Customer Due Diligence & AML/ Sanctions Framework v4.0.1

Aligned with the T&C and the Privacy Policy | Publication Date: 24 September 2026

This Customer Due Diligence & AML/Sanctions Framework (the “Framework”) constitutes the authoritative English-language canonical version of the customer due diligence, anti-money-laundering, and sanctions-compliance framework adopted by Neom Triple A Information Technology LLC, operating under the brand NEOMAAA Funded. This Framework is published as a voluntary commitment to high standards of consumer protection, fraud prevention, sanctions compliance, and ethical business conduct, and is applied to the Company’s activities as a provider of simulated trading evaluation services. This Framework supersedes all previously published versions of the AML / KYC Policy of NEOMAAA Funded.

---

§1 Framework Statement

1.1 Neom Triple A Information Technology LLC (brand: NEOMAAA Funded, hereinafter the “Company”) undertakes an unconditional commitment to comply with all laws and regulations applicable to its activities as a provider of simulated trading evaluation services, including consumer-protection, fraud-prevention, sanctions-compliance, and tax-compliance obligations, and to observe, as voluntary best practice and to the extent applicable, principles derived from international AML/CFT standards. This commitment is fundamental to the Company’s lawful operations and to maintaining the trust of Participants, banking partners, and regulators.

1.2 The Company acknowledges that its activities involving the receipt of payments from Participants under simulated trading evaluation programmes, as well as the disbursement of awards under the Benefit Program in accordance with the T&C, carry risks of exploitation in money-laundering or terrorist-financing schemes. This Framework establishes measures to identify, assess, and mitigate such risks.

1.3 This Framework applies to all Participants (as defined in the T&C §1.5(c)), to all employees, directors, contractors, and agents of the Company, and to all financial operations connected with the Company’s activities. The Company implements this Framework through a Risk-Based Approach (RBA), calibrating the intensity of AML/CFT measures to the level of identified risk.

1.4 This Framework forms part of an integrated document set comprising the T&C, the Privacy Policy, and the Cookie Policy. In the event of any conflict between this Framework and the T&C, the provisions of the T&C shall prevail.

---

§2 Scope and Legal Entity

2.1 Controlling Legal Entity. This Framework applies to the operations of the following legal entity:

Full legal name: Neom Triple A Information Technology LLC Brand: NEOMAAA Funded Registered address: The Binary by Omniyat, Office 2114, Business Bay, Dubai, UAE Website: neomaaafunded.com

2.2 Scope of the Framework. This Framework applies:

1. to all Participants regardless of their jurisdiction of residence or citizenship;

2. to all payment-receipt transactions for Funded Evaluation Accounts (§1.5(f) the T&C) and Express Evaluation Accounts (§1.5(m) the T&C), as well as to all Benefit Program disbursements pursuant to §17 of the T&C;
3. to all employees, directors, contractors, and representatives of the Company;
4. to all third parties acting on behalf of or in the interests of the Company in connection with the receipt or disbursement of funds.

2.3 Activity Classification. The Company is a provider of simulated trading evaluation services. The Company is not a licensed financial institution, credit institution, broker, dealer, investment adviser, or virtual-asset service provider within the meaning of any applicable legislation, and does not hold customer funds, securities, or investments. The Company observes the framework set out below as a matter of voluntary commitment to high standards of consumer protection, fraud prevention, and sanctions compliance, irrespective of any classification of its activities under UAE Federal Decree-Law No. 10 of 2025 on Anti-Money Laundering, Combating the Financing of Terrorism, and Financing of Illegal Organisations or Cabinet Decision No. 134 of 2025.

2.4 Highest-Standard Principle. Where applicable requirements of different jurisdictions conflict, the Company applies the most stringent standard compatible with the Company's operations as a legal entity incorporated in the UAE.

---

§3 Regulatory Framework

3.1 UAE Regulatory Framework — To the Extent Applicable. The Company has regard to the following UAE regulatory instruments as part of its voluntary AML/sanctions framework, to the extent applicable to its activities:

1. UAE Federal Decree-Law No. 20 of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Financing of Illegal Organisations (as superseded by Federal Decree-Law No. 10 of 2025) (hereinafter "UAE FDL 20/2018" or "AML FDL") — the primary UAE legislative instrument establishing principles of Customer Due Diligence (CDD), Enhanced Due Diligence (EDD), suspicious-activity assessment, and record-keeping; observed by the Company as voluntary best practice;
2. Cabinet Decision No. 10 of 2019 concerning the Implementing Regulation of UAE Federal Decree-Law No. 20 of 2018 (superseded by Cabinet Decision No. 134 of 2025, in force from 14 December 2025) — establishing detailed procedural requirements for customer identification, risk management, and reporting;
3. UAE Federal Decree-Law No. 26 of 2021 amending certain provisions of Federal Decree-Law No. 20 of 2018 — expanding the category of obliged entities and strengthening sanctions;
4. UAE Federal Law No. 7 of 2014 on Combating Terrorism Offences — establishing the concept of terrorism financing and related counter-financing obligations;
5. UAE Federal Decree-Law No. 34 of 2021 on Combating Rumours and Cybercrimes — applicable to the digital dimension of the Company's activities, including its online platform and electronic transactions (this instrument repealed and replaced UAE Federal Law No. 5 of 2012 with effect from 2 January 2022);
6. UAE Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data (the "UAE PDPL") — establishing the legal framework for the processing of personal data in the UAE, including the lawful bases, data subject rights, security obligations, and cross-border transfer requirements that apply to the Company's processing of personal data collected, generated, or retained for AML/CFT/CPF purposes (including CDD, EDD, ongoing monitoring, SAER documentation, and the record-keeping period); and

7. UAE Cabinet Decision No. 58 of 2020 on the Regulation of the Beneficial Owner Procedures — establishing the obligations of legal persons in the UAE to identify, record, and report their beneficial owners, and providing the operative definition of Beneficial Owner used in this Framework at §4.1.

3.2 International Standards and Sanctions Regimes. This Framework also has regard to:

1. Financial Action Task Force (FATF) Recommendations — the international standards for combating money laundering, terrorism financing, and proliferation financing, in particular Recommendations 1, 10, 11, 12, 15, 19, and 20;
2. UN Security Council Consolidated List — including the consolidated list of individuals, entities, and jurisdictions subject to sanctions adopted under Chapter VII of the UN Charter;
3. sanctions programmes administered by the U.S. Department of the Treasury Office of Foreign Assets Control (OFAC), the European Union, HM Treasury (United Kingdom), and the UAE Executive Office for AML/CFT.

3.3 Changes to the Regulatory Landscape. The Company monitors changes in applicable legislation and undertakes to update this Framework with reasonable promptness following the entry into force of any material amendment. In accordance with §1.3(a)(iv) of the T&C, changes required by AML/CFT-related obligations take effect immediately upon publication.

---

§4 Definitions

4.1 For the purposes of this Framework, the following definitions apply:

“Money Laundering” — acts as defined under Article 2 of the AML FDL: receiving, acquiring, possessing, using, transferring, or transforming funds or property, where the person knows or ought to know that they constitute proceeds of crime, carried out with the intent of concealing or disguising their illicit origin, or of assisting any person involved in a predicate offence to evade its legal consequences.

“Financing of Terrorism” — the provision or collection of funds with the intent, or with knowledge, that they will be used in whole or in part to finance activities as prescribed by UAE Federal Law No. 7 of 2014 on Combating Terrorism Offences, or to finance individuals or organisations engaging in terrorist activities.

“Beneficial Owner” (Ultimate Beneficial Owner, UBO) — the natural person who ultimately owns or controls a legal entity or other structure that is a customer, or the natural person on whose behalf a transaction is conducted, in accordance with the definition set out in UAE Cabinet Decision No. 58 of 2020 on Beneficial Ownership Registers.

“Politically Exposed Person (PEP)” — a natural person who holds or has held a prominent public function (head of state or government, government minister, senior military official, director of a state-owned enterprise, head of an international organisation, etc.), as well as close family members and known close associates of such a person.

“Customer Due Diligence (CDD)” — the set of standard identification and verification measures applied in respect of a customer, including establishing the source of funds, assessing the business relationship, and its purpose.

“Enhanced Due Diligence (EDD)” — enhanced verification measures applied to higher-risk customers, including Politically Exposed Persons (PEPs), customers from higher-risk jurisdictions, and other persons specified in §7 of this Framework.

“Simplified Due Diligence (SDD)” — reduced verification measures applied to customers of demonstrably low risk, subject to all conditions established under this Framework being satisfied.

“Suspicious Activity Escalation Report (SAER)” — an internal written report prepared by Company personnel documenting grounds to suspect that a transaction or account is connected with money laundering, terrorism financing, fraud, sanctions evasion, or other illicit activity, escalated to Senior Management for assessment and any further action required by applicable law.

“Head of Compliance” — the Company officer responsible for coordinating the customer due diligence, sanctions screening, and internal suspicious-activity escalation procedures set out in this Framework.

“Participant” — a natural person or legal entity registered to use the Services of NEOMAAA Funded in accordance with §1.5(c) of the T&C.

“Funded Evaluation Account” — a simulated account with a virtual balance provided to a Participant who has successfully completed the Evaluation Phase, within the meaning of §1.5(f) of the T&C.

“Express Evaluation Account” — a single-phase Funded Evaluation Account as provided for under §1.5(m) of the T&C.

“Recognition Level” — the contractual parameter selected by the Participant when purchasing a Funded Evaluation Account, determining the Reward Coefficient and Initial Simulated Capital, within the meaning of §1.5(y) of the T&C.

---

§5 Risk-Based Approach

5.1 Proportionality Principle. In accordance with FATF Recommendation 1 and the AML FDL, the Company applies Customer Due Diligence (CDD), Enhanced Due Diligence (EDD), and monitoring measures proportionate to the identified level of risk. The intensity of measures is set in proportion to the risk and is not applied uniformly across all customers.

5.2 Risk Assessment Factors. The Company assesses the following risk factors in respect of each Participant and the business relationship with that Participant:

1. Customer Risk: type of customer (natural person, legal entity, corporate structure), occupation, Politically Exposed Person (PEP) status or PEP affiliation, history of chargebacks or payment disputes, conduct during KYC.
2. Geographic Risk: country of residence and citizenship of the Participant, country of source of funds, consistency of IP address with KYC data, classification of the jurisdiction under FATF lists, EU High-Risk Third Countries lists, or applicable sanctions lists.
3. Product Risk: type of account used (Funded Evaluation Account, Express Evaluation Account), aggregate payment and Benefit Program disbursement amounts, frequency and pattern of transactions, selected Recognition Level.
4. Channel Risk: nature of the interaction (remote/non-face-to-face), use of anonymisation tools (VPN, proxy, Tor) in breach of §7.10.1(l) of the T&C, discrepancy between IP address and the jurisdiction declared at KYC.

5.3 Due Diligence Levels. Based on the aggregate assessment of risk factors, the Company applies one of three due diligence levels:

1. Standard Customer Due Diligence (Standard CDD) — for Participants with a low or moderate risk level. Includes identity verification through Sumsub, screening against sanctions lists and PEP lists, and assessment of source of funds.

2. Enhanced Due Diligence (EDD) — for higher-risk Participants. Applied in the circumstances specified in §7 of this Framework. Includes additional documentation, a source-of-wealth declaration, and senior management approval.
3. Simplified Due Diligence (SDD) — applied exclusively in respect of legal entities listed on regulated exchanges in jurisdictions with an adequate AML regime, and government bodies, in the absence of any risk indicators.

5.4 Documentation. The risk assessment of each Participant is documented in the customer file. Any manual override of a risk assessment requires written justification and approval from the Head of Compliance of the Company.

5.5 Risk Assessment Review. The risk assessment of each Participant is reviewed upon any of the following events: any material change in transaction volume or behaviour; a request for a Benefit Program disbursement; identification of red flags; and in any event no less than once per year for higher-risk Participants.

---

§6 Customer Due Diligence (CDD)

6.1 KYC Triggers. The Company conducts or updates KYC verification in the following circumstances:

1. upon opening a new account or upon the first payment for any type of Prop Account;
2. upon a first request for a Benefit Program disbursement;
3. [Intentionally reserved];
4. upon identification of unusual activity, red flags, or a change in the Participant’s risk profile;
5. upon a request directed to the Participant under §7.10.1(m) of the T&C in connection with possible third-party involvement;
6. upon scheduled periodic review of the customer file (higher-risk Participants: every 6 months; medium-risk: every 12 months; lower-risk: every 36 months).

6.2 Data Collected. As part of standard Customer Due Diligence (CDD), the Company collects the following data and documents:

1. identity document: a valid passport (photo and biographical-data page), an EU national identity card, or a driver’s licence (in jurisdictions where it is accepted as a satisfactory identification document);
2. biometric selfie verification: a dynamic video recording (liveness check) or a static selfie with the identity document, to prevent the use of third-party documents and deepfake accounts;
3. proof of residential address: a utility bill, bank statement, official government letter, or lease agreement issued no earlier than three months prior to submission;
4. Source of Funds Declaration: mandatory where the aggregate volume of payments or disbursements exceeds the thresholds set by the Company (specific thresholds are not disclosed in this public version of the Framework in accordance with the confidentiality principles of the Company’s AML controls).

6.3 KYC/IDV Provider. The Company carries out identity verification and biometric checks through the Sumsub platform (Sum and Substance Ltd / Sumsub Group). Sumsub is the Company’s KYC/AML provider, referred to in recipient category (ii) of §6 of the Privacy Policy. Personal data is transferred to Sumsub under a written data-processing agreement incorporating Standard Contractual Clauses (SCCs) in accordance with Commission Implementing Decision (EU) 2021/914. A full list of current KYC/IDV providers is available on request at privacy@neomaaafunded.com.

6.4 Real-Time PEP and Sanctions Screening. Upon KYC, each Participant undergoes:

1. real-time screening against current Politically Exposed Person (PEP) lists (Dow Jones Risk & Compliance, WorldCheck, or equivalent databases integrated through Sumsub);
2. screening against the sanctions lists set out in §9 of this Framework;
3. adverse media screening against relevant databases.

Screening is conducted both at onboarding and on an ongoing basis. Where a match or potential match is identified, the procedure described in §9 of this Framework applies.

6.5 Phone Number Verification. In accordance with §6.1 of the T&C, the Participant is required to complete phone number verification by SMS code within seven (7) calendar days of the first payment or account registration. Failure to verify results in restricted access to platform features, including the creation of new accounts and requests for Benefit Program disbursements.

6.6 Giveaway Accounts. Participants who have received accounts through giveaways, prize draws, or partner offers must complete full KYC verification before any Benefit Program disbursement request is processed, in accordance with §7.12(B)(v) of the T&C.

6.7 Corporate Customers. Where a legal entity registers, the Company additionally requests: a certificate of incorporation, a Memorandum of Association, documents confirming the authority of the authorised representative, and ownership-structure documents disclosing all Ultimate Beneficial Owners (UBOs) holding more than 25% of shares or voting rights (in accordance with UAE Cabinet Decision No. 58 of 2020). Structures in which the beneficial owner cannot be identified are not accepted for service.

6.8 Consequences of KYC Non-Compliance. In accordance with §6.4 the T&C and §6.4.2 of the T&C, a Participant’s failure to complete KYC verification will result in restricted access to the Services and may result in termination in accordance with §15 of the T&C.

---

§7 Enhanced Due Diligence (EDD)

7.1 Mandatory EDD Triggers. Enhanced Due Diligence (EDD) is mandatory in the following circumstances:

1. PEP status identified or suspected: the Participant is a Politically Exposed Person (PEP), a family member of a PEP, or a known close associate of a PEP;
2. the Participant is a resident or citizen of a jurisdiction included in the FATF “Call for Action” list or in the European Commission list of high-risk third countries;
3. a connection or possible connection with a sanctioned person or entity has been identified;
4. an unusual transaction pattern has been identified: structuring of payments, immediate withdrawal of funds following receipt, payments from payment details that do not match the Participant’s verified information;
5. a discrepancy between the IP address or geolocation and the declared jurisdiction, in accordance with §7.10.1(l) of the T&C;
6. a high aggregate value of Benefit Program disbursements for a single Participant;
7. identification of coordination of trading activity across multiple accounts in accordance with §7.12 of the T&C;
8. any other factor indicating a higher level of risk in the assessment of the Head of Compliance.

7.2 Additional EDD Measures. Enhanced Due Diligence (EDD) includes the following additional measures over and above standard Customer Due Diligence (CDD):

1. obtaining senior management approval prior to commencing or continuing a business relationship with a Participant subject to EDD;
2. obtaining a Source of Wealth Declaration with supporting documentary evidence (tax returns, employment contract, property transaction documents, etc.);
3. obtaining a detailed Source of Funds Declaration for each material transaction;
4. verifying documents through additional independent sources;
5. enhanced ongoing monitoring of the business relationship with the Participant;
6. a shortened periodic review cycle for the customer file (every six (6) months instead of the standard 12 or 36 months).

7.3 EDD Documentation. All Enhanced Due Diligence (EDD) measures are documented in the customer file, recording: the date on which EDD was conducted; the grounds for applying EDD; the results of each measure; the name of the officer conducting EDD; and the decision reached following EDD, bearing the signature of the Head of Compliance.

7.4 Prohibition on Service Without Completion of EDD. All Benefit Program disbursements are suspended pending the completion of the EDD procedure and a positive decision by the Head of Compliance. Such suspension does not constitute a breach of the Company’s obligations to the Participant.

---

§8 Prohibited Jurisdictions

8.1 Absolute Prohibition. The Company does not provide Services to Participants who are residents, citizens of, or acting on behalf of, the following jurisdictions subject to comprehensive sanctions or classified by FATF under “Call for Action”:

1. Cuba;
2. Iran;
3. Democratic People’s Republic of Korea (DPRK / North Korea);
4. Myanmar (to the extent covered by the FATF Call for Action list);
5. Syria;
6. Russia;
7. Venezuela;
8. territories subject to comprehensive sanctions regimes as at the Effective Date: Crimea, Donetsk People’s Republic, Luhansk People’s Republic, Zaporizhzhia Oblast, Kherson Oblast (annexed/occupied territories of Ukraine under OFAC, EU, and UN sanctions);
9. Belarus;
10. Libya, Sudan, Somalia, Iraq, Yemen, Mali, Lebanon — to the extent required by applicable UN, EU, OFAC, and UK HMT sanctions regimes;
11. any other country or territory subject to comprehensive sanctions administered by the UN Security Council, the European Union, OFAC, or HM Treasury.

8.2 FATF Grey List — Enhanced Precautions. In respect of Participants from jurisdictions included in the FATF “Jurisdictions under Increased Monitoring” (grey list), mandatory Enhanced Due Diligence (EDD) applies in accordance with §7 of this Framework. Inclusion on the FATF grey list is not, of itself, grounds for automatic refusal of Services, provided that EDD is completed successfully. The current list is published on the official FATF website: https://www.fatf-gafi.org/.

8.3 Additional Company-Imposed Restrictions. In accordance with §7.17 of the T&C, the Company also does not provide Services in the following jurisdictions for commercial or regulatory reasons: United States of America — except as expressly permitted by the Company in accordance with applicable state law; Canada — except as expressly permitted by the Company. The full and current list of restricted jurisdictions is set out in §7.17 of the T&C, published on neomaaafunded.com.

8.4 Participant Responsibility. In accordance with §7.17(d) of the T&C, the Participant bears sole responsibility for compliance with the applicable laws of their jurisdiction. Registering for or using the Services from a prohibited jurisdiction constitutes a material breach of the T&C and will result in immediate account suspension without prior notice in accordance with §7.17(d) of the T&C.

8.5 Monitoring and Updates. The Company maintains ongoing monitoring of sanctions and regulatory developments and updates the list of prohibited jurisdictions upon each change to the UN, EU, OFAC, and HM Treasury sanctions regimes, as well as following each FATF plenary session (no less than three times per year).

---

§9 Sanctions Screening

9.1 Applicable Sanctions Lists. The Company screens all Participants against the following lists:

1. UN Security Council Consolidated List — all sanctions resolutions adopted under Chapter VII of the UN Charter;
2. EU Consolidated Sanctions List;
3. OFAC SDN List (Specially Designated Nationals and Blocked Persons List), together with OFAC Sectoral Sanctions Identifications (SSI);
4. UK OFSI Consolidated List (HM Treasury Financial Sanctions Consolidated List);
5. UAE Local Terrorist List, together with the sanctions lists administered by the UAE Executive Office for AML/CFT.

9.2 PEP Screening. Screening for Politically Exposed Person (PEP) status is carried out using Dow Jones Risk & Compliance, WorldCheck, or equivalent databases integrated into the Sumsub platform, as well as through public sources: official government registers, international organisation databases, and media publications.

9.3 Screening Frequency. Screening is conducted:

1. at every onboarding of a new Participant, prior to the provision of access to the Services;
2. upon every update to the applicable sanctions lists;
3. prior to every Benefit Program disbursement;
4. upon any change to the Participant’s personal data;
5. upon the addition of a new payment method or withdrawal details.

9.4 Procedure Upon Identification of a Sanctions Match. Where a match or potential match with any applicable sanctions list is identified:

1. the transaction and account are immediately frozen without notifying the Participant;
2. the Head of Compliance analyses the match within 24 hours to determine whether it is a true match or a false positive;
3. where the result is a false positive: the finding is recorded in the customer file with written justification;
4. where a true match is confirmed: the funds remain frozen; a report is submitted to the relevant sanctions authority within the legally prescribed timeframe; no unfreeze is effected without the

explicit written authorisation of the competent sanctions authority; the Head of Compliance notifies Senior Management.

9.5 Prohibition. It is strictly prohibited to unfreeze the funds of a sanctioned person without the written authorisation of the relevant sanctions authority (OFAC, the EU, or the relevant competent authority).

---

§10 Transaction Monitoring

10.1 Monitoring System. The Company operates a multi-layered transaction monitoring system combining automated analysis with manual review by members of the compliance team.

10.2 Automated Triggers. The monitoring system generates alerts upon identification of, among others, the following patterns:

1. Structuring: a pattern of payments structured so as to remain below established thresholds or to avoid verification requirements.
2. Rapid in/out: immediate movement of funds following their receipt, without any apparent economic purpose.
3. Geographic mismatch: payment transactions originating from jurisdictions incompatible with the Participant’s KYC data.
4. Third-party payments: receipt of funds from persons who are not the verified account holder, or requests for withdrawal to details that do not belong to the Participant.
5. [Intentionally reserved];
6. Shared payment details across different accounts: common payment methods or withdrawal destinations shared between different accounts, in accordance with §7.12(C)(vi) of the T&C.
7. Use of anonymisation tools: use of VPN, Tor, or proxy services in breach of §7.10.1(l) of the T&C.

10.3 Behavioural Trading Activity Monitoring. In addition to transaction monitoring, the Company conducts behavioural monitoring of Participants’ trading activity to identify patterns that may indicate coordinated or fraudulent conduct with AML significance: matched trades, group trading / coordinated activity, account sharing, and IP/geolocation inconsistencies in accordance with §7.10.1(l) and (m) of the T&C.

10.4 Thresholds. Specific numerical transaction-monitoring thresholds are not disclosed in this public version of the Framework in order to preserve the confidentiality of the Company’s AML controls. Triggers are applied on a combined basis: threshold AND behavioural.

10.5 Manual Review. All monitoring system alerts are subject to manual review by an authorised member of the compliance team. Indicators not accounted for by legitimate grounds are escalated to the Head of Compliance for assessment of whether a Suspicious Activity Escalation Report (SAER) should be prepared in accordance with §11 of this Framework.

10.6 Typical Red Flags. Red flags requiring the immediate attention of the compliance team include, among others:

- a Participant’s refusal to provide KYC documentation without reasonable explanation;
- documents showing signs of alteration or inconsistency;
- excessive concern by a Participant about monitoring procedures;
- a transactional profile materially inconsistent with the declared source of funds;
- the Participant’s IP address at login does not match the jurisdiction declared at KYC;

- mirror-trading operations between accounts followed by Benefit Program disbursements to both accounts;
- repeated chargebacks or payment disputes followed by fresh account funding.

---

§11 Internal Suspicious Activity Escalation

11.1 Definition. A transaction or account is deemed to give rise to suspicious-activity grounds where the Company has knowledge, suspicion, or reasonable grounds to suspect that the transaction or funds are connected with criminal activity, money laundering, terrorism financing, sanctions evasion, or fraud, regardless of the transaction amount. Where the Company subsequently determines that any external reporting obligation arises under applicable law, the Company shall comply with that obligation in accordance with the procedures of the competent authority.

11.2 Head of Compliance Responsibilities. The Head of Compliance of the Company bears sole responsibility for:

1. receiving internal suspicious-activity disclosures from Company employees;
2. evaluating each internal disclosure and preparing a Suspicious Activity Escalation Report (SAER) for Senior Management where escalation is warranted;
3. assessing whether any external reporting obligation arises under applicable law, and where such obligation arises, complying with it in accordance with the procedures of the competent authority;
4. documenting all decisions, including decisions not to escalate or not to make any external report, with written justification.

11.3 Internal Escalation Process.

Step 1 — Detection: an employee or automated system identifies one or more red flags.

Step 2 — Escalation: within the timeframe prescribed by internal procedures, the employee submits to the Head of Compliance a written internal suspicious-activity disclosure describing the identified red flags and the measures already taken.

Step 3 — Compliance Review: the Head of Compliance reviews the submitted materials. Where necessary, the Head of Compliance requests additional information from employees or from the Sumsub provider.

Step 4 — Decision: the Head of Compliance makes one of two decisions: to prepare a Suspicious Activity Escalation Report (SAER) for Senior Management, or to decline to do so with written justification.

Step 5 — Escalation and external reporting (if applicable): the Head of Compliance escalates the Suspicious Activity Escalation Report (SAER) to Senior Management, and assesses whether any external reporting obligation arises under applicable law. Where such obligation arises, the Head of Compliance ensures timely compliance in accordance with the procedures of the competent authority.

Step 6 — Documentation: the entire process is documented. Internal reports and correspondence are retained for not less than five (5) years in accordance with §12 of this Framework.

11.4 Timeframes. A Suspicious Activity Escalation Report (SAER) is prepared and escalated to Senior Management without undue delay from the moment at which the Company personnel knew, suspected, or had reasonable grounds to suspect grounds for escalation. Any external

reporting obligation arising under applicable law is complied with within the timeframe prescribed by that law.

11.5 Tipping-Off. The Company observes the tipping-off prohibition reflected in Article 25 of UAE Federal Decree-Law No. 10 of 2025 as voluntary best practice. The Company, its employees, directors, and agents shall refrain from disclosing to the Participant or to any third party the fact that internal suspicious-activity escalation has occurred, or that any external report has been or may be made, or that an investigation is being conducted in connection with suspicions of money laundering, terrorism financing, fraud, or sanctions evasion, except where such disclosure is required by applicable law.

11.6 Asset Freezing Upon Suspicious Activity. Upon the preparation of a Suspicious Activity Escalation Report (SAER) or upon identification of a sanctions match, the Company may freeze the Participant's account and suspend all Benefit Program disbursements. Such freezing does not constitute a breach of the Company's obligations to the Participant; any delays to disbursements arising from lawful AML or sanctions requirements do not give rise to liability on the part of the Company, in accordance with §1.5(t)(v) of the T&C.

---

§12 Record-Keeping

12.1 General Principle. In accordance with Article 16(1)(f) of the AML FDL and Financial Action Task Force (FATF) Recommendations (Recommendation 11), the Company retains all documents and records relating to business relationships with Participants and to all transactions for a minimum of five (5) years from the end of the business relationship or the date of the transaction. This retention period is consistent with §8(a) of the Privacy Policy.

12.2 Records Subject to Retention. The following records are subject to mandatory retention, including:

1. identity documents (KYC/CDD): passports, identity cards, proof-of-address documents, Sumsub verification results, biometric check screenshots, and PEP-status screening results;
2. EDD documents: Source of Funds (SOF) and Source of Wealth (SOW) declarations, documentary evidence of source of funds, and senior management EDD approval decisions;
3. transaction records: payment history, Benefit Program disbursement history, and payment-processing logs;
4. sanctions-screening records: results of automated and manual screening in respect of each Participant and each transaction, including notations of matches, potential matches, and their resolution;
5. internal Suspicious Activity Escalation Reports (SAERs) and compliance investigation correspondence;
6. any external reports made to competent authorities under applicable law, where such obligation arose, and receipts confirming their submission;
7. records of periodic customer-file reviews;
8. records of correspondence with Participants relating to KYC/AML procedures.

12.3 Technical Storage Requirements. All records are stored in a secure format (AES-256 encryption at rest, TLS 1.2 or higher in transit) in accordance with §29.9 of the T&C. Records must be accessible to regulatory authorities and the UAE FIU upon first request. Early destruction of records before the expiry of the applicable retention period is prohibited. Upon receipt of a request from a regulator or the UAE FIU, the retention period is suspended until the conclusion of the relevant proceedings.

12.4 Extended Retention Period. Where judicial, regulatory, or AML proceedings are ongoing in respect of a Participant, the retention period for the relevant records is extended until the conclusion of those proceedings plus one (1) year.

12.5 Retention Periods Summary:

- KYC/AML records: minimum 5 years from end of business relationship or date of transaction (UAE FDL 20/2018 + FATF Rec. 11)
- Transaction records: minimum 7 years
- SAER records and any external reports: minimum 5 years after preparation or submission

---

§13 Training and Awareness

13.1 Mandatory Annual Training. In accordance with the requirements of the AML FDL and international best practice, all Company employees with access to customer data, payment operations, or AML/CFT procedures are required to complete AML/CFT/CPF training annually.

13.2 Training Programme. The mandatory training programme covers, among other subjects:

1. the AML/CFT/CPF regulatory framework (the AML FDL, UAE Cabinet Decision No. 134 of 2025, Financial Action Task Force (FATF) Recommendations);
2. money-laundering and terrorism-financing typologies characteristic of the prop-trading industry;
3. the Company’s KYC/CDD/EDD procedures;
4. red flags and escalation procedures;
5. sanctions compliance and screening procedures;
6. the tipping-off prohibition (where applicable) and Suspicious Activity Escalation Report (SAER) procedures, including assessment of any external reporting obligations under applicable law;
7. internal whistleblowing channels;
8. updates to applicable legislation and regulatory practice.

13.3 Specialist Training. The Compliance team and the Head of Compliance undergo an extended specialist training programme, including training on the use of the Sumsub platform, interpretation of sanctions-screening results, and assessment of any external reporting obligations arising under applicable law.

13.4 Training Documentation. All training sessions are documented (date, attendees, programme content, duration). Training records are retained for not less than five (5) years. The Head of Compliance maintains a register of each employee’s training completion.

13.5 New Employees. New employees are required to complete introductory AML/CFT training within thirty (30) days of their commencement date.

---

§14 Governance and Contacts

14.1 Compliance Governance Structure. The Company has established the following governance structure:

1. Head of Compliance: coordinates the customer due diligence, sanctions screening, and suspicious-activity escalation procedures set out in this Framework; receives and evaluates internal suspicious-activity disclosures; prepares Suspicious Activity Escalation Reports (SAERs) for Senior Management; assesses whether any external reporting obligation arises under

applicable law and ensures compliance therewith; organises staff training and independent reviews.

2. Senior Management: approves this Framework and any amendments; approves the onboarding of higher-risk Participants (EDD); receives the Head of Compliance's annual report on the effectiveness of the Framework.
3. Board of Directors: receives the results of the independent annual review of this Framework directly from the reviewer; bears ultimate responsibility for the proper functioning of the Company's compliance programme.

Accountability chain: Head of Compliance → Senior Management → Board of Directors.

14.2 Independent Annual Review. The Company commissions an independent external review of this Framework no less than once per year. The reviewer must be independent of the Company's operational management and must possess demonstrated competence in customer due diligence, AML/sanctions compliance, and consumer protection. The review results are reported directly to the Board of Directors. The Head of Compliance is required to develop a remediation plan for identified deficiencies within thirty (30) days of receipt of the review report.

14.3 Annual Framework Review. This Framework is reviewed no less than once per year, and upon every material change in applicable legislation or the Company's business model.

14.4 Whistleblower Protection. Company employees who in good faith report suspicious transactions or compliance breaches internally or to a competent authority are protected against all forms of retaliation, adverse action, and discrimination, in accordance with applicable UAE law.

14.5 Contact Details. For all queries relating to this Framework, customer due diligence procedures, or sanctions compliance, Participants and interested parties may contact:

Customer due diligence, sanctions, and compliance enquiries: compliance@neomaaafunded.com

General enquiries and support: support@neomaaafunded.com

Registered address: Neom Triple A Information Technology LLC The Binary by Omniyat, Office 2114 Business Bay, Dubai, UAE

Website: neomaaafunded.com

14.6 Framework Amendments. The Company reserves the right to amend this Framework at any time. The current version of the Framework is published on neomaaafunded.com. Material amendments take effect in accordance with the procedure set out in §1.3 of the T&C.

This Customer Due Diligence & AML/Sanctions Framework is effective from 24 September 2026. This Framework supersedes all previous versions of the AML / KYC Policy or equivalent document published by Neom Triple A Information Technology LLC under the brand NEOMAAA Funded.

Customer Due Diligence & AML/Sanctions Framework v4.0.1 | Neom Triple A Information Technology LLC (NEOMAAA Funded) | Publication Date: 24 September 2026