-OP-6	Country Code Address	Number	10	9(5)	Please see **Annex M** for the complete list of Country Codes.	Country Code of the subject party's complete address
D-OP-7	City Code	Text	200	X (200)	Please refer to **Annex N** for the list of City codes)	City Code of the subject party's complete address Mandatory if Address is Philippines (Country Code 608) (Please refer to **Annex Q** for the list of City codes.) For City Codes not included in the list, the covered persons shall use the "**0000000000**" followed by a semi-colon and the name of the region, province, and city, separated by dash (-). • Example: 0000000000; [Region ABC-Province XYZ-Brgy123]
D-OP-8	Birthdate/ Registration Date	Number	8	9(8)	Year Month Date Format (YYYYMMDD)	For Natural Persons: The Date of Birth of the Subject For Juridical persons: The Registration Date of the Company
D-OP-9	Place of Birth/ Registration	Text	90	X (90)	City Code or Country Code **Annex N** for City Codes **Annex M** for Country Codes	City Codes for Filipino and Filipino Entities Country Code for Foreign Nationals and Entities
D-OP-10	Nationality	Text	40	X (40)	City Code or Country Code **Annex N** for City Codes **Annex M** for Country Codes	City Codes for Filipino and Filipino Entities Country Code for Foreign Nationals and Entities

FIELD NO.	FIELD NAME	TYPE	LENGTH	FORMAT	VALUE/REMARKS	DESCRIPTION
D-OP-11	ID Type	Text	4	X (4)	**ID1** – Passport xxxxx **ID27** – Others Please refer to **Annex I** for the list of valid ID Types.	Type of ID presented by the Subject Data (whether Natural or Legal in Nature) For ID Type 0 – Others – the ID no. should be preceded by the ID Type. Please make sure that the ID type indicated does not fall in any one of the ID types before using ID0.
D-OP-12	Identification No.	Text	30	X (30)		Identification No. of the Subject Data (whether Natural or Legal in Nature) For ID Type 0 – Others – the ID no. should be preceded by the ID Type. Details should contain the complete ID type and ID number, separated by dash (-). • Example: ID0; [other ID not listed- 12345] The Identification Number must match when uploading the mandatory KYC documents and/or STR attachment and can be clearly identified.
D-OP-13	Source of Fund	Text	35	X (35)	**SF1** – Employed **SF2** - Business **Xxxxxxx** **SF13** – Covered Services under the AMLA **SF0** – Others Please refer to **Annex J** for the list of Source of Fund.	Specifies the occupation of the Account Holder/Customer, or nature of the business of the Company For Source of Fund Details should contain the specific Source of Fund. SF1 – Employed; (Name of Company) SF2 – Business; (Name of Business) SF13-Covered Service;(Specific covered service as enumerated in Annex J) SF0; [other Source of Fund not listed] For SF0, please ensure that source of funds does not fall in any one of the listed.
D-OP-14	Relationship of Beneficiary to Account Holder/ Insured	Text	30	X (30)	Spouse, child, parents, friend, others	Indicates the relationship of the beneficiary to the account holder/insured
D-OP-15	Designation of Beneficiary Code	Text	1	X (1)	**Y** – Revocable **N** - Irrevocable	Indicates if the designation to beneficiary is revocable or not
D-OP-16	Account Number	Text	40	X (40)	Account Number of the Subject Data	Refers to the assigned Account Number of the Subject Data, Or Client Stock Ref. No. for securities or the Virtual Currency Wallet Address separated by a slash (/). For Covered Persons not maintaining Accounts, please use reference number relating to the Transaction, which is different from the Transaction Reference Number.
D-OP-17	Contact No.	Text	15	X (15)		Contact number of the Subject Data, whether in Landline/Fax/Mobile Number.

Subject Party Data: Subject of Suspicion Data

FIELD NO.	FIELD NAME	TYPE	LENGTH	FORMAT	VALUE/REMARKS	DESCRIPTION
D-S-1	Party Type Flag	Text	1	S	**S – Subject of Suspicion**	This should contain "S" to indicate that the subject party is the Subject of Suspicion. For multiple subjects of suspicion, each subject of suspicion information shall be preceded by its corresponding party flag "S".
D-S-2	Customer Reference Number	Text	50	X (50)	CP's reference number of the client	Refers to the CP's reference number of their client. This will serve as reference for the static data to be submitted by the reporting institution
D-S-3	Name Flag	Text	2	X (2)	**J** – if the subject of suspicion is a Juridical Person	Use Name Flag "J" if the subject of suspicion party is a Juridical person. (ie. Corporation, Partnership)
					CP – if the subject of suspicion is a Covered Person	Use Name Flag "CP" if the subject of suspicion party is a Covered Person
					CO – if the subject of suspicion is a Cooperative	Use Name Flag "CO" if the subject of suspicion party is a Cooperative.
					S – if the subject of suspicion is a Sole Proprietor	Use Name Flag "S" if the subject of suspicion party is a Sole Proprietor
					O – if the subject of suspicion is a One Person Corporation	Use Name Flag "O" if the subject of suspicion party is a One-Party Corporation
					N – if the subject of suspicion is a Natural Person	Use Name Flag "N" if the subject of suspicion party is a Natural Person (i.e. individual)
					U – Unknown subject of suspicion	The name flag "U" indicates that the subject of suspicion is unidentified, and shall be applicable only on the following: • Subject of Suspicion – perpetrator is unknown (ie. hacking incidents, etc.)
D-S-4	Name of Subject of Suspicion Last Name	Text	150	X (150)	Last name of subject of suspicion or name of entity or Unknown if Name Flag is **U.**	Identifies the subject of suspicion: Last Name Field Only – for Corporation, Partnership, Sole Proprietorship, One Party Corporation and Unknown Name Flag. (Name Flag C, CO, S, O & U) Last Name, First Name, Middle Name (if available) – for Natural Person (Name Flag I) For foreign nationals with one (1) name only, the following should be observed: • Name should be placed in Last Name field. • There should be five (5) dots (.....)in the first name Nationality will be mandatory
	First Name		150	X(150)	First name of subject of suspicion	
	Middle Name		150	X (150)	Middle name of subject of suspicion	
D-S-5	Complete Address	Text	600	X (600)	Complete Address	Gives the detailed address of the subject of suspicion, specifying the: Room No./ Office Name, building/house no., Street, District, Town, City, Province
D-S-6	Country Code Address	Number	10	9(10)	Please see **Annex M** for the complete list of Country Codes.	Country Code of the Subject of Suspicion's complete address

FIELD NO.	FIELD NAME	TYPE	LENGTH	FORMAT	VALUE/REMARKS	DESCRIPTION
D-S-7	City Code	Text	200	X (200)	Please refer to **Annex N** for the list of City Codes.	City Code of the Subject of Suspicion's complete address Mandatory if Address is Philippines (Country Code 608) For City codes not included in the list, the covered persons shall use the "0000000000" followed by a semi-colon and the name of the region, province, and city, separated by dash (-). • Example: 0000000000; [Region ABC-Province XYZ-Brgy123]
D-S-8	Account Number/ Policy Number	Text	40	X (40)	Account/Policy Number of the Subject of Suspicion	Refers to the assigned Account Number of the Subject of Suspicion. Or Client Stock Ref. No. for securities or the Virtual Currency Wallet Address separated by a slash (/). For Covered Persons not maintaining Accounts, please use reference number relating to the Transaction, which is different from the Transaction Reference Number.
D-S-9	Birthdate/ Registration Date	Number	8	9(8)	Year Month Date Format (YYYYMMDD)	For Natural Persons: The Date of Birth of the Subject of Suspicion For Juridical persons: The Registration Date of the Company
D-S-10	Place of Birth/ Registration	Text	90	X (90)	City Code or Country Code **Annex N** for City Codes **Annex M** for Country Codes	City Codes for Filipino and Filipino Entities Country Code for Foreign Nationals and Entities
D-S-11	Nationality	Text	40	X (40)	City Code or Country Code **Annex N** for City Codes **Annex M** for Country Codes	City Codes for Filipino and Filipino Entities Country Code for Foreign Nationals and Entities
D-S-12	ID Type	Text	4	X (4)	**ID1** – Passport xxxxx **ID27** – Others Please refer to **Annex I** for the list of valid ID Types.	Type of ID presented by the Subject of Suspicion (whether Natural or Legal in Nature) For ID Type 0 – Others – the ID no. should be preceded by the ID Type. Please make sure that the ID type indicated does not fall in any one of the ID types before using ID0.
D-S-13	Identification No.	Text	30	X(30)		Identification No. of the Subject of Suspicion For ID Type 0 – Others – the ID no. should be preceded by the ID Type. Details should contain the complete ID type and ID number, separated by dash (-). • Example: ID0;[other ID not listed- 12345] The Identification Number must match when uploading the mandatory KYC documents and/or STR attachment and can be clearly identified.

FIELD NO.	FIELD NAME	TYPE	LENGTH	FORMAT	VALUE/REMARKS	DESCRIPTION
D-S-14	Source of Fund	Text	35	X (35)	**SF1 –** Employed **SF2** - Business **xxxxxxx** **SF13** – Covered Services under the AMLA **SF0 –** Others Please refer to **Annex J** for the list of Source of Fund.	Specifies the occupation of the Account Holder/Customer, or nature of the business of the Company For Source of Fund Details should contain the specific Source of Fund. SF1 – Employed; (Name of Company) SF2 – Business; (Name of Business) SF13-Covered Service;(Specific covered service as enumerated in Annex J) SF0; [other Source of Fund not listed] For SF0, please ensure that source of funds does not fall in any one of the listed.
D-S-15	Contact No.	Text	15	X (15)		Contact number of the Subject of Suspicion, whether in Landline/Fax/Mobile Number.

STR Details Data

FIELD NO.	FIELD NAME	TYPE	LENGTH	FORMAT	VALUE/REMARKS	DESCRIPTION
D-SD-1	STR Flag Indicator	Text	1	SF	**SD - for STR Flag**	This should contain "SD" indicating the start of Suspicious Transaction Details data
D-SD -2	Date of Determination	Number	8	9(8)	Year Month Date Format (YYYYMMDD)	Refers to the date the covered person was advised/alerted or had knowledge that a transaction/series of transactions may be related to an unlawful activity or suspicious circumstance.
D-SD -3	STR Trigger	Text	1	X	**A-**CP (proactive/alerts) **B-**PPP (Public Private Partnership); **C-**KYC Docs requested by AMLC/AMLC Referrals; **D-**Shared AMLC Studies; **E-**Watch list; **F-**Freeze Orders **G-**Targeted Financial Sanctions (TFS)	This identifies the trigger of the STR.
D-SD -4	Primary Reason for Suspicion	Memo	800	X (800)	Reason for Suspicion **Suspicious Circumstance (SC)** Please refer to **Annex K** for the list of Reason of Suspicion. Please refer to "SC" codes for Suspicious Circumstance. **Predicate Crime (PC)** Please refer to **Annex K** for the list of Reason of Suspicion. Please refer to "PC" codes for Predicate Crimes.	For STRs, reason field refers to the coded reason for suspicion categorized by suspicious circumstance (SC) or predicate crime (PC). If the value in the reason field is "SC6", the description of the suspicious activity should always be specified separated by a semicolon. Please make sure that the reason for suspicion indicated in SC6 does not fall in any one of the Suspicious Circumstance or Predicate Crimes before using SC6. Example: xxx,SC6;suspected boiler room operations, the client was named in one foreign news article xxx
D-SD -5	Additional Reason	Memo	800	X (800)	Reason for Suspicion **Suspicious Circumstance (SC)** Please refer to **Annex K** for the list of Reason of	Optional Applicable for STRs with a secondary Reason for Suspicion. In case of more than 3 Reason; Please use semi-colon to separate each Reason:

FIELD NO.	FIELD NAME	TYPE	LENGTH	FORMAT	VALUE/REMARKS	DESCRIPTION
					Suspicion. Please refer to "SC" codes for Suspicious Circumstance. **Predicate Crime (PC)** Please refer to **Annex K** for the list of Reason for Suspicion. Please refer to "PC" codes for Predicate Crimes.	e.g. PC5;PC9
D-SD -6	Narrative	Memo	200-4000	Min X (200) Max: X (10,000)	Narrative of events leading to Suspicion	Narrates the events leading to the suspicion including other information which might be of help or importance to the report, i.e., where the possible violation took place, related litigations, relation to other transactions, description of supporting documents, etc. Minimum of 200 characters.

TRAILER RECORD

FIELD NAME	TYPE	LENGTH	FORMAT	VALUE/REMARKS
Trailer Record Indicator	Text	1	T	**T** - for Trailer
Records Total of batch to be sent	Number	10	9(10)	Total number of CTR/STRs

TRANSACTION CODES FOR IC SUPERVISED COVERED PERSONS

A TRANSACTION CODE	B TRANSACTION TITLE	C TRANSACTION DEFINITION	D MANDATORY PARY FLAG	E OTHER MANDATORY PARTIES AND FIELDS AS DETERMINED BY THE TYPE OF CUSTOMER OR MODE OF TRANSACTION (MOT) D-TD-5)	F MANDATORY DATA FIELDS FOR MANDATORY PARTIES
NCAP	Capital Infusion	Infusion of funds by a shareholder to the reporting Covered Person	**O** **OPB** – if MOT is 2, 8,9, 10,11,12,14	MOT is the manner of funding for the additional capital. Please refer to MOT Table for additional mandatory fields, based on the MOT chosen	**Transaction Detail:** **D:** D-TD-1 to D-TD -7 **PARTIES** **O:** D-O-1; D-O-3 to D-O-5
NREIT	Reinsurance Transaction	Reinsurance transaction is an agreement between a ceding company and one or more reinsurers whereby the ceding company agree to cede, and the reinsurer agree to accept the reinsurance of all the risks written by the ceding company which falls within the terms subject to the limits specified therein.	**O** – Policy Owner **OBP** – other CP (OP)	**MOT 0** All Mandatory fields and Parties are defined in Column F	**Transaction Detail:** **D:** D-TD-1 to D-TD-7 **PARITES** **O:** D-O-1; D-O-3 to D-O-13 **OBP:** D-OBP-1 to D-OBP-3
NCLTR	Cancel Reinsurance Transaction	Cancellation of reinsurance transaction.	**O** – Policy Owner **OBP** – other CP (OP)	**MOT 0** All Mandatory fields and Parties are defined in Column F	**MOT - 0** **Transaction Detail:** **D:** D-TD-1 to D-TD-7 **PARITES** **O:** D-O-1; D-O-3 to D-O-13 **OBP:** D-OBP-1 to D-OBP-3
NPLCA	Cancellation of Insurance Policy Application	Refund of premium for both traditional life or life with investment policy/ Free look/ NREC cancellation	**O** **OPB** – if MOT is 2, 8,9, 10,11	MOT is the manner of refund. Please refer to MOT Table for additional mandatory fields, based on the MOT chosen	**Transaction Detail:** **D:** D-TD-1 to D-TD-7 **PARTY** **O:** D-O-1; D-O-3 to D-O-8
NPLCR	Cancellation of policy or plan by company thru rescission	Premium may be refunded depending on the nature of the case involving fraud or concealment on the part of the policyholder. Refund due to cancellation of HMO plan/service agreement" to ensure application for HMO transactions.	**O** **OPB** – if MOT is 2, 8,9, 10,11	MOT is the manner of refund. Please refer to MOT Table for additional mandatory fields, based on the MOT chosen	**Transaction Detail:** **D:** D-TD-1 to D-TD-7 **PARTY** **O:** D-O-1; D-O-3 to D-O-8
NCOL	Collateral received from clients	Collateral received from clients for the purchase of insurance policies and assets.	**O** **OPB** – if MOT is 2, 8,9, 10,11,12,14	MOT is how the collateral was received. Please refer to MOT Table for additional mandatory fields, based on the MOT chosen	**Transaction Detail:** **D:** D-TD-1 to D-TD-7 **PARTY** **O:** D-O-1; D-O-3 to D-O-13
NFFWV	Partial/Full Fund withdrawal	Fund withdrawal on a variable unit link or investment linked policy	**O, I** **OPB** – if MOT is 2, 8,9, 10,11,12,14	MOT is how the payment was released. Please refer to MOT Table for additional mandatory fields, based on the MOT chosen	**Transaction Detail:** **D:** D-TD-1 to D-TD-14 **PARTIES** **O: O:** D-O-1; D-O-3 to D-O-13 **I:** D-OP-1; D-OP-3 to D-OP-8

A TRANSACTION CODE	B TRANSACTION TITLE	C TRANSACTION DEFINITION	D MANDATORY PARY FLAG	E OTHER MANDATORY PARTIES AND FIELDS AS DETERMINED BY THE TYPE OF CUSTOMER OR MODE OF TRANSACTION (MOT) D-TD-5)	F MANDATORY DATA FIELDS FOR MANDATORY PARTIES
NLOIP	Other Loans	Other loans granted and availed by insurance or pre-need companies and HMO companies	**O** **OPB** – if MOT is 2, 8,9, 10,11	MOT is how the loan was released was received. Please refer to MOT Table for additional mandatory fields, based on the MOT chosen	**Transaction Detail:** **D:** D-TD-1 to D-TD-7 **PARTY** **O:** D-O-1; D-O-3 to D-O-13
NPLN	Policy/Plan Loans	Loan against an insurance policy or pre-need plan subject to the accrued cash surrender value and dividend.	**O** **OPB** – if MOT is 2, 8,9, 10,11	MOT is how the loan was released. Please refer to MOT Table for additional mandatory fields, based on the MOT chosen	**Transaction Detail:** **D:** D-TD-1 to D-TD-14, & D-TD-16 **PARTY** **O:** D-O-1; D-O-3 to D-O-13
NPLY	Loan Payment	Payment of policy or plan loans by the policyholders/plan holders	**O** **OPB** – if MOT is 2, 8,9, 10,11,12,14	MOT is how the payment was received. Please refer to MOT Table for additional mandatory fields, based on the MOT chosen	**Transaction Detail:** **D:** D-TD-1 to D-TD-14, & D-TD-16 **PARTY** **O:** D-O-1; D-O-3 to D-O-13
NPL	Purchase of Life Insurance Policy	Purchase of life without investment insurance policy	**O, I** **OPB** – if MOT is 2, 8,9, 10,11,12,14	MOT is how the payment was received from client. Please refer to MOT Table for additional mandatory fields, based on the MOT chosen	**Transaction Detail:** **D:** D-TD-1 to D-TD-14 **Parties:** **O:** D-O-1; D-O-3 to D-O-13 **I:** D-OP-1; D-OP-3 to D-OP-8
NPLI	Purchase of Life Insurance Policy with Investment	Purchase of life with investment insurance policy	**O, I** **OPB** – if MOT is 2, 8,9, 10,11,12,14	MOT is how the payment was received from client. Please refer to MOT Table for additional mandatory fields, based on the MOT chosen	**Transaction Detail:** **D:** D-TD-1 to D-TD-14 **Parties:** **O:** D-O-1; D-O-3 to D-O-13 **I:** D-OP-1; D-OP-3 to D-OP-8
NPPP	Premium/Plan Payment	Premium paid by the policyholder/ plan holder, including top-ups or excess premium. This is for succeeding payments	**O** **OPB** – if MOT is 2, 8,9, 10,11,12,14	Please refer to Mode of Transaction Table for other mandatory fields **I:** D-OP-1; D-OP-3 to D-OP-8 (for life insurance only)	**Transaction Detail:** **D:** D-TD-1 to D-TD-14 *D-TD-15 if with top-up* **Parties:** **O:** D-O-1; D-O-3 to D-O-13
NPNL	Purchase of non-life Insurance Policy	Purchase of non-life insurance policy	**O** **OPB** – if MOT is 2, 8,9, 10,11,12,14	MOT is how the payment was received from client. Please refer to MOT Table for additional mandatory fields, based on the MOT chosen	**Transaction Detail:** **D:** D-TD-1 to D-TD-14 **Parties:** **O:** D-O-1; D-O-3 to D-O-13
NPHMO	Purchase of HMO	Purchase of HMO, which may include riders.	**O** **OPB** – if MOT is 2, 8,9, 10,11,12,14	MOT is how the payment was received from client. Please refer to MOT Table for additional mandatory fields, based on the MOT chosen	**Transaction Detail:** **D:** D-TD-1 to D-TD-7 & T-TD-14 **Parties:** **O:** D-O-1; D-O-3 to D-O-13

A TRANSACTION CODE	B TRANSACTION TITLE	C TRANSACTION DEFINITION	D MANDATORY PARY FLAG	E OTHER MANDATORY PARTIES AND FIELDS AS DETERMINED BY THE TYPE OF CUSTOMER OR MODE OF TRANSACTION (MOT) D-TD-5)	F MANDATORY DATA FIELDS FOR MANDATORY PARTIES
NPPN	Purchase of Pre-Need Plan	Purchase of pre-need plan	**O** **OPB** – if MOT is 2, 8,9, 10,11,12,14	MOT is how the payment was received from client. Please refer to MOT Table for additional mandatory fields, based on the MOT chosen	**Transaction Detail:** **D:** D-TD-1 to D-TD-14 **Parties:** **O:** D-O-1; D-O-3 to D-O-13
NPRSD	Receipt of Refundable Security Deposits (RSD)	Receipt of RSD for clients' future claims	**O** **OPB** – if MOT is 2, 8,9, 10,11,12,14	MOT is how the payment was received from client. Please refer to MOT Table for additional mandatory fields, based on the MOT chosen	**Transaction Detail:** **D:** D-TD-1 to D-TD-7 **Parties:** **O:** D-O-1; D-O-3 to D-O-13
NPSA	Purchase/Sale of Asset	Asset purchased by members, e.g., Real estate offered to members	**O** **OPB** – if MOT is 2, 8,9, 10,11,12,14	MOT is how the payment was received from client. Please refer to MOT Table for additional mandatory fields, based on the MOT chosen	**Transaction Detail:** **D:** D-TD-1 to D-TD-7 **Party** **O:** D-O-1; D-O-3 to D-O-13
NPTT	Pretermination of Transaction (VUL Part)	Pretermination of the VUL Part of an Insurance Policy	**O** **OPB** – if MOT is 2, 8,9, 10,11	MOT is how the payment was released to client. Please refer to MOT Table for additional mandatory fields, based on the MOT chosen	**Transaction Detail:** **D:** D-TD-1 to D-TD-14 **Parties:** **O:** D-O-1; D-O-3 to D-O-13
NPYBC	Pay Benefits/Claims	Payment of benefits or claims as provided under the insurance policy, pre-need plan, or HMO companies.	**O, B, I** **OPB** – if MOT is 2, 8,9, 10,11	MOT is how the payment was released to client. Please refer to MOT Table for additional mandatory fields, based on the MOT chosen	**Transaction Detail:** **D:** D-TD-1 to D-TD-14 **Parties** **O:** D-O-1; D-O-3 to D-O-13 **B: I:** D-OP-1; D-OP-3 to D-OP-8 **I: I:** D-OP-1; D-OP-3 to D-OP-8
NPYCV	Pay Cash Surrender Value (CSV)/Equity Value	Pay cash surrender value - the amount due the assured/plan holder, net of outstanding policy loans and interest thereon, upon the surrender of the policy before its maturity date	**O** **OPB** – if MOT is 2, 8,9, 10,11	MOT is how the payment was released to client. Please refer to MOT Table for additional mandatory fields, based on the MOT chosen	**Transaction Detail:** **D:** D-TD-1 to D-TD-14 **Party** **O:** D-O-1; D-O-3 to D-O-13
NREC	Receipt of Provisional Insurance Payment	Receipt of provisional payment of sourced insurance policy, wherein the actual policy has not been issued since underwriting is still ongoing.	**O** **OPB** – if MOT is 2, 8,9, 10,11,12,14	MOT is how the payment was received from client. Please refer to MOT Table for additional mandatory fields, based on the MOT chosen	**Transaction Detail:** **D:** D-TD-1 to D-TD-7 **Party:** **O:** D-OP-1; D-OP-3 & D-OP-4
NRMP	Reinvestment of Matured Policies	Reinvestment of matured policies into other policies or investment products	**O**	**MOT 0** All Mandatory fields and Parties are defined in Column F	**Transaction Detail:** **D:** D-TD-1 to D-TD-14 & D-TD-17 **Party** **O:** D-O-1; D-O-3 to D-O-13

A TRANSACTION CODE	B TRANSACTION TITLE	C TRANSACTION DEFINITION	D MANDATORY PARY FLAG	E OTHER MANDATORY PARTIES AND FIELDS AS DETERMINED BY THE TYPE OF CUSTOMER OR MODE OF TRANSACTION (MOT) D-TD-5)	F MANDATORY DATA FIELDS FOR MANDATORY PARTIES
NRPPY	Refund of Premium Payment	Refund of excess premium payment shall cover over payment of premiums for traditional policies and refund of top-ups or excess premiums for variable or unit-link policies and HMOs.	**O** **OPB** – if MOT is 2, 8,9, 10,11	MOT is how the payment was released to client. Please refer to MOT Table for additional mandatory fields, based on the MOT chosen	**Transaction Detail:** **D:** D-TD-1 to D-TD-14 **Party** **O:** D-O-1; D-O-3 to D-O-13
NRRSD	Refund of Refundable Security Deposit	Client request return of unutilized RSD	**O** **OPB** – if MOT is 2, 8,9, 10,11	MOT is how the payment was released to client. Please refer to MOT Table for additional mandatory fields, based on the MOT chosen	**Transaction Detail:** **D:** D-TD-1 to D-TD-7 **Party** **O:** D-OP-1; D-OP-5 & D-OP-8
NPPN	Placement/ Deposits in the Form of Promissory Notes	Placement/deposit taking in the form of promissory notes/loans etc.	**O** **OPB** – if MOT is 2, 8,9, 10,11,12,14	MOT is how the payment was received from client. Please refer to MOT Table for additional mandatory fields, based on the MOT chosen	**Transaction Detail:** **D:** D-TD-1 to D-TD-7 **Party** **O:** D-O-1; D-O-3 to D-O-13
NIDCP	Payment of Interest/ Dividends/ Coupon and others	Payment of Interest/ Dividends/ Coupon and others	**O** **OPB** – if MOT is 2, 8,9, 10,11,12,14	Please refer to Mode of Transaction Table for other mandatory fields	**Transaction Detail:** **D:** D-TD-1 to D-TD-14 & D-TD-18 (Type of account, transaction, or product, e.g. investments) **PARTY** **O:** D-O-1 to D-O-13
NTAS	Transaction adjustments	Any adjustment/s made on an insurance policy initiated by clients. These may include but not limited to the following: payment term/adjustment, premium adjustment, benefit adjustment, changes in investment as a result of top-ups, change of beneficiary and other changes that may occur in a policy.	**O** – Name o of Client	**MOT 0** All Mandatory fields and Parties are defined in Column F	**Transaction Detail:** **D:** D-TD-1 to D-TD-7 & D-TD-18 (Type of account, transaction, or product, that needs to be adjusted) **PARTIES** **O: D-O-1; D-O-3 to D-O-13**
NXOFI	Other Fees and income	Collection/Payment of Management/ Admin/ Access Fees, Volume Discounts/ Rebates from Providers, Interbranch transfers (in/out), and Interest/Dividends Income and Proceeds from Investments and Other Fees related to a transaction	**O** – Name of providers, etc.	**MOT 0** All Mandatory fields and Parties are defined in Column F	**Transaction Detail:** **D:** D-TD-1 to D-TD-7 except T-TD-6 & D-TD-18 (Type of account, transaction, or product are the fees for) **O:** D-O-1; D-O-3; D-O-4
STR Related					
STRA	STR – Per Account	STR Transaction code for STRs on TFS and referrals from AMLC. (Requires the uploading of an ESOA and KYC Docs)	**S**	**MOT 0** All Mandatory fields and Parties are defined in Column F	**Transaction Detail:** **D:** D-TD-1 to D-TD-5 **Party** **O:** D-O-1 to D-O-13 **S**:D-S-1 to D-S-14

A TRANSACTION CODE	B TRANSACTION TITLE	C TRANSACTION DEFINITION	D MANDATORY FLAG	E OTHER MANDATORY PARTIES AND FIELDS AS DETERMINED BY THE TYPE OF CUSTOMER OR MODE OF TRANSACTION (MOT) D-TD-5)	F MANDATORY DATA FIELDS FOR MANDATORY PARTIES
					SD: D-SD-1 to D-SD-4; D-SD-6
ZSTR	STR transactions	Shall be used if the subject is an accountholder but has no monetary transaction with the covered person at the time the suspicious activity was determined.	**S**	**MOT 0** All Mandatory fields and Parties are defined in Column F	**Transaction Detail:** **D:** D-TD-1 to D-TD-5 **Party** **O:** D-O-1, D-O-3 to D-O-13 **S**:D-S-1; D-S-3 to D-S-14 **SD**: D-SD-1 to D-SD-4; D-SD-6
ZSTRN	STR transactions – for non-account holders	Shall be used if no account holder is party to the transaction being reported. May or may not have a monetary transaction at the time of reporting.	**S**	**MOT 0** All Mandatory fields and Parties are defined in Column F	**Transaction Detail:** **D:** D-TD-1 to D-TD-5 **Party** **S**:D-S-1; D-S-3; D-S-4 **SD**: D-SD-1 to D-SD-4; D-SD-6
ZSTRA	STR transactions	Shall be used for attempted transaction that is deemed as suspicious.	**S**	**MOT 0** All Mandatory fields and Parties are defined in Column F	**Transaction Detail:** **D:** D-TD-1 to D-TD-5 **S**:D-S-1; D-S-3; D-S-4 **SD**: D-SD-1 to D-SD-4; D-SD-6

Note:

1. For foreign currency transactions, **FX Currency Code and FX currency Amount** shall be mandatory.
2. For optional fields: Please follow the rule the if data is available, always populate said field/fields in the CTR/STR, even if tagged as optional.
3. For Transaction code with no specified MOT in column E, please refer to Annex F (MOT table) for the appropriate MOT for the C/STR being reported.
4. In addition to the mandatory fields/parties defined in Column F, **please check Column E**, if there will be additional mandatory fields/parties, based on the **MOT** used.
5. If Column E states that "All Mandatory fields/Parties are defined in Column F", please disregard the mandatory fields and parties under the MOT Table (Annex F).

MODE OF TRANSACTION TABLE

Code	Mode of Transaction	Description		Mandatory Fields for CTRs/STRs or as defined		
			BSP(Banks)	Other BSIs	SEC/DNFBPs/ Casinos/ APECO/CEZA	IC
1	Over the counter (Cash)	Pay/settle/accept hard cash to/from teller or any authorized representative.	No additional mandatory party/fields			
2	Check (1)	Pay/settle/accept a single check or multiple checks with a total of more than PHP500K, with 1 or more checks having an amount of more than PHP500K. Example: 1 Deposit Slip – 1 check (1M) 1 Deposit Slip – 2 Checks (400K & 600K) 1 Deposit Slip – 3 checks (300K, 1M, 700K)	D-OBP-1 to D-OBP-5 (No. of OBP depends on the number of checks of more than PHP500K)	D-OPB 1 – D-OBP-5 (No. of OBP depends on the number of checks of more than PHP500K)	D-OPB 1 – D-OBP-5 (No. of OBP depends on the number of checks of more than PHP500K)	D-OPB 1 – D-OBP-5 (No. of OBP depends on the number of checks of more than PHP500K)
3	Check (2)	Pay/settle/accept multiple checks with a total of more than PHP500K, with none of the checks have amounts of more than PHP500K. Example: 1 Deposit Slip – 2 Checks (400K & 400K) 1 Deposit Slip – 3 checks (300K, 500K, 200K)	No additional mandatory party/fields			
4	Debit Bank Account	Transaction is settled through debit to account. Account maintained is with the reporting CP.	D-OP-1, D-OP-3 to D-OP-14 (Counterparty – C)	For banks only	For banks only	For banks only
5	Credit – Bank Account	Transaction is settled through credit to account. Account maintained is with the reporting CP.	D-OP-1, D-OP-3 to D-OP-14 (Beneficiary – B)	For banks only	For banks only	For banks only
6	Debit EMIs	Transaction is settled through debit to e-wallet. E-wallet maintained is with the reporting CP.	D-OP-1, D-OP-3 to D-D-OP-5, D-OP-8, D-OP-9(Counterparty – C)	For banks only	For banks only	For banks only
7	Credit EMIs/	Transaction is settled through credit e-wallet. E-wallet maintained is with the reporting CP.	D-OP-1, D-O P-3 to D-OP5, D-OP-8, D-OP-9 (Beneficiary – B)	For banks only	For banks only	For banks only
8	Wire/ Remittance	Transaction is settled via wire/remittance	D-OBP-1 to D-OPB-7 Counterparty: D-OP-1, D-OP-3 & D-OP-4	D-OPB-1 to D-OPB-4 Beneficiary: D-OP-1, D-OP-3 & D-OP-4	D-OPB-1 to D-OPB-4 Beneficiary: D-OP-1, D-OP-3 & D-OP-4	D-OPB-1 to D-OPB-4 Beneficiary: D-OP-1, D-OP-3 & D-OP-4
9	Collecting Agents	Transaction is settled via collecting agents	Party type OP (Other Participant) D-OP-1, D-OP-3, D-OP-4			
10	Settled thru other banks/CPs	Pay/settle to/from depository/partner CPs of the reporting CP	D-OPB-1 to D-OPB-5	D-OPB-1 to D-OPB-5	D-OPB-1 to D-OPB-3	D-OPB-1 to D-OPB-3

GoTRACS: Mode of Transaction Table **ANNEX A**

Code	Mode of Transaction	Description		Mandatory Fields for CTRs/STRs or as defined		
			BSP(Banks)	Other BSIs	SEC/DNFBPs/ Casinos/ APECO/CEZA	IC
11	Virtual Asset	Pay/settle/transacts using virtual asset	D-OPB-1 to D-OBP-5	D-OPB-1 to D-OPB-3	D-OPB-1 to D-OPB-3	D-OPB-1 to D-OPB-3
12	Demand Draft/Treasury Fund Capital Check (TFC)	Pay/settle/transacts via Demand Draft/TFC and similar instruments.	D-OBP-1 to D-OBP-6	D-OBP-1 to D-OBP-6	D-OBP-1 to D-OBP-6	D-OBP-1 to D-OBP-6
13	Cash Deposit Machine (CDM)/ Automated Teller Machine (ATM)	Transaction via CDM or ATM	D-OBP-1, D-OBP-2 & D-OPB-4	D-OBP-1, D-OBP-2 & D-OPB-4	N/A	N/A
14	Credit Card	Pay/settle/transacts using credit cards	D-OBP-1 to D-OBP-5	D-OPB-1 to D-OPB-5	D-OPB-1 to D-OPB-3	D-OPB-1 to D-OPB-3
15	Others (such as kiosk and those not included above; also used for Mixed transactions) also for assets, securities, and the likes	Transaction is settled using other modes other than those enumerated above	E.G. 1. 15; cash check 2. 15; real estate 3. 15; securities 4. 15; no amount			
0	No monetary amount involved, agreement or contract only, or as defined in the mandatory fields for a specific transaction code					

Sample CTR for Receipt of Provisional Insurance Payment (NREC) – IC Supervised

Receipt of provisional payment of sourced insurance policy, wherein the actual policy has not been issued since underwriting is still ongoing.

Below are the mandatory fields for NREC based on:

- Annex E:

NREC	Receipt of Provisional Insurance Payment	Receipt of provisional payment of sourced insurance policy, wherein the actual policy has not been issued since underwriting is still ongoing.	**O** **OPB** – if MOT is 2, 8,9, 10,11,12,14	MOT is how the payment was received from client. Please refer to MOT Table for additional mandatory fields, based on the MOT chosen	**Transaction Detail:** **D:** D-TD-1 to D-TD-7 **Party:** **O:** D-OP-1; D-OP-3 & D-OP-4

- Annex F:

Code	Mode of Transaction	Description		Mandatory Fields for CTRs/STRs or as defined		
			BSP(Banks)	Other BSIs	SEC/DNFBPs/ Casinos/ APECO/CEZA	IC
10	Settled thru other banks/CPs	Pay/settle to/from depository/partner CPs of the reporting CP	D-OPB-1 to D-OPB-5	D-OPB-1 to D-OPB-5	D-OPB-1 to D-OPB-3	D-OPB-1 to D-OPB-3

Sample CTR:

- **Transaction Detail**

A	B	C	D	E	F	G
H	3	723456789000000000	CTR	X	A	
D	20240604	NREC	TRANSREF1	10	OR000090	550000
T	1					

- **Transaction Party Data: Other Participant Bank/Covered Person**

H	I	J
OPB	OP	ABC BANK CORP.

- **Subject Party Data: Policy Owner**

K	L	M	N	O	P
O		N	DELA CRUZ	JUAN	CRUZ

Sample CTR for Purchase of Life Insurance Policy (NPL) – IC Supervised

Purchase of life without investment insurance policy

Below are the mandatory fields for NPL based on:

- Annex E:

NPL	Purchase of Life Insurance Policy	Purchase of life without investment insurance policy	**O, I** **OPB** – if MOT is 2, 8,9, 10,11,12,14	MOT is how the payment was received from client. Please refer to MOT Table for additional mandatory fields, based on the MOT chosen	**Transaction Detail:** **D:** D-TD-1 to D-TD-14 **Parties:** **O:** D-O-1; D-O-3 to D-O-13 **I:** D-OP-1; D-OP-3 to D-OP-8

- Annex F:

Code	Mode of Transaction	Description	Mandatory Fields for CTRs/STRs or as defined			
			BSP(Banks'	Other BSIs	SEC/DNFBPs/ Casinos/ APECO/CEZA	IC
0	No monetary amount involved, agreement or contract only, or as defined in the mandatory fields for a specific transaction code					

Sample CTR:

- **Transaction Detail**

A	B	C	D	E	F	G	H	I	J	K	L	M	N
H	3	723456789000000000	CTR	X	A								
D	20240604	NPL	TRANSREF2	0	OR000029	300000	1200000	13000000	20240604	20340603	Life	10	POL123456
T	1												

- **Subject Party Data: Policy Owner**

O	P	Q	R	S	T	U	V	W	X	Y	Z	AA	AB	AC
O		N	DELA CRUZ	JUAN	CRUZ	123 ABC ST. BRGY. BEL AIR MAKATI CITY METRO MANILA PHILIPPINES	608	1380300000	19500101	1380300000	608	ID1	P123456789	SF1

- **Subject Party Data: Other Parties: Insured**

AD	AE	AF	AG	AH	AI	AJ	AK	AL	AM
I		N	DELA CRUZ	MARIA	CRUZ	123 ABC ST. BRGY. BEL AIR MAKATI CITY METRO MANILA PHILIPPINES	608	1380300000	20110523

BO INFORMATION REPORTING TEMPLATE

Version 1 | Updated 15 June 2023

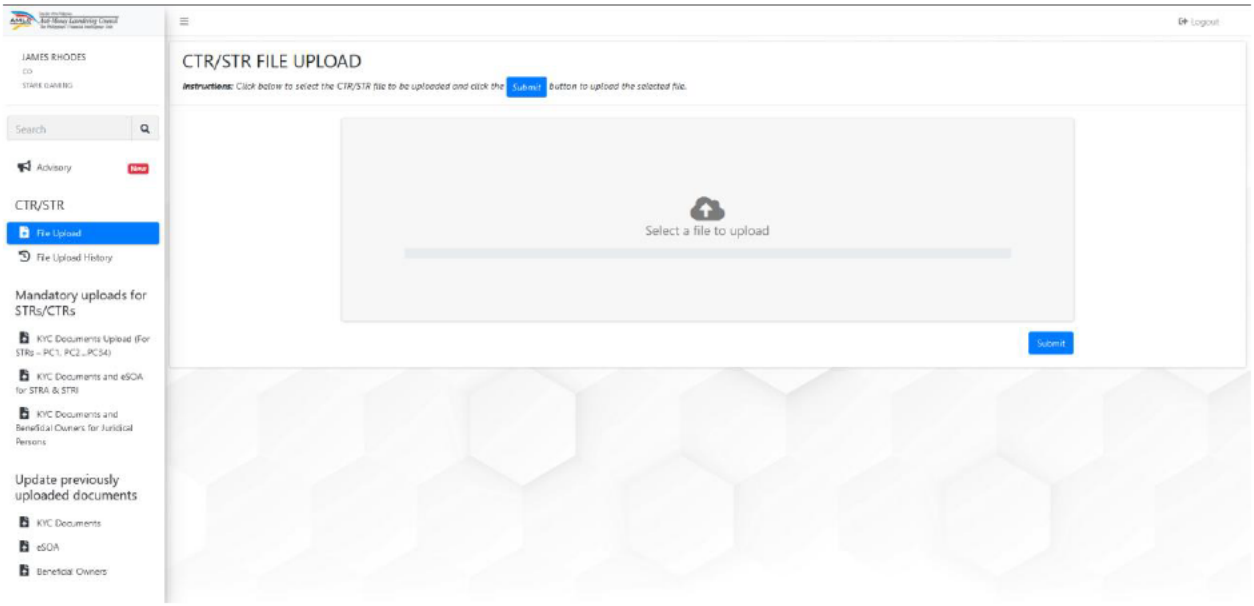
Information on Legal Person Accountholder						
Customer Reference Number of Legal Person Accountholder	SEC Registration Number	GIS Year	Source of Information	Other Source of Information	Registered Name	Registered Name of Associated Legal Entity (For Indirect BO)
Mandatory	*Mandatory*	*Mandatory if Source = 1*	*Mandatory*	*Mandatory if Source = 3*	*Mandatory*	*Optional*

Beneficial Ownership (BO) Information											
First Name	*Middle Name*	*Family Name*	Residential or Corporate Address of BO	Nationality	Date of Birth (mmddyyyy)	Tax Identification or Passport Number/Country of Origin	Position	Ownership Percentage	Voting Rights (Yes/No)	Type of BO (Direct/Indirect)	Category
Mandatory	*Optional*	*Mandatory*	*Mandatory*	*Mandatory*	*Optional*	*Mandatory if Source of Information = 1*	*Optional*	*Mandatory if Category = 1*	*Optional*	*Mandatory*	*Mandatory*

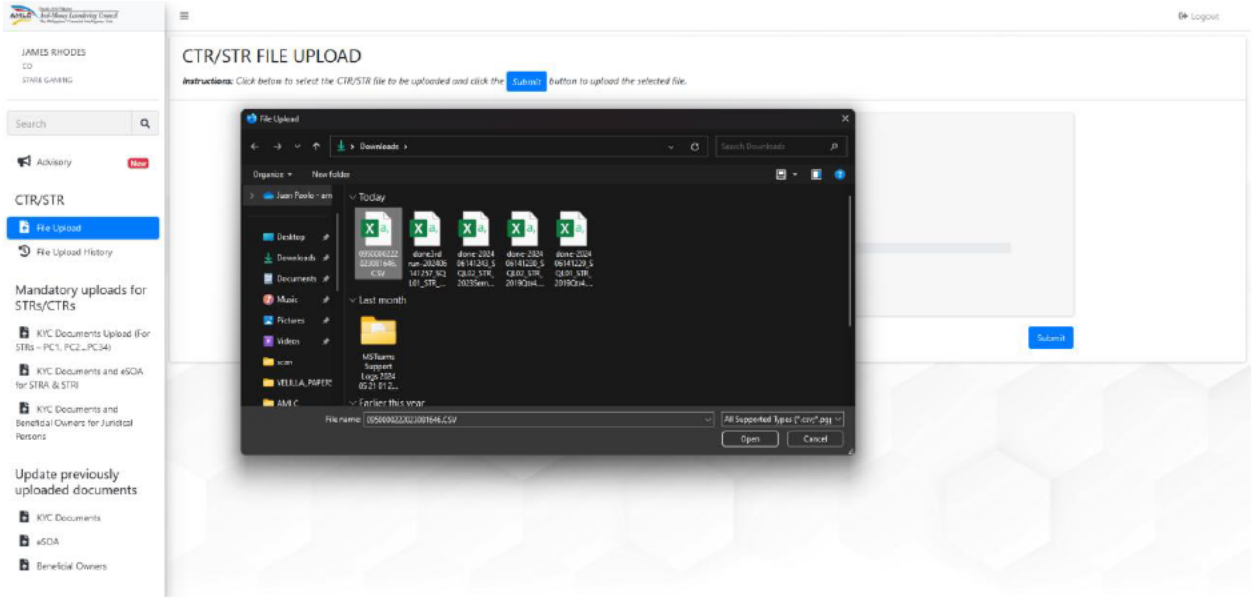
Uploading of CTR/STR, STR Attachment, KYC Documents, ESOA, and Beneficial Ownership Template

A. CTR/STR File Upload

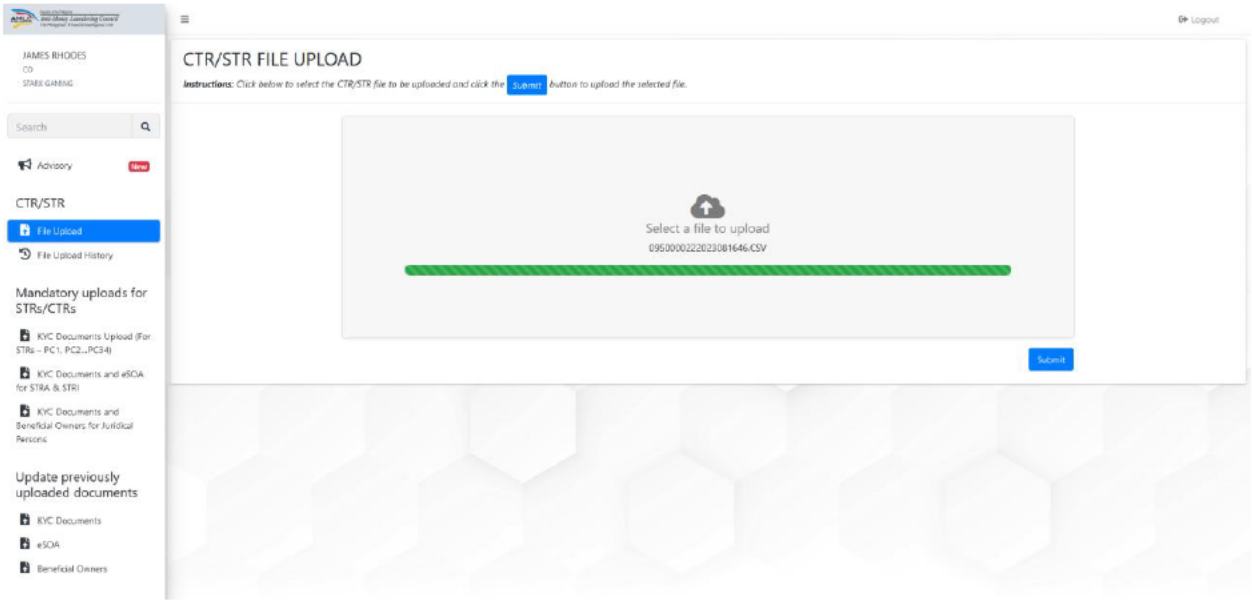
1. From the menu on the left, choose file upload then click select a file to upload in the CTR/STR File Upload screen.



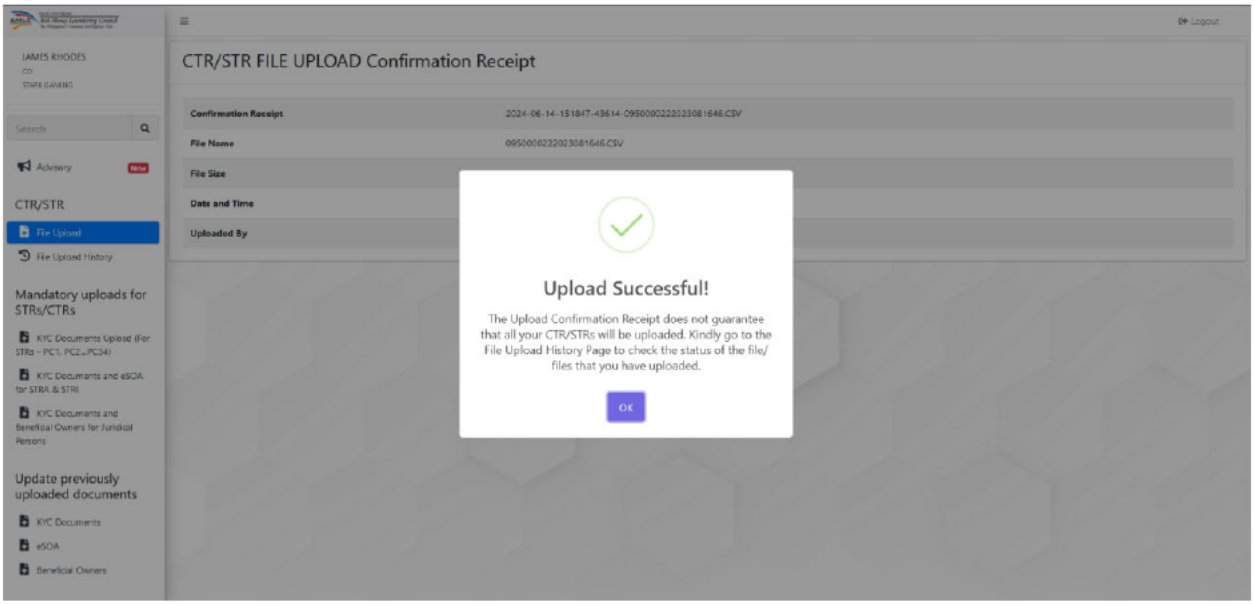
2. Browse the file.



3. Click submit to upload the file.



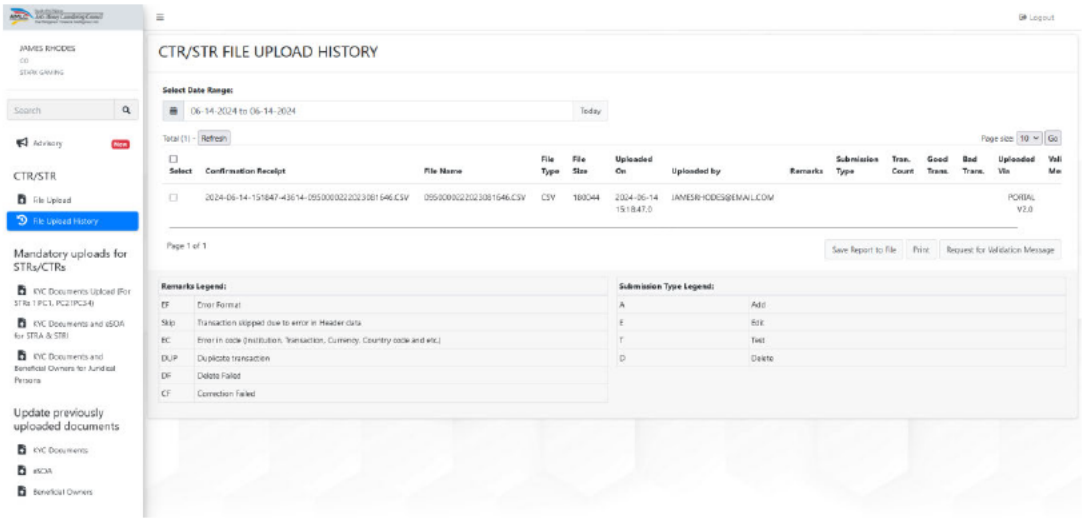
4. A confirmation will appear that upload was successful.



Note: The Upload Confirmation Receipt does not guarantee that all CTRs/STRs in the CSV file/s have been uploaded. To check if all files/CTR have been accepted by the system (without format errors), files should be viewed in the File Upload History P

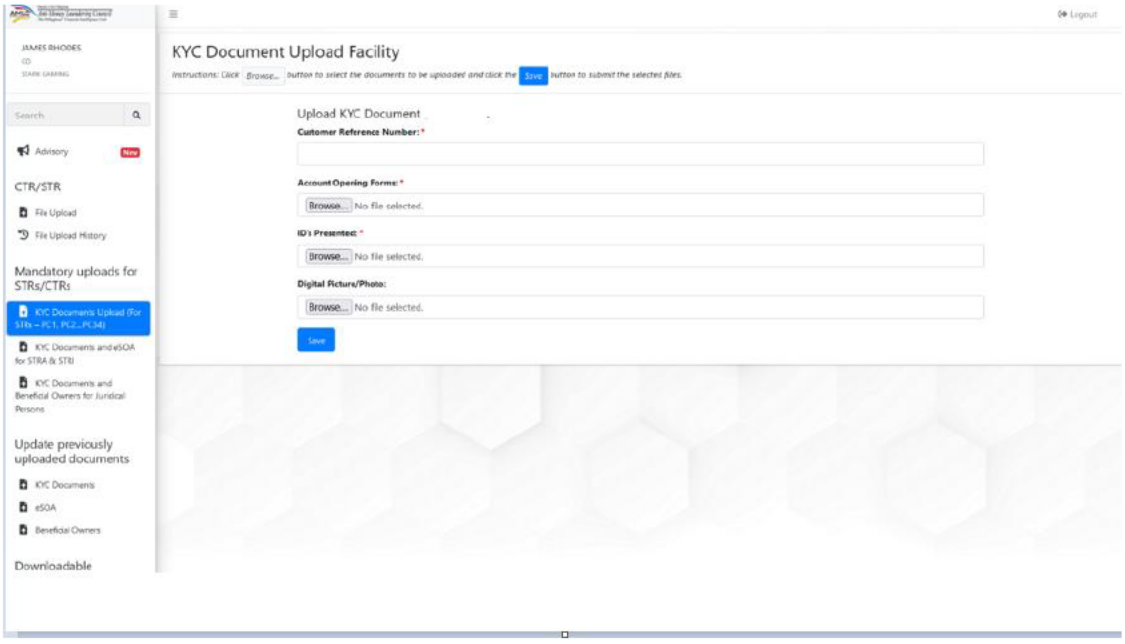
File Upload History

From the menu on the left, choose File Upload History, to view the history of the uploaded files.

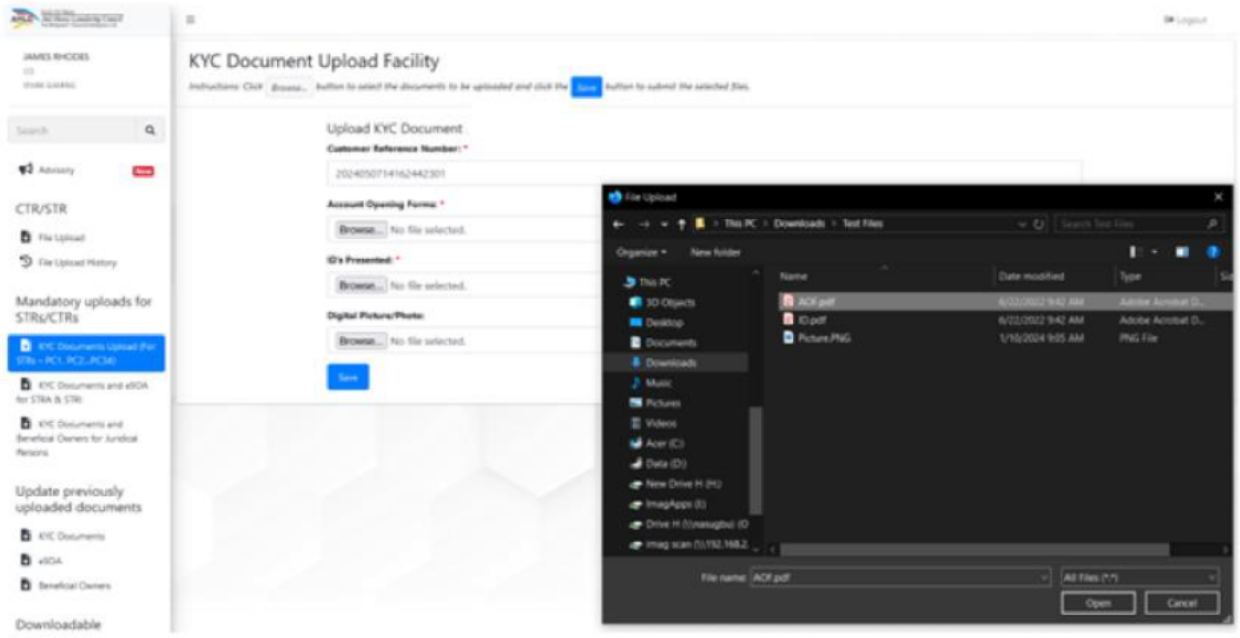


B. KYC Documents Upload

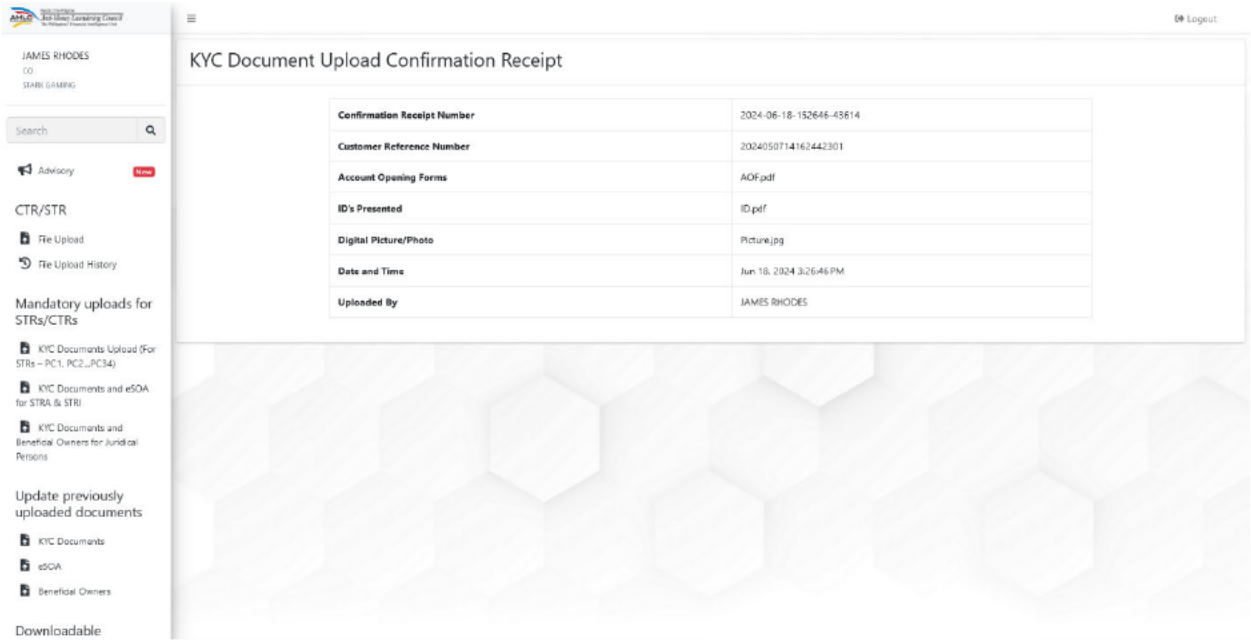
1. From the menu on the left, choose KYC Documents Upload for STRs – PC1, PC2...PC34). On the KYC Docs Upload Facility, enter the Customer Reference Number (CRN) of the of the account holder/customer or party name, this should be the same CRN for the STR to be filed.



2. Browse the file to be uploaded in each field then click Save button.



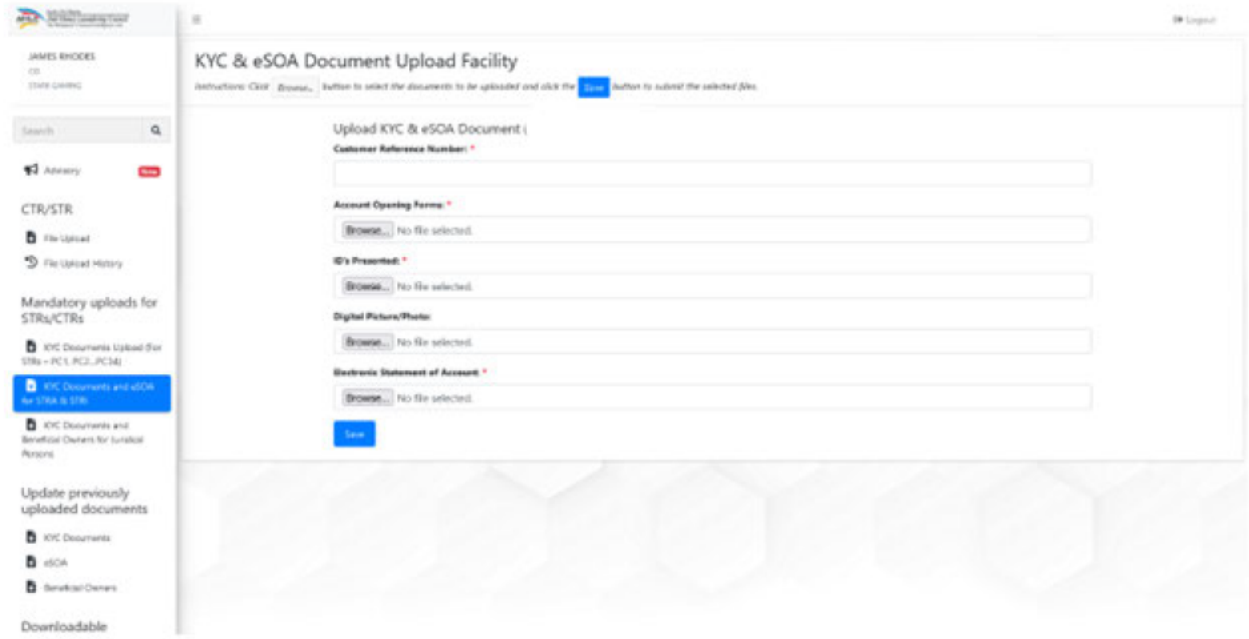
3. A confirmation receipt will be displayed after a successful upload.



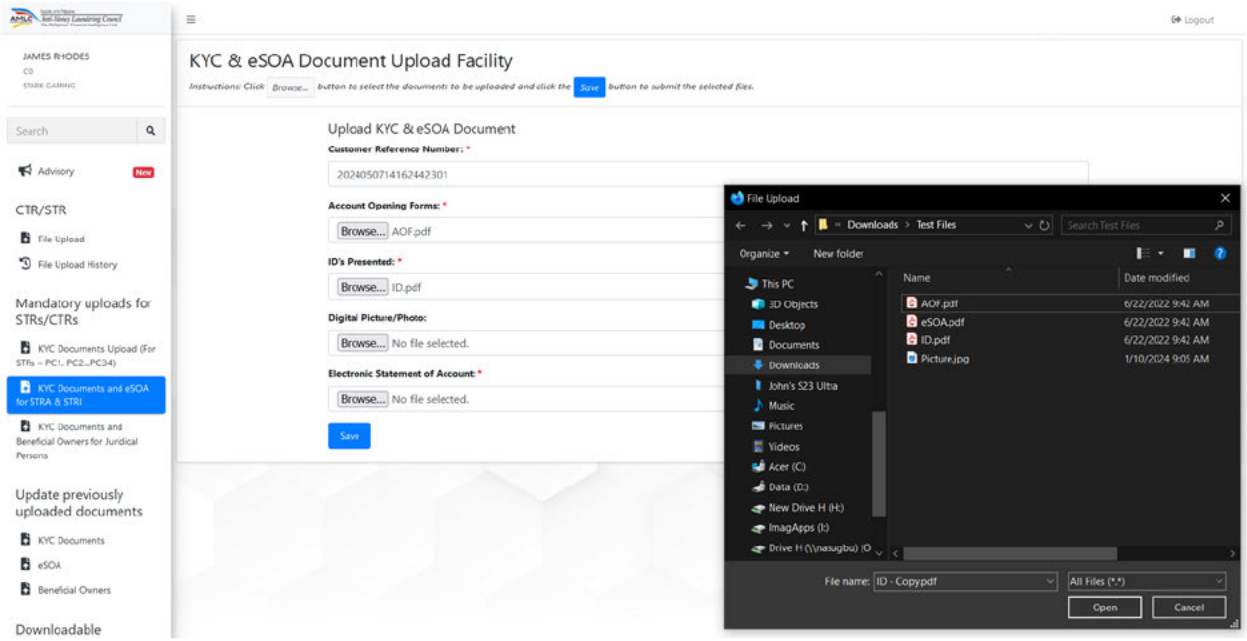
4. Please proceed to the uploading of the corresponding STR.

C. KYC Documents & ESOA Document Upload (For STRA)

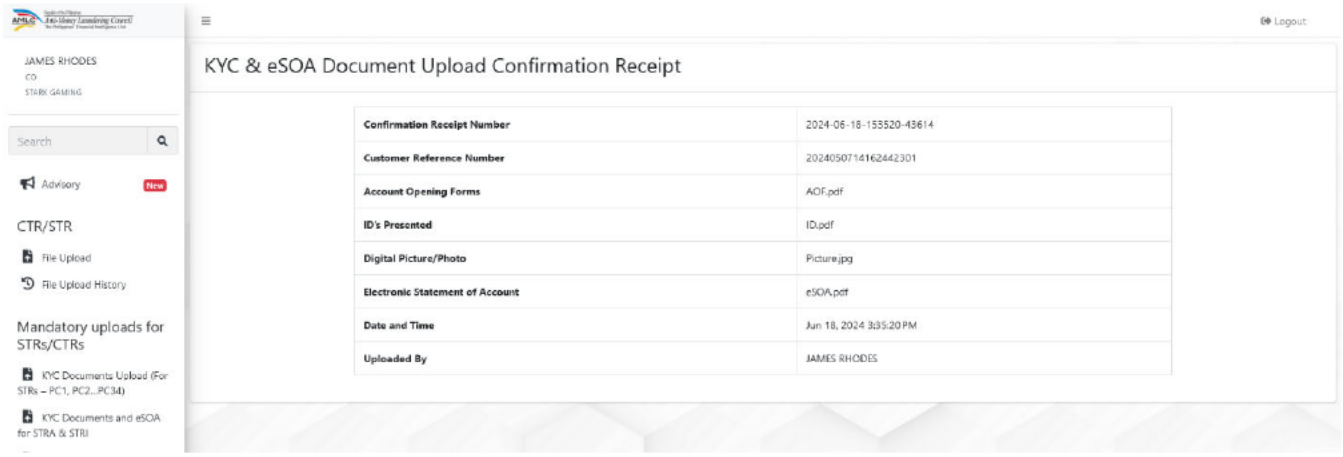
1. From the menu on the left, choose KYC Documents and ESOA for STRA. On the KYC and ESOA Upload Facility, enter the CRN of the of the account holder/customer or party name, this should be the same CRN for the STR to be filed.



2. Browse the file to be uploaded in each field then click Save button.



3. A confirmation receipt will be displayed after a successful upload.

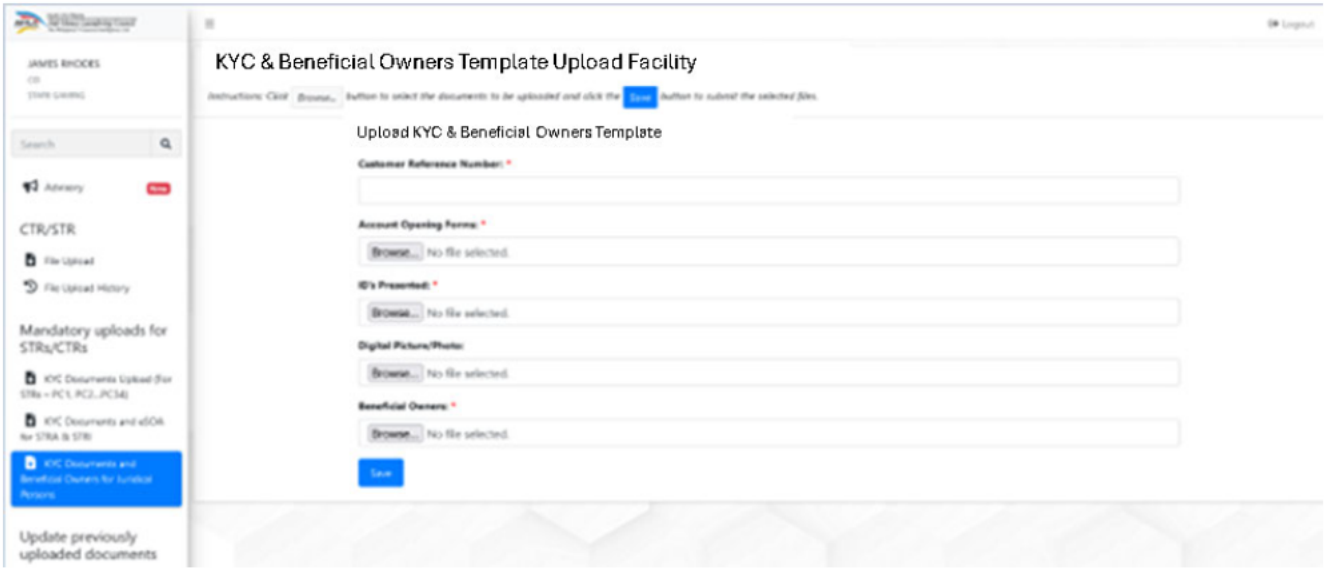


4. Please proceed with the uploading of the corresponding STR.

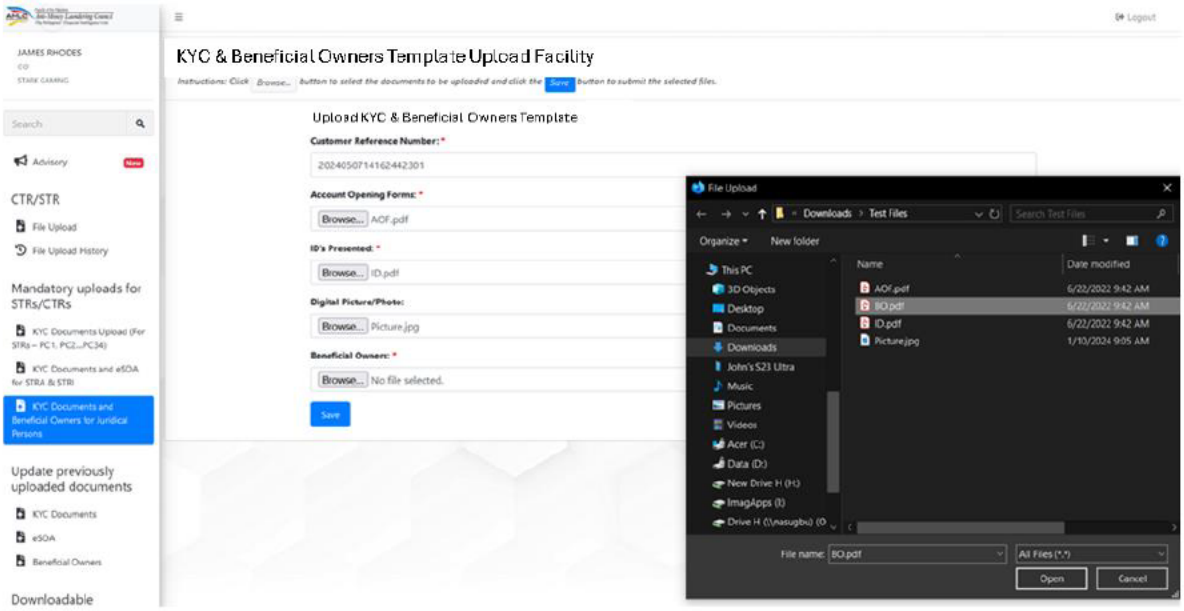
D. KYC Documents & Beneficial Owners Document Upload

1. From the menu on the left, choose Downloadable Electronic Forms – Beneficial Owner (BO) template to download a copy of the BO Template. Properly fill-up the BO template to be uploaded in the succeeding steps.

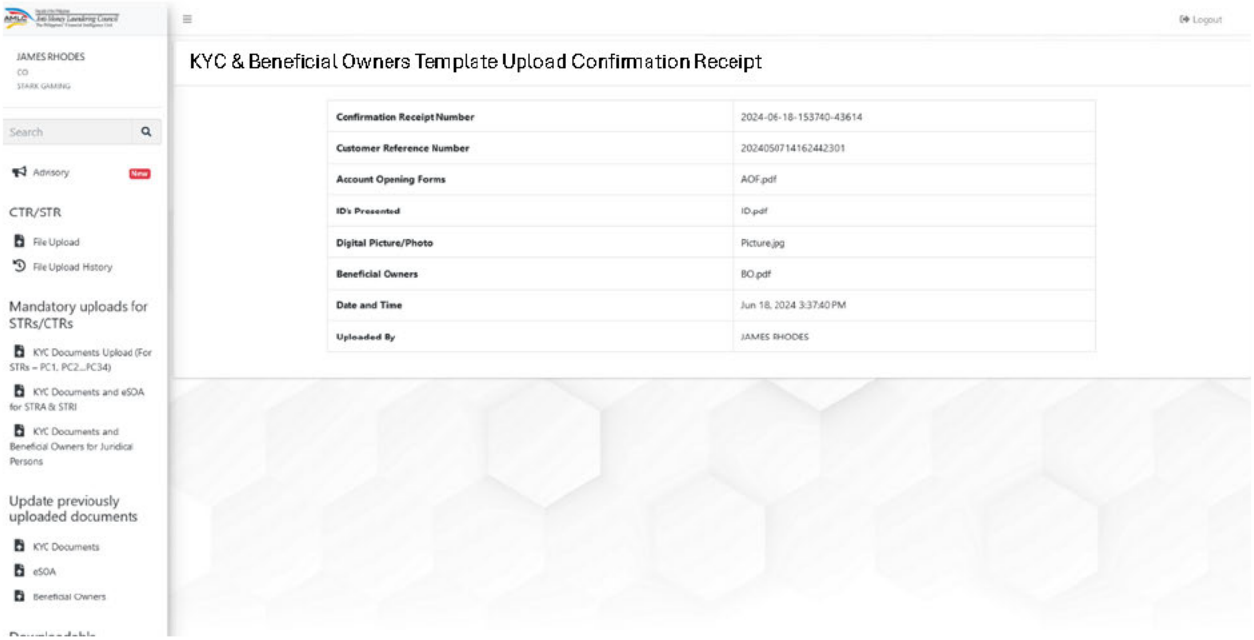
2. From the menu on the left, choose KYC Documents and Beneficial Owners for Juridical Persons. On the KYC and BO Document Facility, enter the CRN of the of the account holder/customer or party name, this should be the same CRN for the STR to be filed.



3. Browse the file to be uploaded in each field then click Save button.



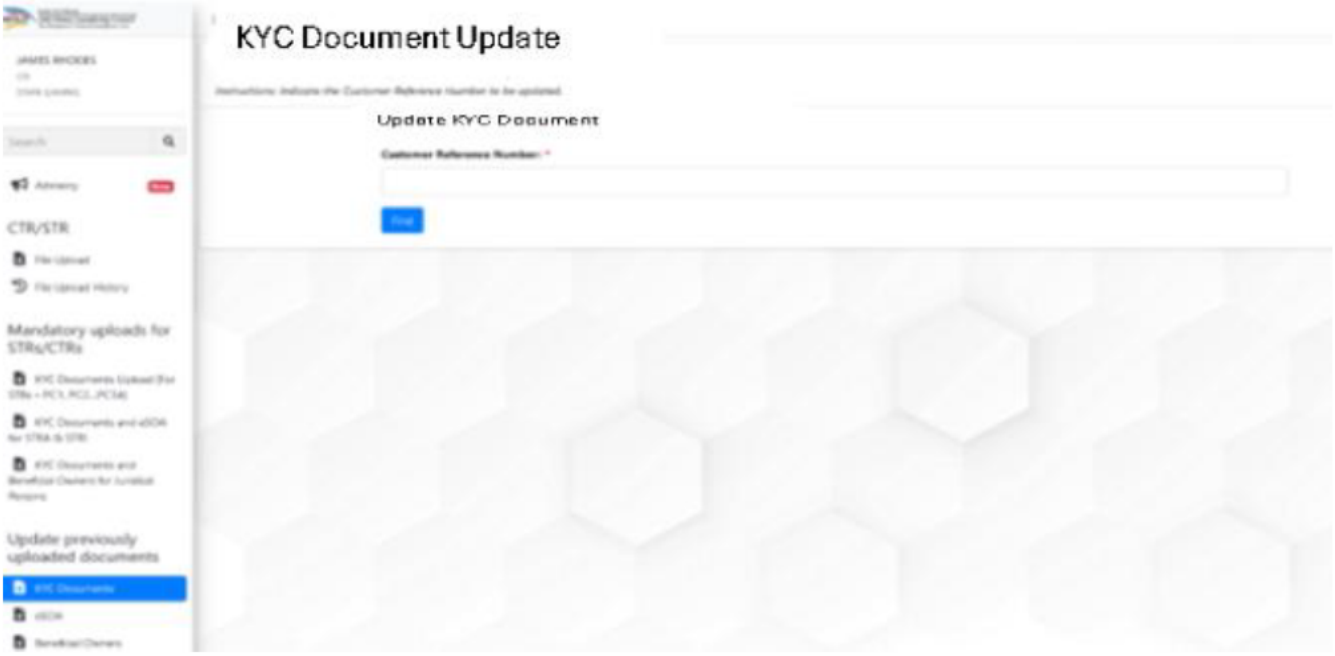
4. A confirmation receipt will be displayed after a successful upload.



5. Please proceed with the uploading of the corresponding CTR/STR.

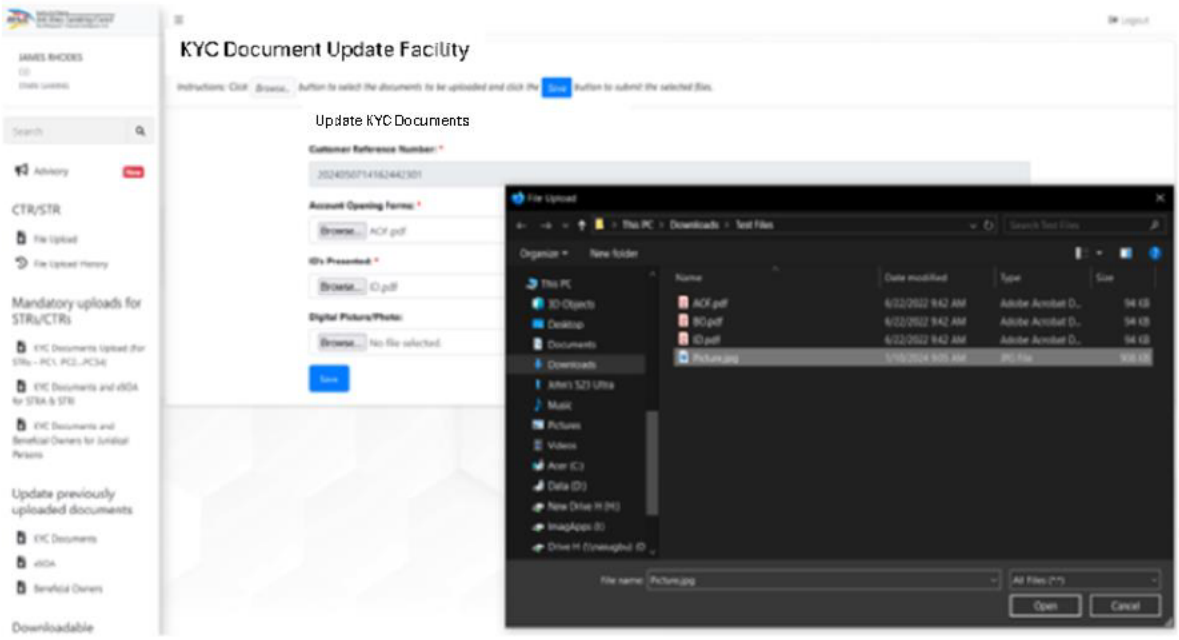
E. KYC Documents Update

1. From the menu on the left, choose Update previously uploaded documents – KYC Docs, enter the CRN and click the Find button.

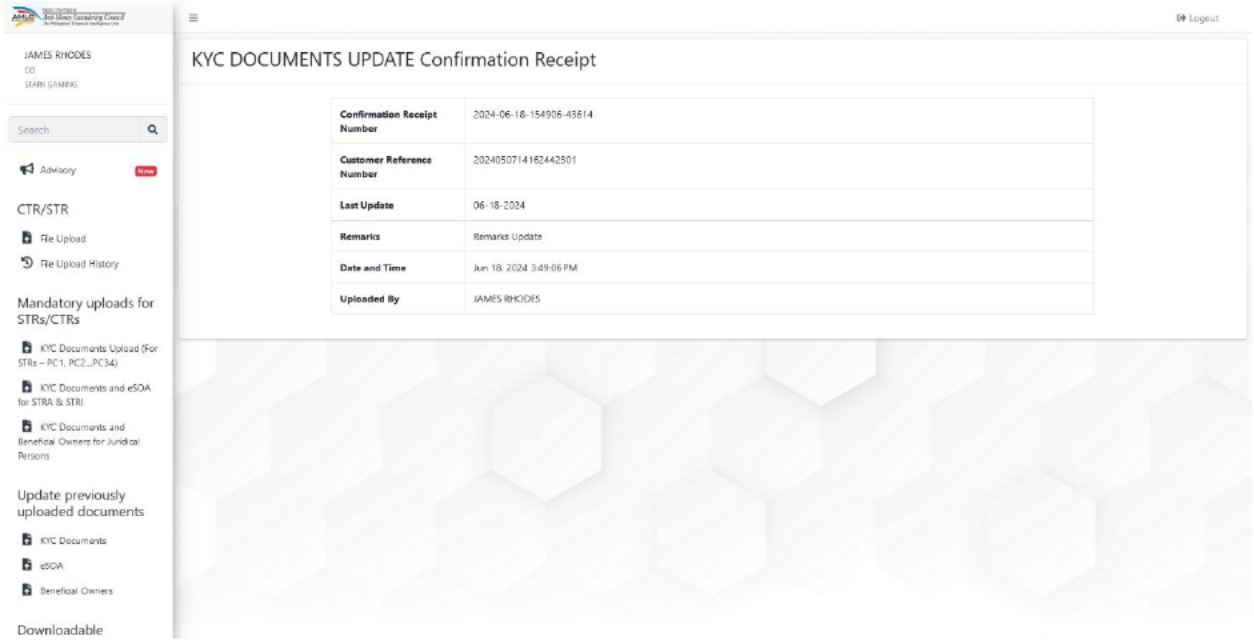


2. If there is no update, enter the reason in the Remarks portion and click Update. Otherwise leave the Remarks portion blank and click the Upload New button to update previously uploaded KYC Docs.

3. When updating new files, browse the file to be uploaded in each field then click Save button.

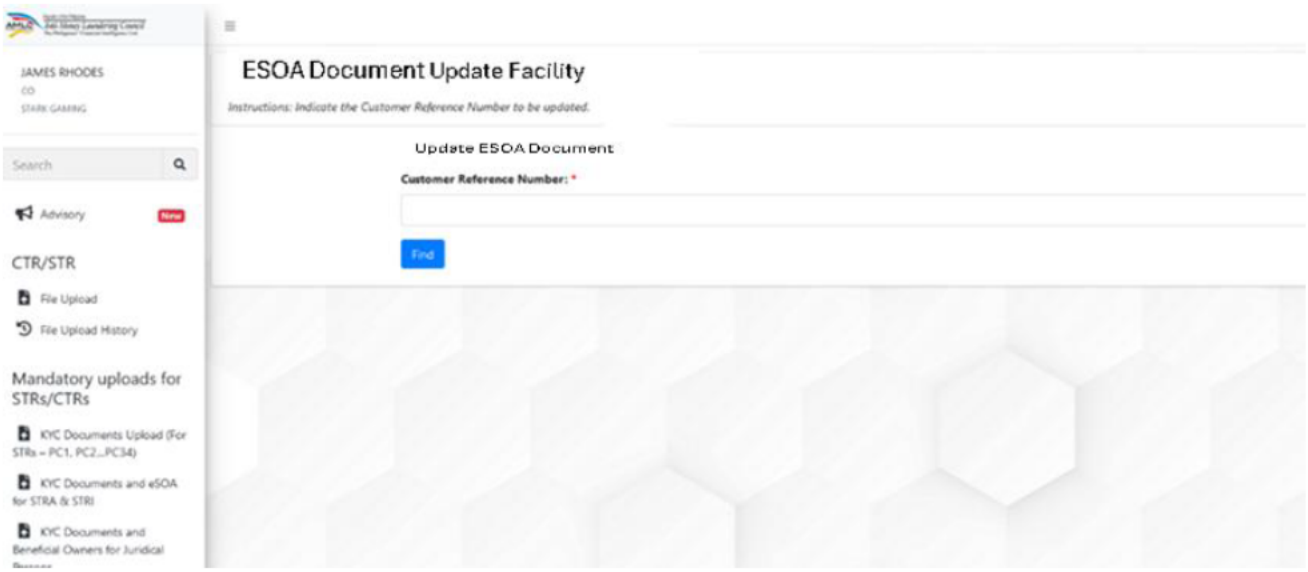


4. A confirmation receipt will be displayed after a successful update

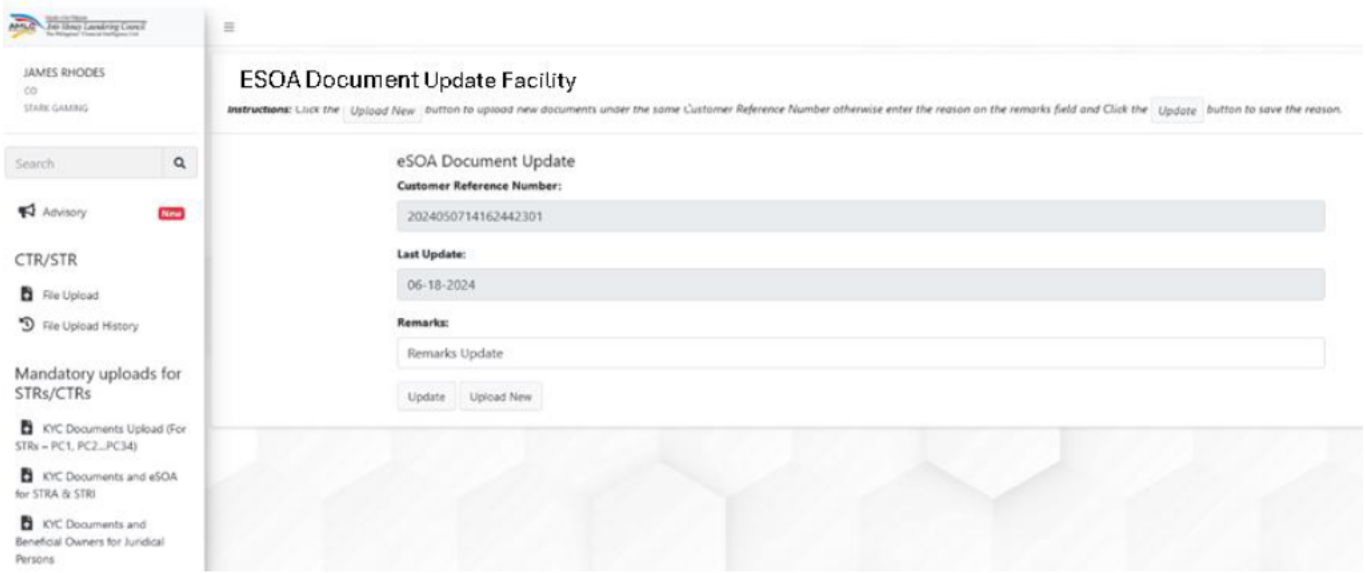


F. ESOA Update

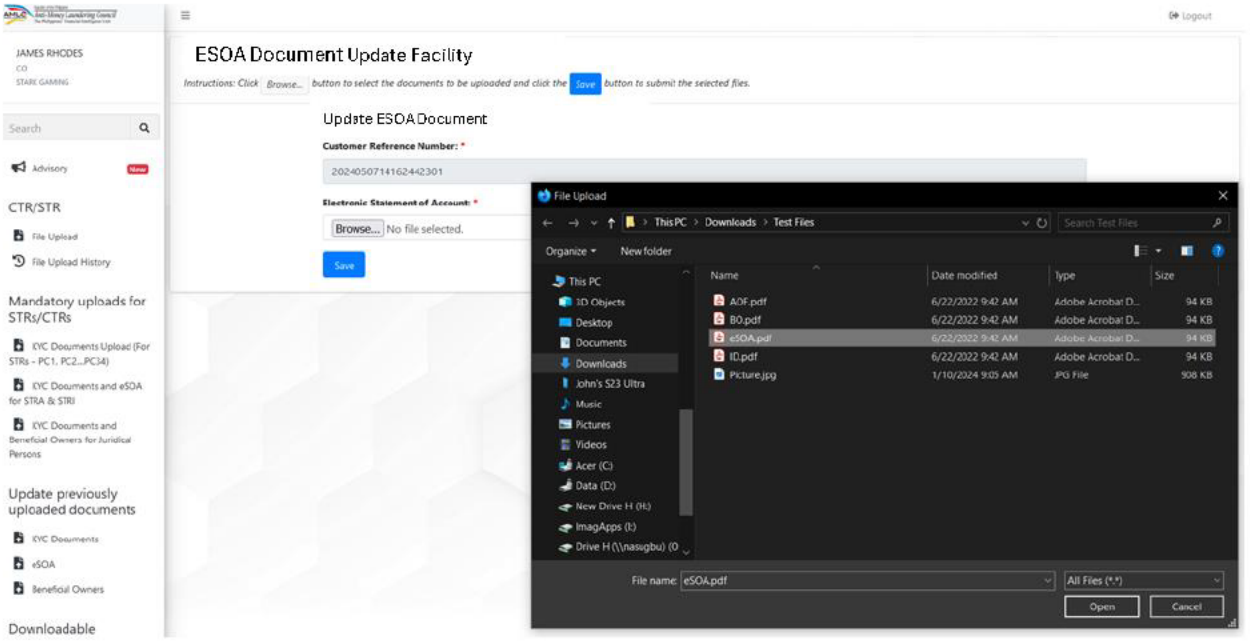
1. From the menu on the left, choose Update previously uploaded documents – ESOA, enter the CRN and click the Find button.



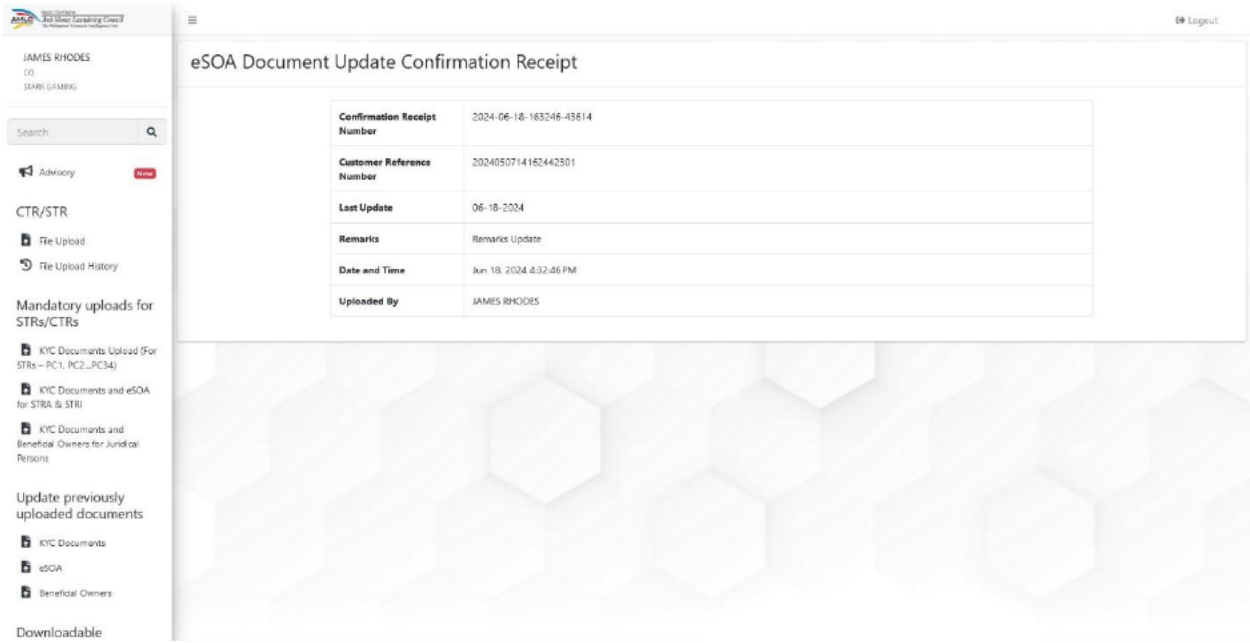
2. If there is no update, enter the reason in the Remarks portion and click Update. Otherwise leave the Remarks portion blank and click the Upload New button to update previously uploaded ESOA.



3. When updating new files, Browse the file to be uploaded in each field then click Save button.

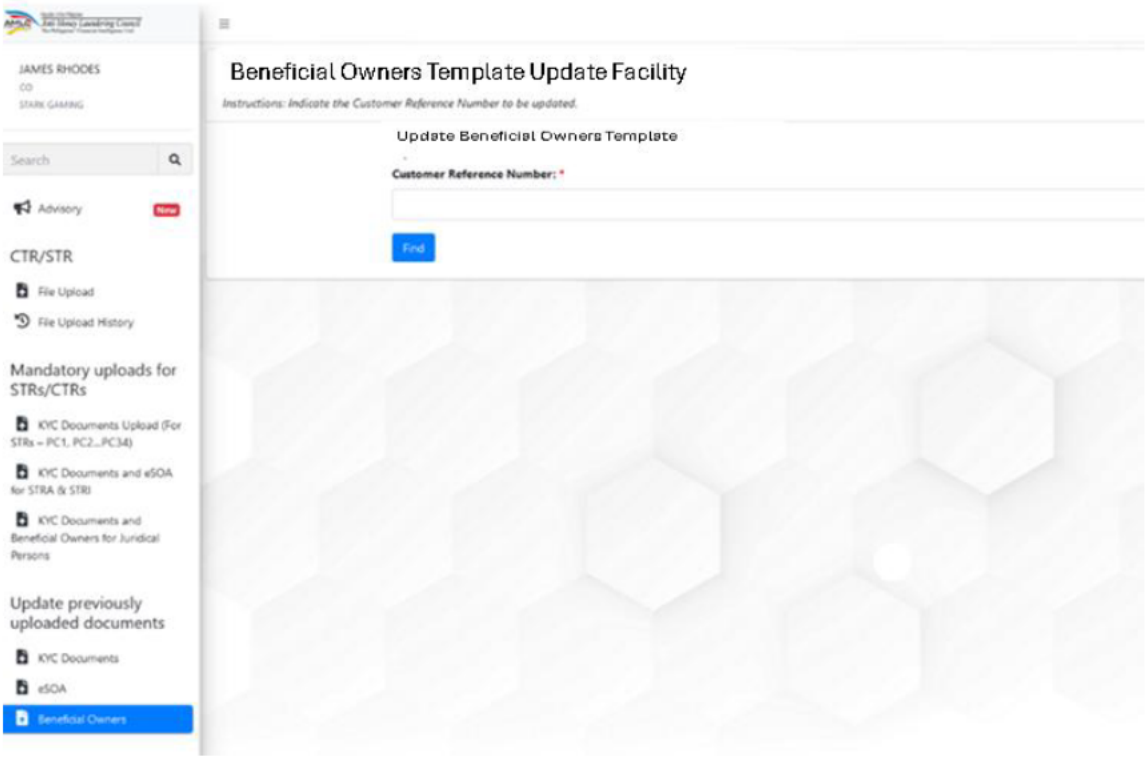


4. A confirmation receipt will be displayed after a successful update.

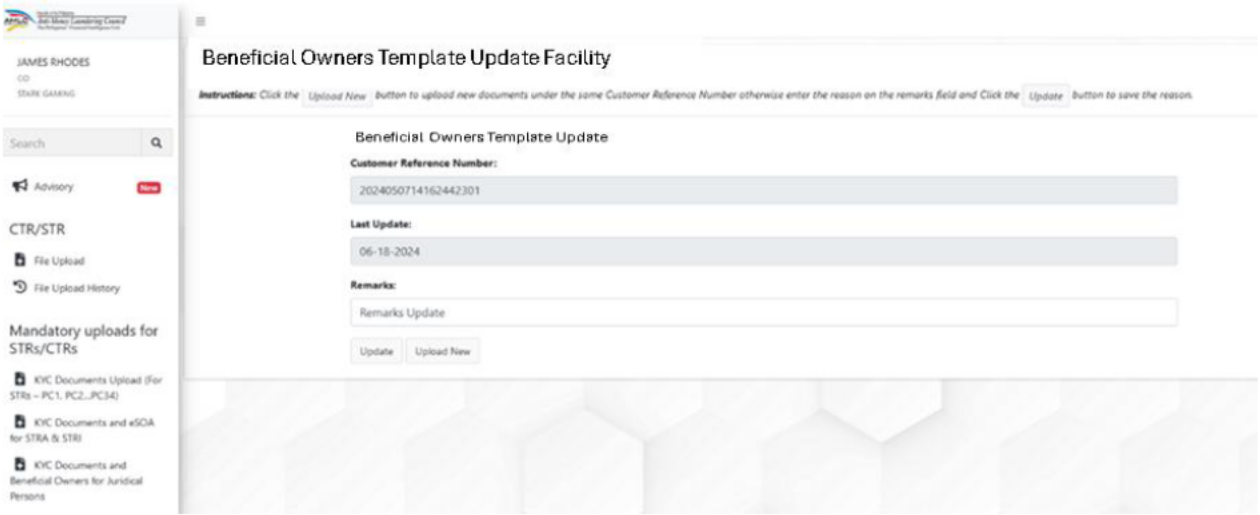


G. Beneficial Owners Update

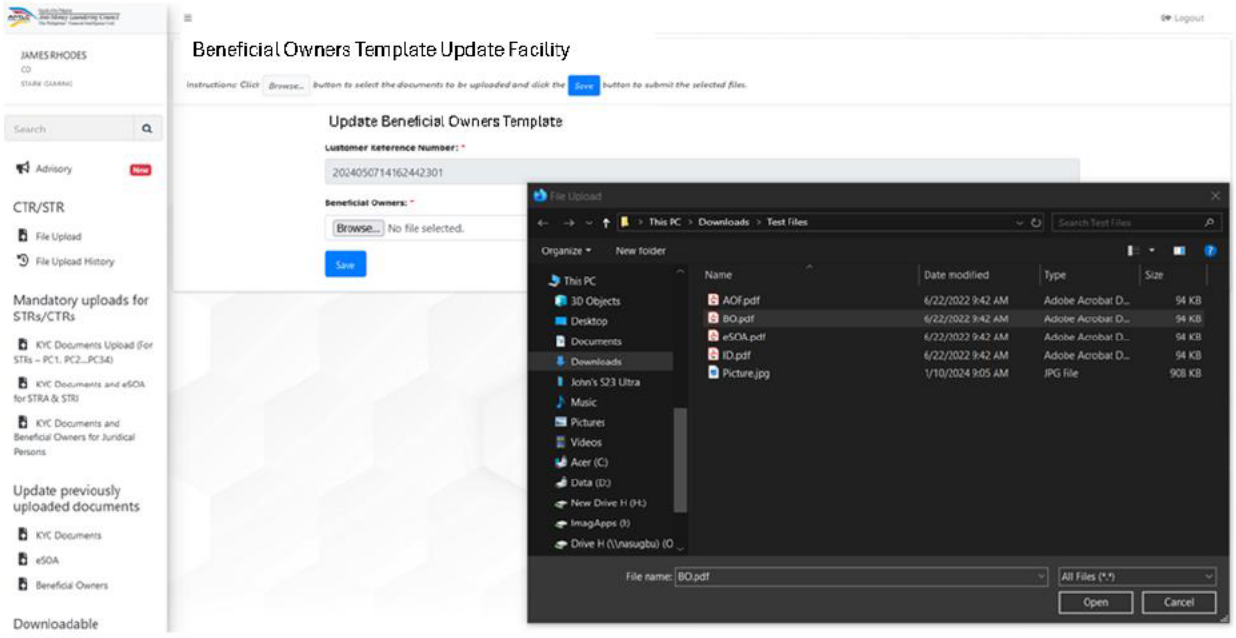
1. From the menu on the left, choose Update previously uploaded documents – Beneficial Owners, enter the CRN and click the Find button.



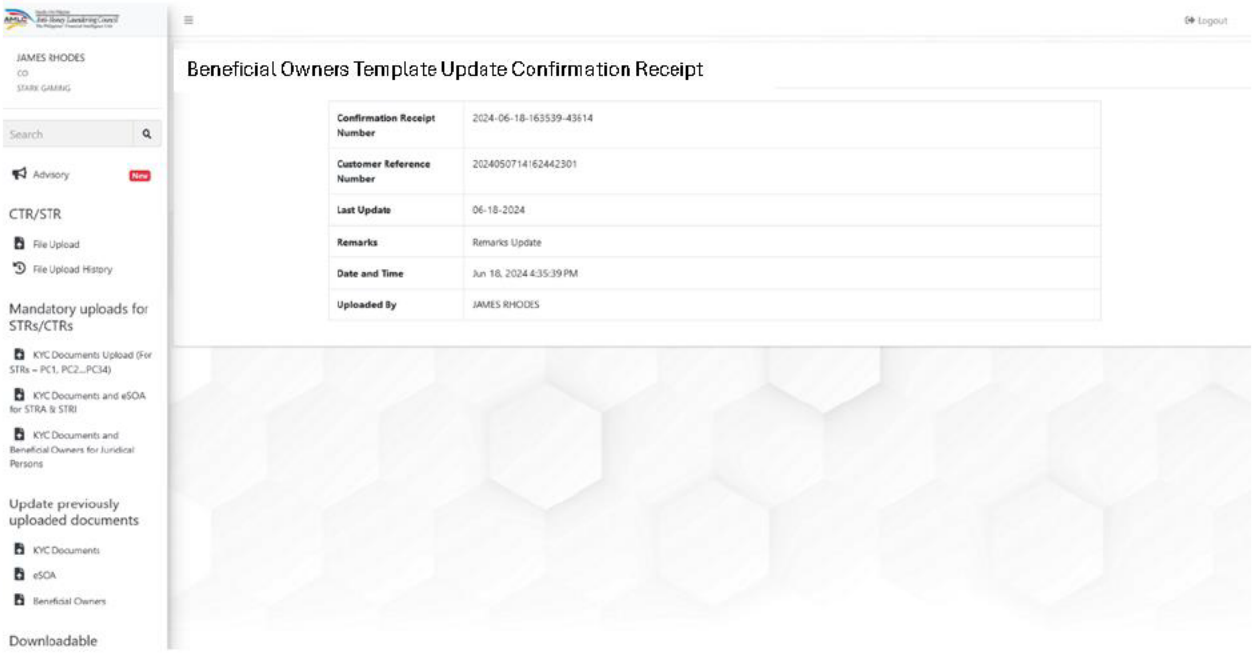
2. If there is no update, enter the reason in the Remarks portion and click Update. Otherwise leave the Remarks portion blank and click the Upload New button to update previously uploaded Beneficial Owners template.



3. When updating new files, Browse the file to be uploaded in each field.

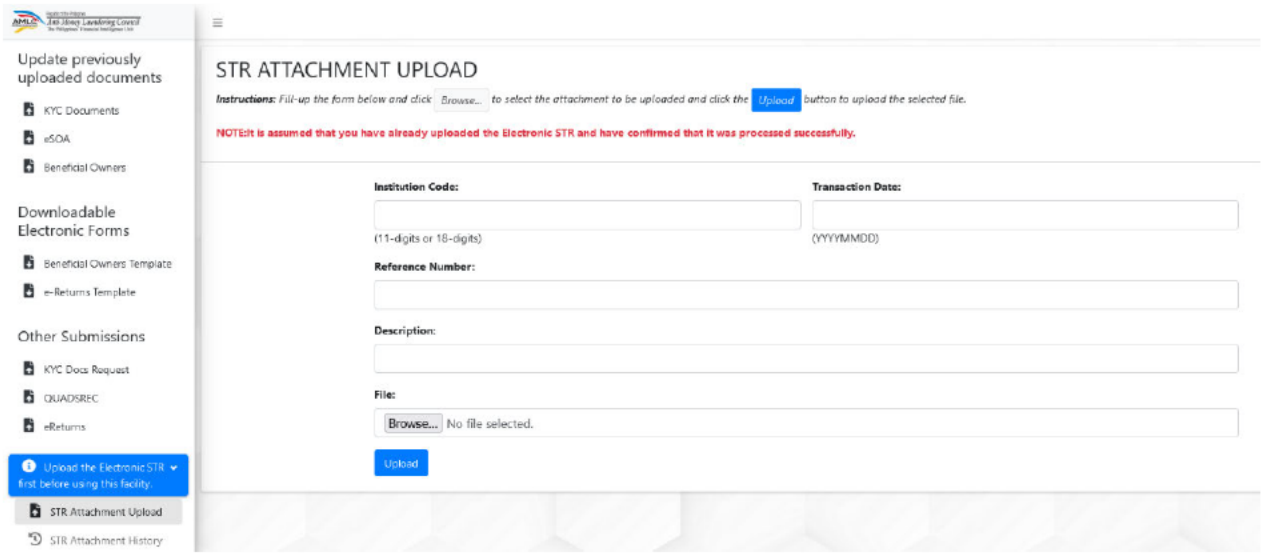


4. A confirmation receipt will be displayed after a successful update.

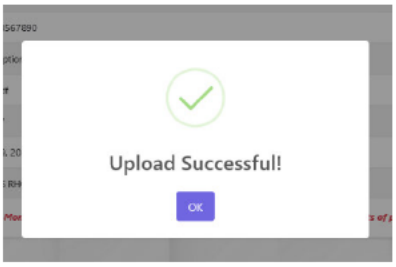


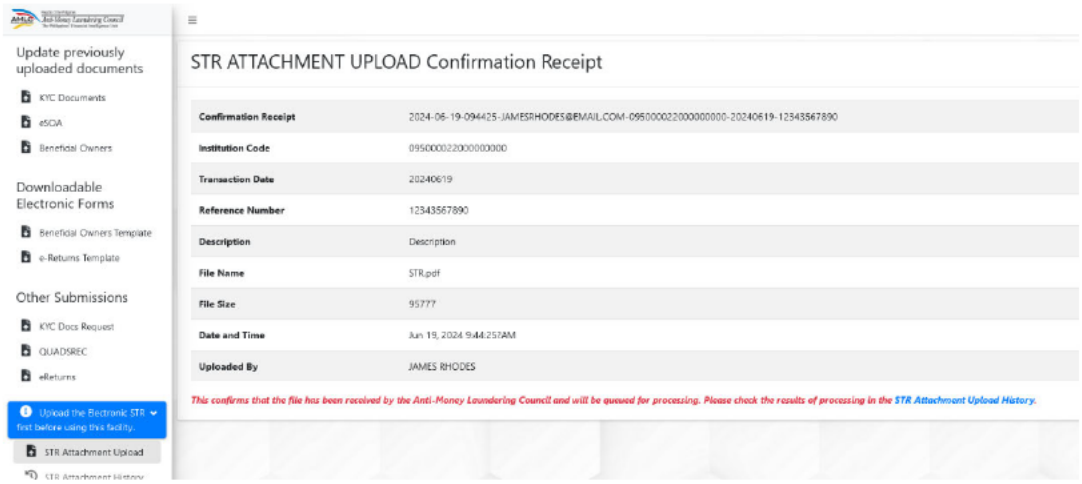
H. STR Attachment Upload

1. From the menu on the left, choose STR Attachment upload, enter the Institution code, transaction date, reference number, description, and browse the file to be uploaded then click Upload button to proceed.



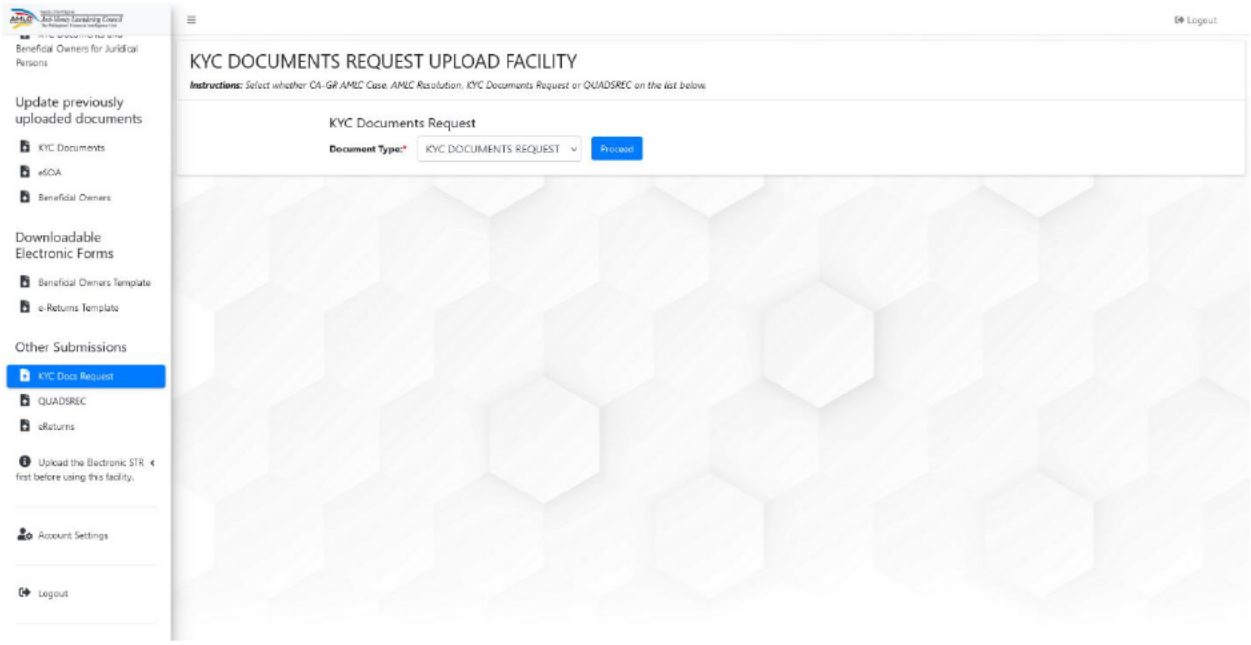
2. A confirmation receipt will be displayed after a successful upload.



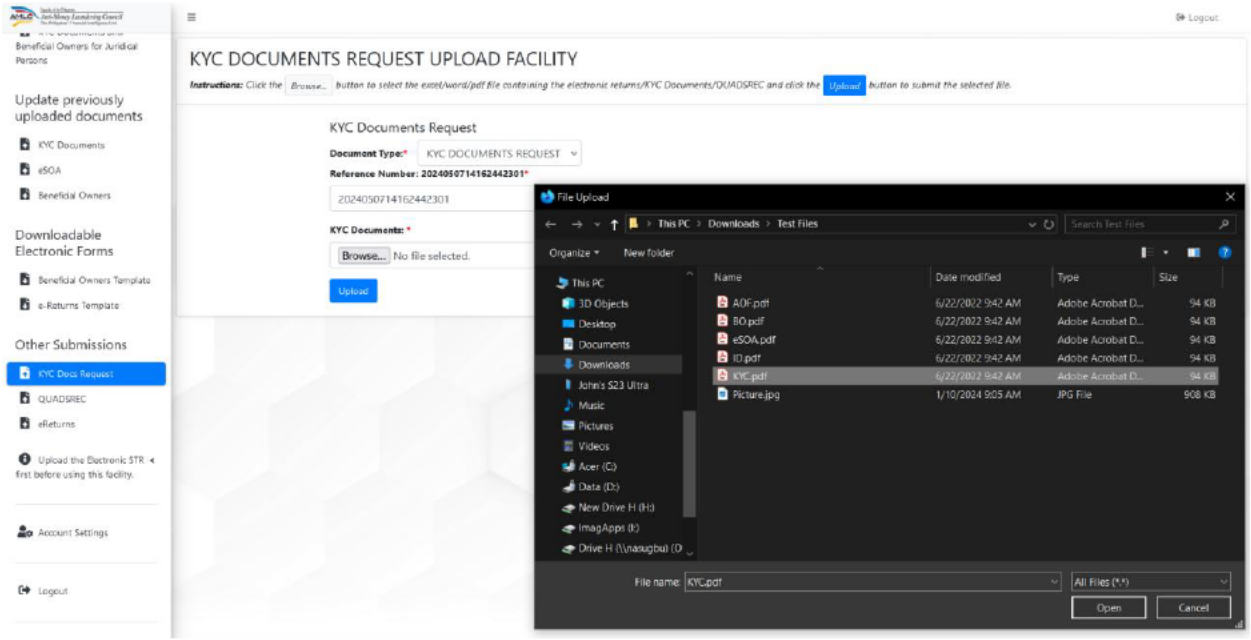


KYC Documents upload as requested by the AMLC (AMLC REFERRALS)

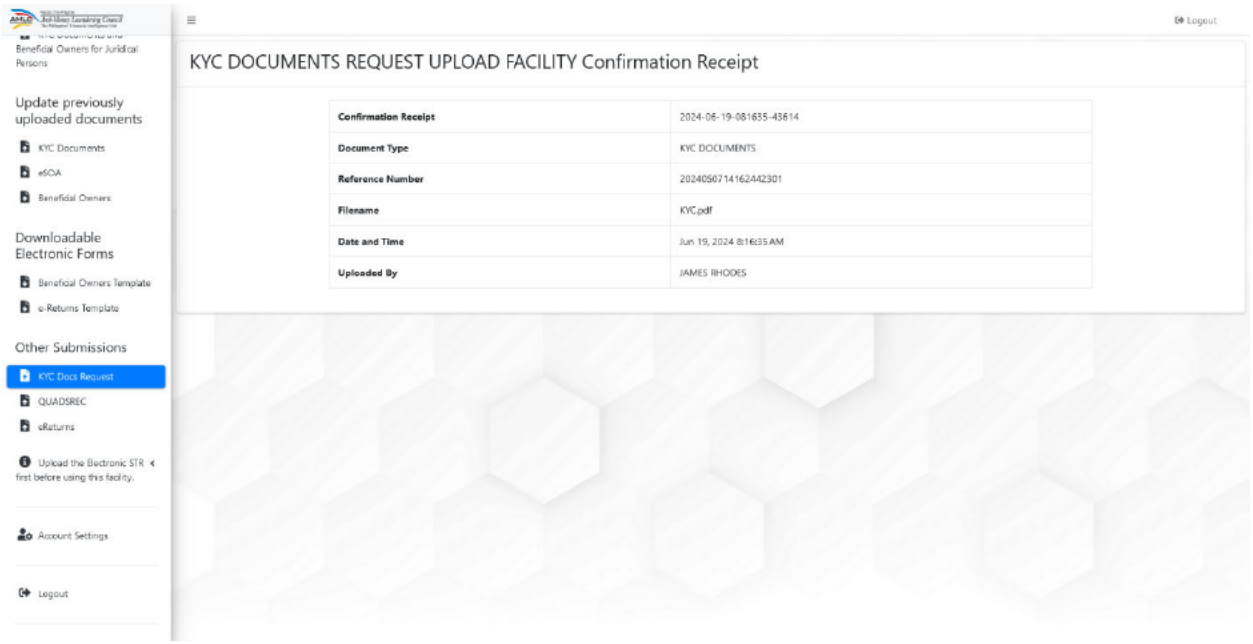
1. From the menu on the left, choose Other Submissions - KYC Docs Request and click the proceed button to display the form.



2. Enter the Reference number then browse the KYC file to be uploaded then click Upload button to proceed.



3. A confirmation receipt will be displayed after a successful upload.



STR Timelines

AMLC Referral

Day 0
AMLC referral

Day 1
At any time, Submission of
STRA
(next **working** day after AMLC referral)

*Mandatory Uploading of ESOA & KYC

Targeted Financial Sanctions

Day 0
At any time, Submission of
STRR
With Trigger Code: "G"
To be filed on the day of determination as Targeted Financial Sanction subject/ Freeze Order was implemented

*Mandatory Uploading of KYC

Highly Unusual Suspicious Transaction – not under High Priority Unlawful Activity for PC13, PC14, PC19, PC31

Day 0
Occurrence of Suspicious Transaction / Suspicious Circumstance / Unlawful Activity

Day 1
Submission of
STRHU
(next **working** day)

STR Timelines

Related to Unlawful Activity (except if PC13, PC14, PC19, PC31)

Day 0
Occurrence of Suspicious Transaction / Suspicious Circumstance / Unlawful Activity

Day 1
CP investigation

Day 11 **(10 calendar days after)**
Submission of
STRI or STRR

Day 71 **(60 calendar days after)**
Submission of
STRF

*Requires initial STRI
*Mandatory Uploading of ESOA & KYC if STRI

Related to Unlawful Activity (High Priority Unlawful Activity for PC13, PC14, PC19, PC31)

Day 0
Occurrence of Suspicious Transaction / Suspicious Circumstance / Unlawful Activity

Day 1
Submission of
STRHP
(next **working** day)

*Mandatory Uploading of KYC

STR Timelines

Suspicious Circumstance enumerated under Section 3 (b-1) of AMLA and Rule 3.a.15 of IRR of TFPSA

- **Day 0**
  Occurrence of Suspicious Transaction / Suspicious Circumstance enumerated under Section 3 (b-1) of AMLA and Rule 3.a.15 of IRR of TFPSA
- **Day 1**
  CP investigation
- **Day 11** **(10 calendar days after)**
  Submission of **STRR**

TMS Generated Alerts

- **Day 0**
  Extraction Day of TMS Generated Alert/s
- **Day 61** **(60 calendar days after)**
  Submission of **STRR**

Suspicious Indicators/Red Flags and Typologies

I. Suspicious Indicators/Red Flags (General)

A. Identity Documents

1. Customer refuses or fails to provide registration document issued by authorities, such as pertinent business papers and certificate of registration issued by the Bangko Sentral ng Pilipinas and the AMLC.
2. Identification presented seems very recent.
3. Identification documents present are only copies of the originals.
4. Identification documents presented differ for every transaction.
5. Customer usually provides reasons for not present the required identification documents.
6. Identification document presented cannot be verified, e.g. issued by foreign jurisdictions.
7. Identification documents lack important details, such as telephone numbers

B. Areas of Suspicion:[2]

1. Customer admits to or makes statements about involvement in criminal activities.
2. You are aware that a customer is the subject of a criminal investigation.
3. Customer does not want correspondence sent to residential address.
4. Customer appears to have accounts with several financial institutions in one area for no apparent reason.
5. Customer conducts transactions at different physical locations in an apparent attempt to avoid detection.
6. Customer repeatedly uses an address but frequently changes the names involved.
7. Customer is accompanied and watched.
8. Significant and/or frequent transactions in contrast to known or expected business activity(ies).
9. Significant and/or frequent transactions in contrast to known employment status.
10. Ambiguous or inconsistent explanations as to the source and/or purpose of funds.
11. Where relevant, money presented in unusual condition, for example, damp, odorous, or coated with substance.

[2] ADB's Handbook on Anti-Money Laundering and Combating the financing of Terrorism for Nonbank Financial Institutions

12. Where relevant, nervous or uncooperative behavior exhibited by employees and/or customers.
13. Customer shows uncommon curiosity about internal systems, controls, and policies.
14. Customer has only vague knowledge of the amount of a deposit.
15. Customer presents confusing details about the transaction or knows few details about its purpose.
16. Customer over-justifies or -explains the transaction.
17. Customer is secretive and reluctant to meet in person.
18. Customer is nervous, not in keeping with the transaction.
19. Customer is involved in transactions that are suspicious but seems blind to being involved in money-laundering activities.
20. Customer's home or business telephone number has been disconnected, or there is no such number when an attempt is made to contact the customer shortly after opening the account.
21. Customer appears to be acting on behalf of a third party but does not inform the credit institution staff.
22. Customer insists that a transaction be done quickly.
23. Inconsistencies appear in the customer's presentation of the transaction.
24. Customer attempts to develop close rapport with the staff.
25. Customer uses aliases and a variety of similar but different addresses.
26. Customer spells his or her name differently from one transaction to another.
27. A new or prospective customer is known as having a questionable legal reputation or criminal background.
28. Transaction involves a suspected shell entity (i.e., a corporation that has no assets, operations, or other reasons to exist)

C. Behavioral Red Flags: [3]

1. A third party speaks on behalf of the customer (a third party may insist on being present and/ or translating).
2. A third party insists on being present for every aspect of the transaction. A third party attempts to fill out paperwork without consulting the customer.
3. A third party maintains possession and/or control of all documents or money.
4. A third party claims to be related to the customer but does not know critical details.
5. A prospective customer uses, or attempts to use, third-party identification (of someone who is not present) to open an account.
6. A third party attempts to open an account for an unqualified minor.
7. A third party commits acts of physical aggression or intimidation toward the customer.

[3] See FINCEN Advisory, FIN-2020-A008, "Supplemental Advisory on Identifying and Reporting Human Trafficking and Related Activity," (October 15, 2020). (https://www.fincen.gov/sites/default/files/advisory/2020-10-15/Advisory%20Human%20Trafficking%20508%20FINAL_0.

8. A customer shows signs of poor hygiene, malnourishment, fatigue, signs of physical and/or sexual abuse, physical restraint, confinement, or torture.
9. 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.

D. Financial Red Flags:[4]

1. Customers frequently appear to move through, and transact from, different geographic locations in the United States. These transactions can be combined with travel and transactions in and to foreign countries that are significant conduits for human trafficking.
2. 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.
3. 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.
4. A customer frequently makes cash deposits with no Automated Clearing House (ACH) payments.
5. An individual frequently purchases and uses prepaid access cards.
6. 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.
7. Frequent transactions with online classified sites that are based in foreign jurisdictions.
8. 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.
9. Frequent transactions using third-party payment processors that conceal the originators and/or beneficiaries of the transactions.
10. A customer avoids transactions that require identification documents or that trigger reporting requirements.

[4] See FINCEN Advisory, FIN-2020-A008, "Supplemental Advisory on Identifying and Reporting Human Trafficking and Related Activity," (October 15, 2020). (https://www.fincen.gov/sites/default/files/advisory/2020-10-15/Advisory%20Human%20Trafficking%20508%20FINAL_0.pdf)

E. Personal Transactions[5]

1. Customer appears to have accounts with several financial institutions in one geographic area.
2. Customer has no employment history but makes frequent, large transactions or maintains a large account balance.
3. The flow of income through the account does not match what was expected based on the stated occupation of the account holder or the intended use of the account.
4. Customer makes one or more cash deposits to the general account of a foreign correspondent bank (i.e., pass-through account).
5. Customer makes frequent or large payments through online payment services.
6. Customer runs large positive credit card balances.
7. Customer uses cash advances from a credit card account to purchase money orders or drafts or to wire funds to foreign destinations.
8. Customer takes cash advance to deposit into savings or checking account.
9. Large cash payments for outstanding credit card balances.
10. Customer makes credit card overpayment and then requests a cash advance. Customer visits the safety deposit box area immediately before making cash deposits.
11. Customer has numerous accounts and deposits cash into each of them with the total credits being a large amount.
12. Customer deposits large 2nd endorsed checks in the name of a third party.
13. Customer frequently makes deposits to the account of another individual who is not an employee or family member.
14. Customer frequently exchanges currencies.
15. Customer frequently makes automatic banking machine deposits just below the reporting threshold.
16. Customer's access of the safety deposit facilities increases substantially or is unusual in light of their past usage.
17. Many unrelated individuals make payments to one account without any rational explanation.
18. Third parties make cash payments or deposit checks to a customer's credit card.
19. Customer acquires significant assets and liquidates them quickly with no explanation.
20. Customer requests movement of funds that are uneconomical.
21. High volume of wire transfers are made or received through the account.

[5] ADB's Handbook on Anti-Money Laundering and Combating the financing of Terrorism for Nonbank Financial Institutions

F. Irregularities observed during account creation and CDD process[6]

1. Creating separate accounts under different names to circumvent restrictions on trading or withdrawal limits imposed by VASPs.
2. Transactions initiated from non-trusted IP addresses, IP addresses from sanctioned jurisdictions, or IP addresses previously flagged as suspicious.
3. Trying to open an account frequently within the same VASP from the same IP address.
4. Regarding merchants/corporate users, their Internet domain registrations are in a different jurisdiction than their jurisdiction of establishment or in a jurisdiction with a weak process for domain registration.
5. Incomplete or insufficient KYC information, or a customer declines requests for KYC documents or inquiries regarding source of funds.
6. Sender / recipient lacking knowledge or providing inaccurate information about the transaction, the source of funds, or the relationship with the counterparty.
7. Customer has provided forged documents or has edited photographs and/or identification documents as part of the on-boarding process.

II. Suspicious Indicators/Red Flags (Transaction Specific)

A. Transactions for nonprofit organizations (including registered charities) [7]

1. Inconsistencies between apparent modest sources of funds of the organization (e.g., communities with modest standard of living) and large amounts of funds raised.
2. Inconsistencies between the pattern or size of financial transactions and the stated purpose and activity of the organization.
3. Sudden increase in the frequency and amounts of financial transactions for the organization, or the inverse, that is, the organization seems to hold funds in its account for a very long period.
4. Large and unexplained cash transactions by the organization.
5. Absence of contributions from donors located in the country.
6. Organization's directors are outside the country, particularly if large outgoing transactions are made to the country of origin of the directors and especially if that country is a high-risk jurisdiction.
7. Large number of nonprofit organizations with unexplained links.
8. Nonprofit organization appears to have little or no staff, no suitable offices, or no telephone number, which is incompatible with their stated purpose and financial flows.

[6] ADB's Handbook on Anti-Money Laundering and Combating the financing of Terrorism for Nonbank Financial Institutions
[7] ADB's Handbook on Anti-Money Laundering and Combating the financing of Terrorism for Nonbank Financial Institutions

9. Nonprofit organization has operations in, or conducts transactions to or from, high-risk jurisdictions.

B. Suspicious indicators related to lending [8]

1. Customer suddenly repays a problem loan unexpectedly.
2. Customer makes a large, unexpected loan payment with unknown source of funds, or a source of funds that does not match the credit institution's knowledge about the customer.
3. Customer repays a long-term loan, such as a mortgage, within a relatively short period.
4. Source of down payment is inconsistent with borrower's background and income.
5. Down payment appears to be from an unrelated third party.
6. Down payment uses a series of money orders or bank drafts from different financial institutions.
7. Customer shows income from "foreign sources" on loan application without providing further details.
8. Customer's employment documentation lacks important details that would make it difficult for the credit institution to contact or locate the employer.
9. Customer's documentation to ascertain identification, support income, or verify employment is provided by an intermediary who has no apparent reason to be involved.
10. Customer offers the credit institution large dollar deposits or some other form of incentive in return for favorable treatment of loan request.
11. Customer seems unconcerned with terms of credit or costs associated with completion of a loan transaction.
12. Down payment or other loan payments are made by a party who is not a relative of the customer.
13. Reluctance to use favorable facilities, for example, avoiding high interest rate facilities for large balances.
14. Frequent and/or unscheduled cash deposits to loan accounts.
15. Frequent deposits of winning gambling checks followed by immediate withdrawal or transfer of funds.
16. Children's accounts being used for the benefit of parents and/or guardians.

C. Real Estate Sector[9]

1. Transactions in which there are signs, or it is certain, that the parties are not acting on their own behalf and are trying to hide the identity of the real customer.

[8] ADB's Handbook on Anti-Money Laundering and Combating the financing of Terrorism for Nonbank Financial Institutions
[9] FATF – Money Laundering & Terrorist Financing through the Real Estate Sector (June 2007)

2. Transactions which are begun in one individual's name and finally completed in another's without a logical explanation for the name change. (For example, the sale or change of ownership of the purchase or option to purchase a property which has not yet been handed over to the owner, reservation of properties under construction with a subsequent transfer of the rights to a third party, etc.).
3. Transactions in which the parties:
   a. Do not show particular interest in the characteristics of the property (e.g. quality of construction, location, date on which it will be handed over, etc.) which is the object of the transaction.
   b. Do not seem particularly interested in obtaining a better price for the transaction or in improving the payment terms.
   c. Show a strong interest in completing the transaction quickly, without there being good cause.
   d. Show considerable interest in transactions relating to buildings in particular areas, without caring about the price they must pay.

4. Transactions in which the parties are foreign or non-resident for tax purposes and:
   a. Their only purpose is a capital investment (that is, they do not show any interest in living at the property they are buying, even temporarily, etc.).
   b. They are interested in large-scale operations (for example, to buy large plots on which to build homes, buying complete buildings or setting up businesses relating to leisure activities, etc.).
5. Transactions in which any of the payments are made by a third party, other than the parties involved. Cases where the payment is made by a credit institution registered in the country at the time of signing the property transfer, due to the granting of a mortgage loan, may be excluded.

D. Life insurance companies, brokers, and agents [10]

1. Client wants to use cash for a large transaction.
2. Client proposes to purchase an insurance product using a check drawn on an account other than his or her personal account.
3. Client requests an insurance product that has no discernible purpose and is reluctant to divulge the reason for the investment.
4. Client who has other small policies or transactions based on a regular payment structure makes a sudden request to purchase a substantial policy with a lump-sum payment.
5. Client conducts a transaction that results in a conspicuous increase in investment contributions.
6. Scale of investment in insurance products is inconsistent with the client's economic profile.

[10] Money laundering and terrorist financing indicators—Life insurance companies, brokers and agents (June 2021)

7. Unanticipated and inconsistent modification of client's contractual conditions, including significant or regular premium top-ups.
8. Unforeseen deposit of funds or abrupt withdrawal of funds.
9. Involvement of one or more third parties in paying the premiums or in any other matters involving the policy.
10. Overpayment of a policy premium with a subsequent request to refund the surplus to a third party.
11. Funds used to pay policy premiums or deposits originate from different sources.
12. Use of life insurance product in a way that resembles the use of a bank account, such as making additional premium payments and frequent partial redemptions.
13. Client cancels investment or insurance soon after purchase.
14. Early redemption takes place in the absence of a reasonable explanation or in a significantly uneconomic manner.
15. Client shows more interest in the cancellation or surrender of an insurance contract than in the long-term results of investments or the costs associated with termination of the contract.
16. Client makes payments with small denomination notes, uncommonly wrapped, with postal money orders or with similar means of payment.
17. Duration of the life insurance contract is less than 3 years.
18. First (or single) premium is paid from a bank account outside the country.
19. Repeated and unexplained changes in beneficiary.
20. Relationship between the policy holder and the beneficiary is not clearly established.

E. Securities Firm[11]

1. Accounts that have been inactive suddenly receive large deposits that are inconsistent with the normal investment practice of the client or their financial ability.
2. Any dealing with a third party when the identity of the beneficiary or counterparty is undisclosed.
3. Client attempts to purchase investments with cash.
4. Client wishes to purchase a number of investments with money orders, traveler's checks, cashier's checks, bank drafts, or other bank instruments, where the transaction is inconsistent with the normal investment practice of the client or their financial ability.
5. Client uses securities or futures brokerage firm as a place to hold funds that are not being used in trading of securities or futures for an extended period of time, and such activity is inconsistent with the normal investment practice of the client or their financial ability.

[11] Money laundering and terrorist financing indicators—Life insurance companies, brokers and agents (June 2021)

6. Client wishes monies received through the sale of shares to be deposited into a bank account rather than a trading or brokerage account, which is inconsistent with the normal practice of the client.
7. Client frequently makes large investments in stocks, bonds, investment trusts, or other securities in cash or by check within a short time period, inconsistent with the normal practice of the client.
8. Client makes large or unusual settlements of securities in cash.
9. The entry of matching buying and selling of particular securities or futures contracts (called match trading), creating the illusion of trading.
10. Transfers of funds or securities between accounts not known to be related to the client.
11. Several clients open accounts within a short period of time to trade the same stock.
12. Client is willing to deposit or invest at rates that are not advantageous or competitive.
13. Client attempts to purchase investments with instruments in the name of a third party.
14. Third-party purchases of shares in other names (i.e., nominee accounts).
15. Transactions in which clients make settlements with checks drawn by third parties or remittances from third parties.

F. Dealers of Precious Metals & Stones – Red Fags[12]

1. Customer Behavior
   a. Established customer (including bullion dealers) dramatically increases his purchase of precious metals or stones for no apparent reason
   b. Purchase of gold bullion through multiple transactions over a short time period.
   c. Bullion is transferred among associates using bullion accounts (including family members) for no apparent commercial purpose.
   d. Occupation is inconsistent with the transaction. For example, the customer claimed to be a student but transferred large values of funds to bullion accounts.
   e. A new customer requests a refiner to turn gold into bullion.
   f. A customer does not ask for the reduced price or haggles over the list price.
   g. Buyer/seller apparently does not have reasonable expertise/experience in the precious metals/stones sector.

2. Company Behavior

[12] FIIB, "Strategic Analysis Report on Dealers in Precious Metals and Stones", (December 2021) (https://www.jfiu.gov.hk/info/doc/SAR_ON_DPMS.pdf)

a. Company name is changed to precious metal related. Incorporation or registration of a trading company in a tax haven even though its business relates to another jurisdiction.
b. Movement of abnormally large sums of money in various accounts of the individuals and companies which are not related to the nature of their business. Unusual deposits i.e. use of cash or negotiable instruments (such as traveller's cheques, cashier's cheques and money orders) in round denominations (to keep below reporting threshold limit) to fund bank accounts and to pay for gold.
c. Numerous sole proprietorship businesses/private limited companies set up by seemingly unrelated people (proxies) but controlled by the same group of people.
d. No clarity of how the company transports the merchandise it has bought.

3. Payment Behavior

E. A number of affiliated entities in the payments chain.
F. Natural person or business sells gold saying that it comes from a place with no extraction license or from places with no gold mines.
G. Purchase of gold bullion with bank cheques may be an attempt to conceal the source of the funds and underlying ownership.
H. The use of cash to purchase bullion, especially when there are multiple purchases in a short timeframe, or when large amounts are purchased at once, or when there are structured cash deposits into an account to finance a single gold bullion purchase.
I. Original source of funds to buy gold bullion cannot be established. The transaction involves the receipt of funds from third party entities that have no apparent connection with the transaction.
J. Transactions between domestic buyers and sellers with sales proceeds sent to unknown third parties overseas.

G. Cyber-enabled Fraud[13]

1. Transaction patterns

a. Rapid or immediate, high or low value transactions after opening of an account, inconsistent with the purpose of the account.
b. Rapid or immediate cash withdrawals or transfers of large amounts following the receipt of a funds transfer in order to empty the account.
c. Frequent and large transactions, which are inconsistent with the account holder's economic profile (e.g., sudden international transfers,

[13] FATF, A: Risk indicators for CEF, "Illicit Financial Flows from Cyber-enabled Fraud (fatf-gafi.org)" (November 2023) (https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Methodsandtrends/illicit-financial-flows-cyber-enabled-fraud.html)

withdrawals of cash performed through payment cards at foreign ATMs, large purchases of VA or goods to be exported abroad, or payments in favor of unlicensed foreign MVTS).

d. Transfers of funds to and from high-risk money laundering jurisdictions.
e. Large frequent transactions with recently established companies and/or whose main activities are not consistent with the activities carried out by the beneficiary or have a general purpose.
f. Small payment to a beneficiary, which once successfully completed, is rapidly followed by larger value payments to the same beneficiary.
g. Round value amount purchases that are frequent and/or in large amounts, which can indicate gift card purchases.

2. Customer transaction instructions and remarks

a. A customer transaction requests for additional payments immediately following a successful payment to an account not previously used by the customer to pay its suppliers/vendors. Such behaviour may be consistent with a criminal attempting to issue additional unauthorized payments upon learning that a fraudulent payment was successful.
b. A customer's seemingly legitimate transaction instructions contain a different language vernacular, timing, and amounts than previously verified transaction instructions.
c. Transaction instructions include markings, assertions, or language designating the transaction request as "Urgent", "Secret" or "Confidential."
d. A customer presents poorly formatted messages / emails (spelling and/or grammar mistakes) as justification of a transaction.
e. Transaction instructions direct payment to a known beneficiary; however, the beneficiary's account information is different from what was previously used.
f. The intended beneficiary in the transaction description and the name of the account holder known to the beneficiary bank are inconsistent.
g. Transfers ordered by natural persons (alleged investors) with no financial experience and expertise, in favour of companies (in many cases established in high-risk jurisdictions) with reasons for payments related to investments and financial products.
h. Counterparties incommensurate with the business/company name of the account might suggest which may provide cover for the movement of large amounts of funds internationally (e.g., the company reported as a furniture company made multiple large transfer to a company named as petroleum trading company).
i. Transactions conducted with device time zone mismatch.

3. Suspicion in account holder's profile

a. Account holder is unwilling or unable to pass CDD checks.
b. Account holder is unfamiliar with the source of the funds moving through their account or claiming they are transacting for someone else.
c. Frequent changes of legal entities'/sole proprietorships' names using foreign expressions and terminology.
d. The customer shows to have inadequate knowledge on the nature, object, amount or purpose of the transaction/s or relationship or provides nonrealistic, confusing or inconsistent explanations, which drive to the suspicion that the customer is acting as a mule.

4. Suspicion in account user's identity

a. The user is attempting to conceal their identity by using shared, falsified, stolen or altered identification (address, telephone number, email)
b. Frequent changes of contact details, phone numbers, email addresses after opening of the account
c. E-mail addresses that do not seem compatible with the name of the account holder, or a pattern of similar email addresses seen across multiple accounts.
d. Irregularities in customer profile particulars, such as shared credentials (e.g., shared by two or more users) with other accounts.
e. Abnormalities identified via online behaviour, such as hesitation inputting data, keystroke delays, signs of automation, multiple failed login attempts, etc
f. Accounts relating to entities who could be expected that they are no longer active in the jurisdiction (e.g., overseas students' account sold when completed study)
g. IP addresses or GPS coordinates originating from high-risk money laundering jurisdictions.
h. Use of virtual private networks (VPNs), compromised devices (such as IOT devices), and hosting companies that may mask a user's IP address.
i. Multiple IP addresses or electronic devices associated with a single online account.
j. Single static IP address or electronic device associated with multiple accounts of various account holders.
k. Remote desktop connection access to an account through computer ports used by applications such as TeamViewer etc. which prevents the true device and location to be seen.
l. Accounts operated with excessively quick keystrokes or navigation suggesting possible bot control.

5. VA transactions

a. Sending/receiving large volumes or high frequency low amounts worth of VAs to unhosted wallet addresses; or addresses associated with darknet marketplaces, child sexual abuse material platforms, cyber exploit marketplaces, ransomware groups, mixing/tumbling services, high-risk jurisdictions, gambling sites, and scammers.
b. Maxing out daily funding limits at Bitcoin ATMs
c. No documents proving the origin of VA or of the money converted in crypto assets.
d. Transfers of VAs to wallets linked to illegal activities on the dark web (e.g., terrorism, child pornography, narcotics, etc.).
e. Transactions involving more than one type of VAs, particularly those that provide higher anonymity.
f. Abnormal transaction activity of VAs from peer-to-peer platform associated wallets with no logical business explanation

II. Typologies

A. Human Trafficking[14]

1. Front Companies

Human traffickers routinely establish and use front companies, sometimes legal entities, to hide the true nature of a business, and its illicit activities, owners, and associates. Front companies are businesses that combine illicit proceeds with those gained from legitimate business operations.

Examples of front companies used by human traffickers for labor or sex trafficking include massage businesses, escort services, bars, restaurants, and cantinas. Often, these establishments will appear to be a single storefront, yet are part of a larger network.

Payments for these illicit services are usually in cash, and traffickers may invest the illicit proceeds in high-value assets, such as real estate and cars.

2. Funnel Accounts

Funnel accounts generally involve an individual or business account in one geographic area that receives multiple cash deposits, often in amounts below the cash reporting threshold, from which the funds are withdrawn in

[14] See FINCEN Advisory, FIN-2020-A008, "Supplemental Advisory on Identifying and Reporting Human Trafficking and Related Activity," (October 15, 2020) (https://www.fincen.gov/sites/default/files/advisory/2020-10 15/Advisory%20Human%20Trafficking%20508%20FINAL_0.pdf)

a different geographic area with little time elapsing between the deposits and withdrawals.

Human traffickers may use interstate funnel accounts to transfer funds between geographic areas, move proceeds rapidly, and maintain anonymity. In labor and sex trafficking schemes, human traffickers may open accounts in their name, or escort victims to a bank, and force them to open an account. Traffickers maintain control of the victims' bank accounts through coercion, and direct victims to deposit money into their accounts and other accounts that the traffickers can access. In some cases, victims also are coerced or forced to wire proceeds via money services businesses (MSBs) to facilitate the funneling of proceeds.

3. Alternative Payment Methods

In addition to payment via cash, traffickers also have accepted payment via credit cards, prepaid cards, mobile payment applications, and convertible virtual currency. Illicit actors also use virtual currency to advertise commercial sex online. For example, human traffickers have purchased prepaid cards, and then used the cards to purchase virtual currency on a peer-to-peer exchange platform. Human traffickers then use the virtual currency to buy online advertisements that feature commercial sex acts to obtain customers.

FinCEN also has identified transactions in which human traffickers use third-party payment processors (TPPPs) to wire funds, which gives the appearance that the TPPP is the originator or beneficiary of the wire transfer and conceals the true originator or beneficiary. For example, human traffickers facilitate payments via TPPPs for the operation of online escort services and online streaming services that use voice-over Internet protocol technology. Human traffickers and their facilitators use TPPPs to wire funds to individuals or businesses both domestically and abroad.

B. Illicit Drug Trafficking[15]

Use of professional money laundering networks
Organised crime groups use professional money laundering networks to launder the proceeds of their illegal activities36. As the main purpose of professional money launderers is to facilitate the transfer of value for their customers, they are rarely involved in the proceeds-generating illegal activities. Instead, they provide expertise to disguise the nature, source, location, ownership, control,

[15] FATF, "Money Laundering from Fentanyl and Synthethic Opiods" (November 29, 2022) (https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Money-Laundering-Fentanyl-Synthetic-Opioids.pdf.coredownload.inline.pdf)

origin and/or destination of funds to avoid detection. Professional money launderers generally do not differentiate between drug dealers, fraudsters, human traffickers or any other criminal with a need to move or conceal ill-gotten gains. They engage in sophisticated, large-scale laundering on behalf of drug cartels, motorcycle gangs and traditional organized crime organizations.

While professional money laundering networks may include accountants, bankers or lawyers, current financial intelligence suggests that they often are owners of, or associated with, trading companies or money-services businesses, as well as a variety of legitimate commercial enterprises they use as fronts. Professional money launderers use their occupation and knowledge, as well as the infrastructure associated with their line of work and their networks, to facilitate money laundering, providing a veneer of legitimacy to criminals and criminal organizations.[16]

C. Use of offshore banks, international business companies, and offshore trusts, including trust company service providers

Mr. ES, the Director of Company A (a State-Owned Airline Company) and a politically exposed person (PEP), procured a shipment of RR Trent 700 engines and three Airbus aircraft and CRJ 1000 NG aircraft. ES is also the founder and beneficial owner of Company B, a company incorporated under the laws of Jurisdiction A (an offshore financial center).

ES received a fee, which constituted a bribe, when procuring aircraft and engine maintenance from Company F, Company G and Company H which was received through Company I and Company J (owned by Mr. STK). Ultimately, this fee was received from Company K through Company L in Jurisdiction B.
ES used Company B's account at Bank U in Jurisdiction C to receive the fee received from the procurement and used MB's (ES' wife) bank account as a holding account for SGD 480,000 (approx. USD 350,787), before transferring it to another party by breaking up the transaction to SAB (daughter of ES) of SGD 162,124 (approx. USD 118,479) and SGD 45,300 (approx. USD 33,104), transferring SGD 291,785 (approx. USD 213,229) to the account in the name of MS (Parent of ES) and transferring SGD 2,476 (approx. USD 1,809) to the account in the name of ER (Son of ES).

While ES had attempted to obscure the ownership of Company B using the establishing of a trust, cooperation between PPATK (Indonesia FIU) and law enforcement agencies abroad identified that Company B belongs to ES and SAB (daughter of ES).

[16] FATF, "Money Laundering from Fentanyl and Synthethic Opiods" (November 29, 2022) (https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Money-Laundering-Fentanyl-Synthetic-Opioids.pdf.coredownload.inline.pdf)

A number of foreign bribes were received into Company B's account, then ES deposited the money amounting to USD 1,458,364 to STK through STK's personal account, then he provided a means to return the deposit of funds belonging to ES by setting up a company in Jurisdiction A along with their accounts, namely Company M in Jurisdiction C and Company N's account in Bank A. An underhand agreement accompanied by AR (lawyer) was then made as if buying and selling apartments in Jurisdiction C and avoiding a stamp duty of 13% of the selling price. This underlying transaction appears to be legitimate economic activity in the form of buying and selling apartments between ES and STK. [17]

D. Casino Related Typologies[18]

1. Purchase of Chips with Small-Denomination Currency, Followed by Modest Gambling Actions

   MGK, a Malaysian, was reported by the Cage Team of Casino B as he purchased gaming chips, totaling PHP1.5 million, using 14,970 pieces of PHP100 bills and 3 pieces of PHP1,000 bills. Review of surveillance footage revealed that MGK entered the property with bags containing the cash in question. The subject purchased gaming chips, with which he played for roughly two hours, wagering an average of PHP14,211 and winning PHP0.15 million. MGK proceeded to the cage where he attempted to redeem PHP1.04 million but cancelled the transaction after realizing he would be refunded with his original PHP100 bills. MGK went to a separate cage a few minutes later and successfully redeemed PHP0.25 million. MGK left the premises following the aforementioned transactions without cashing out his remaining chips. The individual returned to the property the following day and used PHP1.1 million in funds to win a total of PHP1.31 million on two separate occasions and cages. The earnings were then transferred to the NDW Junket Cage. Notably, MGK was previously the subject of five (5) similar STRs that were submitted to the AMLC. There is no other information available on MGK.

2. Involvement in CPH Criminal Syndicate

   Casino E reported the subject persons as members of the CPH criminal syndicate. Table 12 identified the 12 STRs related to the individuals allegedly connected to the syndicate. Notably, HLP, one of the identified members, is involved in various businesses, such as construction, cosmetics

[17] APG Typologies Report 2022 (13 August 2022) (http://www.apgml.org/includes/handlers/get-document.ashx?d=d2972f3d-aa22-4b7f-ac9e-848cd26e9461)

[18] AMLC Typology – Analysis of Suspicious Transactions associated with Casino Junkets, January 2023 (http://www.amlc.gov.ph/images/PDFs/PR2023/2023%20JAN%20ANALYSIS%20OF%20SUSPICIOUS%20TRANSACTIONS%20ASSOCIATED%20WITH%20CASINO%20JUNKETS_FINAL.pdf)

distributorship, and lending. He is also an official of one company that is allegedly running a Ponzi scheme and was involved in an adverse news about casino junket operations. HLP had personal and corporate accounts with a domestic bank, both of which were closed due to unresolved red-flag transactions. Notably, HLP issued a bogus check in the amount of PHP10.50 million in another domestic bank. Given the circumstances, an STR pertinent to the fraudulent issue of the bogus check was warranted, and the checking account was closed. Related to this, Casino B received a letter from the AGA for Casinos on the alleged investment fraud activities of the CPH. The aforementioned letter indicated that the group is run by HLP, who, upon verification, is a member of Casino B's rewards program. HLP allegedly entices investors into a contract of loan by promising them exorbitant returns or interest by issuing post-dated checks that ultimately bounce. The group asserted that they had a junket deal with private casinos and that the funds will be used to pay their international guests' gaming operations. In an effort to provide the appearance of a real organization, the gang uses names of legitimate businesses.

3. Transactions Not Commensurate with Declared Source of Funds

Due to suspicious circumstances, a bank reported 32 STRs, totaling PHP262.73 million tied to the account of AMG. Upon account-opening, AMG purportedly submitted an SEC registration document. LYM, who produced his driver's license and Chinese passport as identification, is the authorized signatory. AMG's client information file shows that it is involved in management consulting. Per branch's inquiries, however, AMG was found to be a casino junket operator at Casino D. According to the branch's evaluation of the account statement, AMG's transactions do not correspond to its declared source of funds. From account-opening in April 2015 to March 2016, the only activity in the account was the initial deposit of PHP50,000. In April 2016, however, the account began to have a large number of transactions. AMG's deposits and on-us credits, which were usually processed inter-branch, had values as high as eight digits. Between October 2016 and March 2017, the reporting branch identified transactions worth PHP262.73 million, which are deemed suspicious or not commensurate with the declared source of funds of AMG.

E. Use of Virtual Assets [19]

1. Money Laundering thru Mix of Bank Accounts & Virtual Assets

[19] APG Typologies Report 2022 (13 August 2022)
(http://www.apgml.org/includes/handlers/get-document.ashx?d=d2972f3d-aa22-4b7f-ac9e-848cd26e9461)

Under the guise of friendship, Person A was coaxed into providing his bank account details online. Consequently, he received funds in his bank account, which turned out to be criminal proceeds from a business email compromise scam conducted outside Singapore. Person A further provided his personal information to facilitate the creation of an account with a cryptocurrency trading platform based outside Singapore, control of which was ceded to the unknown person. Under the instructions of the unknown person, Recipient A then transferred most of the criminal proceeds to the bank account of Recipient B. Consequently, investigations revealed that Recipient B sent Bitcoin to Recipient A's trading account, and the proceeds were further laundered via cryptocurrency.

2. Cryptocurrency Trading related to Phishing

Several online news articles and stories circulated in social media regarding several accounts hacked by unknown perpetrators. Based on the report submitted by a bank (which was shared by a Supervising Agency), certain accounts were identified as recipients of the funds from another bank (alleged hacked accounts). Most of the identified recipients had financial transactions, particularly inter-account transfers (outflows), during the period when the alleged hacking incident transpired.

The aforementioned funds which may possibly represent the funds that were unlawfully transferred from multiple accounts were then transferred by the subjects to another bank's accounts (layering), which may indicate that the accountholders may likely be money mules and that their accounts may have been used as a pass-through account. Furthermore, the second beneficiaries, who are either individuals or businesses, appear to be engaged in cryptocurrency trading based on their financial activities.

STRs related to the subjects indicated that their accounts were involved in phishing activities or had received unauthorised fund transfers. The initial beneficiaries had outgoing transactions (inter-account transfers) involving significant amounts which were transacted after the period of the alleged hacking incident. The total amount of debit transactions of some of the subjects almost totalled the amount of their credit transactions, indicating that their accounts were merely just pass-through accounts. According to an online news article, the hacked funds were used to buy cryptocurrencies. During the layering stage, the initial beneficiaries (possible money mules) transferred funds to businesses and individuals (second beneficiaries), some of which were allegedly engaged in cryptocurrency trading. Some of the second beneficiaries have had outgoing transactions to companies who are associated with cryptocurrency exchanges. The second beneficiaries received significant amounts of incoming fund transfers from numerous

individuals, which appeared not to be commensurate with their declared businesses and financial capacities.

3. Cryptocurrency Investment Program Scam

The suspect, Mr. C, has been the owner of Company T since 2017. Mr. C established four investing platforms and promoted his cryptocurrency investment programs in online chat groups, promising investors that his programs can generate 80% to 720% returns per year. However, many of the investment programs did not exist. To invest, investors could either deposit cash into Company T's bank account or transfer cryptocurrencies to the crypto wallets provided by Company T or Mr. C's personal wallet. In order to convince investors that these programs could genuinely make profits, Mr. C sent cryptocurrencies to investors as returns from his own crypto wallets or Company T's bank accounts. However, Mr. C was fraudulently operating a pyramid scheme. Finally, in order to conceal and disguise the illegal gains, Mr. C sold his cryptocurrencies through over-the-counter trading (OTC) markets, then transferred the money into Company T's bank account and withdrew the cash. In August 2021, a District Prosecutors Office prosecuted Mr. C for fraud and offenses against Article 29 of the Banking Act.

F. Online Sexual Abuse and Exploitation of Children

Please refer to AMLC Study: ***"ONLINE SEXUAL ABUSE AND EXPLOITATION OF CHILDREN IN THE PHILIPPINES: An Evaluation Using STR Data (July 2020 – December 2022)***, published in the AMLC Website - OSAEC in the Philippines

G. Gold Smuggling

Involvement of Unrelated Counterparties:

Mr. DWK was involved in the business of selling raw materials for building constructions. Mr. DWK maintained multiple personal and business accounts at different banks and his transactional activity was unusual comprising of home remittances, online transfers, clearing of cheques, cash deposits and withdrawals. The transactions were conducted with various unrelated counterparties including clearing/forwarding agents, jewellers, car dealers, real estate dealers, overseas Pakistanis etc. A few counterparties were identified to be involved in illegal foreign exchange businesses which strengthened the suspicion of the involvement of Mr. DWK in Hawala/Hundi. During analysis, STRs were also found on the family members of Mr. DWK including 1) Mr. RWK (brother), 2) Mr. TWK (brother), 3) Mr. AUK (brother), 4) Mr. YK (son), 5) Mr. AK (son), whereby similar transactional activity was identified, and suspicions were reported. Some of the family members were residing in Country A and involved

in businesses related to transport, while a few of them were living in Pakistan and involved in trading businesses.

During analysis, Mr. DWK was found to be under investigation by a law enforcement agency (LEA) in Pakistan for his involvement in the smuggling of gold. The individual was apprehended for smuggling of gold from the airport. The LEA informed that the individual managed to import artificial jewellery against the export of pure gold, which is in violation of the Procedure for Export of Gold Jewellery and Precious / Semi-Precious Stones and Import Facility.[20]

[20] APG Typologies Report 2022 (13 August 2022) (http://www.apgml.org/includes/handlers/get-document.ashx?d=d2972f3d-aa22-4b7f-ac9e-848cd26e9461)