Marco de Diligencia Debida del Cliente y AML/Sanciones v4.0.1 (Customer Due Diligence & AML/ Sanctions Framework v4.0.1)

Alineado con los T&C y la Política de Privacidad | Fecha de Publicación (Publication Date): 24 de septiembre de 2026

El presente Marco de Diligencia Debida del Cliente y AML/Sanciones (Customer Due Diligence & AML/Sanctions Framework) (el “Marco” (Framework)) constituye la versión canónica autorizada en lengua inglesa del marco de diligencia debida del cliente, prevención del blanqueo de capitales (AML, Anti-Money Laundering) y cumplimiento de sanciones adoptado por Neom Triple A Information Technology LLC, que opera bajo la marca NEOMAAA Funded. El presente Marco se publica como compromiso voluntario con elevados estándares de protección al consumidor, prevención del fraude, cumplimiento de sanciones y conducta empresarial ética, y se aplica a las actividades de la Sociedad como prestadora de servicios de evaluación mediante operativa simulada. El presente Marco sustituye a todas las versiones previamente publicadas de la Política AML / KYC (Conocimiento del Cliente, Know Your Customer) de NEOMAAA Funded.

---

§1 Declaración del Marco

1.1 Neom Triple A Information Technology LLC (marca: NEOMAAA Funded, en lo sucesivo la “Sociedad” (Company)) asume un compromiso incondicional de cumplir todas las leyes y normativas aplicables a sus actividades como prestadora de servicios de evaluación mediante operativa simulada (simulated trading evaluation services), incluidas las obligaciones en materia de protección al consumidor, prevención del fraude, cumplimiento de sanciones y cumplimiento fiscal, y de observar, como buena práctica voluntaria y en la medida aplicable, los principios derivados de los estándares internacionales AML (Prevención del Blanqueo de Capitales) / CFT (Lucha contra la Financiación del Terrorismo, Combating the Financing of Terrorism). Este compromiso es fundamental para la operación lícita de la Sociedad y para mantener la confianza de los Participantes (Participants), socios bancarios y reguladores.

1.2 La Sociedad reconoce que sus actividades, que comportan la recepción de pagos de los Participantes en el marco de programas de evaluación mediante operativa simulada, así como el desembolso de premios bajo el Programa de Beneficios (Benefit Program) conforme a los T&C, conllevan riesgos de aprovechamiento en esquemas de blanqueo de capitales (money laundering) o financiación del terrorismo (terrorist financing). El presente Marco establece medidas para identificar, evaluar y mitigar tales riesgos.

1.3 El presente Marco se aplica a todos los Participantes (según se definen en el §1.5(c) de los T&C), a todos los empleados, administradores, contratistas y agentes de la Sociedad, y a todas las operaciones financieras vinculadas a las actividades de la Sociedad. La Sociedad implementa el presente Marco mediante un enfoque basado en el riesgo (Risk-Based Approach, RBA), calibrando la intensidad de las medidas AML/CFT al nivel de riesgo identificado.

1.4 El presente Marco forma parte de un conjunto documental integrado que comprende los T&C, la Política de Privacidad y la Política de Cookies. En caso de conflicto entre el presente Marco y los T&C, prevalecerán las disposiciones de los T&C.

---

§2 Ámbito y Entidad Jurídica

2.1 Entidad Jurídica Controladora. El presente Marco se aplica a las operaciones de la siguiente entidad jurídica:

Denominación legal completa: Neom Triple A Information Technology LLC Marca: NEOMAAA Funded Domicilio social: The Binary by Omniyat, Office 2114, Business Bay, Dubai, UAE Sitio web: neomaaafunded.com

2.2 Ámbito del Marco. El presente Marco se aplica:

1. a todos los Participantes con independencia de su jurisdicción de residencia o de su ciudadanía;
2. a todas las transacciones de recepción de pagos por Cuentas de Evaluación Financiada (Funded Evaluation Accounts) (§1.5(f) de los T&C) y Cuentas de Evaluación Exprés (Express Evaluation Accounts) (§1.5(m) de los T&C), así como a todos los desembolsos del Programa de Beneficios conforme al §17 de los T&C;
3. a todos los empleados, administradores, contratistas y representantes de la Sociedad;
4. a todos los terceros que actúen por cuenta o en interés de la Sociedad en relación con la recepción o el desembolso de fondos.

2.3 Clasificación de la Actividad. La Sociedad es una prestadora de servicios de evaluación mediante operativa simulada. La Sociedad no es una entidad financiera autorizada, entidad de crédito, bróker, dealer, asesor de inversiones ni proveedor de servicios sobre activos virtuales (virtual-asset service provider) en el sentido de ninguna legislación aplicable, y no mantiene fondos, valores ni inversiones de clientes. La Sociedad observa el marco que se establece a continuación como cuestión de compromiso voluntario con elevados estándares de protección al consumidor, prevención del fraude y cumplimiento de sanciones, con independencia de la clasificación de sus actividades bajo el UAE Federal Decree-Law No. 10 of 2025 on Anti-Money Laundering, Combating the Financing of Terrorism, and Financing of Illegal Organisations o la Cabinet Decision No. 134 of 2025.

2.4 Principio del Estándar Más Elevado. Cuando los requisitos aplicables de distintas jurisdicciones entren en conflicto, la Sociedad aplicará el estándar más exigente que sea compatible con sus operaciones como entidad jurídica constituida en los Emiratos Árabes Unidos (UAE).

---

§3 Marco Regulatorio

3.1 Marco Regulatorio de los UAE — En la Medida Aplicable. La Sociedad toma en consideración los siguientes instrumentos regulatorios de los UAE como parte de su marco voluntario AML (Prevención del Blanqueo de Capitales) / sanciones, en la medida aplicable a sus actividades:

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) (en lo sucesivo, “UAE FDL 20/2018” o “AML FDL”) — el principal instrumento legislativo de los UAE que establece los principios de Diligencia Debida del Cliente (CDD, Customer Due Diligence), Diligencia Debida Reforzada (EDD, Enhanced Due Diligence),

evaluación de actividades sospechosas y conservación de registros; observado por la Sociedad como buena práctica voluntaria;

2. Cabinet Decision No. 10 of 2019 concerning the Implementing Regulation of UAE Federal Decree-Law No. 20 of 2018 (sustituida por la Cabinet Decision No. 134 of 2025, en vigor desde el 14 de diciembre de 2025) — que establece los requisitos procedimentales detallados para la identificación del cliente, la gestión del riesgo y la elaboración de informes;
3. UAE Federal Decree-Law No. 26 of 2021 amending certain provisions of Federal Decree-Law No. 20 of 2018 — que amplía la categoría de sujetos obligados y refuerza las sanciones;
4. UAE Federal Law No. 7 of 2014 on Combating Terrorism Offences — que establece el concepto de financiación del terrorismo (terrorist financing) y las obligaciones conexas de lucha contra la financiación;
5. UAE Federal Decree-Law No. 34 of 2021 on Combating Rumours and Cybercrimes — aplicable a la dimensión digital de las actividades de la Sociedad, incluida su plataforma en línea y las transacciones electrónicas (este instrumento derogó y sustituyó al UAE Federal Law No. 5 of 2012 con efectos desde el 2 de enero de 2022);
6. UAE Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data (la "UAE PDPL") — que establece el marco jurídico para el tratamiento de datos personales en los UAE, incluidas las bases jurídicas, los derechos del interesado, las obligaciones de seguridad y los requisitos de transferencia transfronteriza aplicables al tratamiento por la Sociedad de los datos personales recogidos, generados o conservados para fines de AML/CFT/CPF (Lucha contra la Financiación de la Proliferación, Counter-Proliferation Financing) (incluidos la CDD, la EDD, la monitorización continua, la documentación del SAER y el período de conservación de registros); y
7. UAE Cabinet Decision No. 58 of 2020 on the Regulation of the Beneficial Owner Procedures — que establece las obligaciones de las personas jurídicas en los UAE de identificar, registrar y comunicar a sus titulares reales (beneficial owners), y que aporta la definición operativa de Titular Real (Beneficial Owner) utilizada en el §4.1 del presente Marco.

3.2 Estándares Internacionales y Regímenes de Sanciones. El presente Marco toma asimismo en consideración:

1. las Financial Action Task Force (FATF) Recommendations — los estándares internacionales para la lucha contra el blanqueo de capitales, la financiación del terrorismo y la financiación de la proliferación (proliferation financing), en particular las Recomendaciones 1, 10, 11, 12, 15, 19 y 20;
2. la UN Security Council Consolidated List — incluida la lista consolidada de personas, entidades y jurisdicciones sometidas a sanciones adoptadas en virtud del Capítulo VII de la Carta de la ONU;
3. los programas de sanciones administrados por la U.S. Department of the Treasury Office of Foreign Assets Control (OFAC), la European Union, el HM Treasury (United Kingdom) y la UAE Executive Office for AML/CFT.

3.3 Cambios en el Marco Regulatorio. La Sociedad monitoriza los cambios en la legislación aplicable y se compromete a actualizar el presente Marco con razonable celeridad tras la entrada en vigor de cualquier modificación sustancial. De conformidad con el §1.3(a)(iv) de los T&C, los cambios exigidos por obligaciones relacionadas con AML/CFT surten efecto inmediatamente desde su publicación.

---

§4 Definiciones

4.1 A los efectos del presente Marco, se aplican las siguientes definiciones:

“Blanqueo de Capitales” (Money Laundering) — actos según se definen en el Artículo 2 del AML FDL: recibir, adquirir, poseer, utilizar, transferir o transformar fondos o bienes, cuando la persona sepa o deba saber que constituyen producto del delito, realizados con la intención de ocultar o disimular su origen ilícito, o de asistir a cualquier persona implicada en un delito previo a eludir las consecuencias jurídicas del mismo.

“Financiación del Terrorismo” (Financing of Terrorism) — la provisión o recaudación de fondos con la intención, o con el conocimiento, de que serán utilizados, total o parcialmente, para financiar actividades de las prescritas por la UAE Federal Law No. 7 of 2014 on Combating Terrorism Offences, o para financiar a personas u organizaciones que participen en actividades terroristas.

“Titular Real” (Beneficial Owner) (Titular Real Último, Ultimate Beneficial Owner, UBO) — la persona física que en último término posee o controla una entidad jurídica u otra estructura que sea cliente, o la persona física por cuya cuenta se realiza una transacción, conforme a la definición establecida en la UAE Cabinet Decision No. 58 of 2020 on Beneficial Ownership Registers.

“Persona Políticamente Expuesta (PEP, Politically Exposed Person)” — la persona física que desempeñe o haya desempeñado una función pública relevante (jefe de Estado o de gobierno, ministro, alto cargo militar, director de una empresa de titularidad estatal, dirigente de una organización internacional, etc.), así como los familiares próximos y los allegados conocidos de dicha persona.

“Diligencia Debida del Cliente (CDD)” — el conjunto de medidas estándar de identificación y verificación aplicadas respecto de un cliente, incluida la determinación del origen de los fondos (source of funds), la evaluación de la relación de negocio y de su finalidad.

“Diligencia Debida Reforzada (EDD)” — medidas de verificación reforzadas aplicadas a clientes de mayor riesgo, incluidas las Personas Políticamente Expuestas (PEPs), los clientes de jurisdicciones de mayor riesgo y otras personas especificadas en el §7 del presente Marco.

“Diligencia Debida Simplificada (SDD, Simplified Due Diligence)” — medidas de verificación reducidas aplicadas a clientes de bajo riesgo demostrable, siempre que se cumplan todas las condiciones establecidas en el presente Marco.

“Informe de Escalado de Actividad Sospechosa (SAER, Suspicious Activity Escalation Report)” — un informe interno escrito preparado por el personal de la Sociedad que documenta los motivos para sospechar que una transacción o cuenta está vinculada con blanqueo de capitales, financiación del terrorismo, fraude, elusión de sanciones u otra actividad ilícita, escalado a la Alta Dirección (Senior Management) para su evaluación y para cualquier actuación ulterior exigida por la legislación aplicable.

“Responsable de Cumplimiento (Head of Compliance)” — el directivo de la Sociedad responsable de coordinar los procedimientos de diligencia debida del cliente, filtrado de sanciones (sanctions screening) y escalado interno de actividades sospechosas establecidos en el presente Marco.

“Participante” — persona física o entidad jurídica registrada para utilizar los Servicios de NEOMAAA Funded de conformidad con el §1.5(c) de los T&C.

“Cuenta de Evaluación Financiada” — una cuenta simulada con saldo virtual proporcionada a un Participante que haya completado satisfactoriamente la Fase de Evaluación, en el sentido del §1.5(f) de los T&C.

“Cuenta de Evaluación Exprés” — una Cuenta de Evaluación Financiada de fase única conforme a lo previsto en el §1.5(m) de los T&C.

“Nivel de Reconocimiento (Recognition Level)” — el parámetro contractual seleccionado por el Participante al adquirir una Cuenta de Evaluación Financiada, que determina el Coeficiente de Recompensa (Reward Coefficient) y el Capital Simulado Inicial (Initial Simulated Capital), en el sentido del §1.5(y) de los T&C.

---

§5 Enfoque Basado en el Riesgo

5.1 Principio de Proporcionalidad. De conformidad con la FATF Recommendation 1 y el AML FDL, la Sociedad aplica medidas de Diligencia Debida del Cliente (CDD), Diligencia Debida Reforzada (EDD) y monitorización proporcionadas al nivel de riesgo identificado. La intensidad de las medidas se establece en proporción al riesgo y no se aplica de manera uniforme a todos los clientes.

5.2 Factores de Evaluación de Riesgo. La Sociedad evalúa los siguientes factores de riesgo respecto de cada Participante y de la relación de negocio con dicho Participante:

1. Riesgo del Cliente (Customer Risk): tipo de cliente (persona física, entidad jurídica, estructura societaria), ocupación, condición de Persona Políticamente Expuesta (PEP, Politically Exposed Person) o afiliación a PEP, historial de retrocesiones (chargebacks) o disputas de pago, conducta durante el KYC (Conocimiento del Cliente, Know Your Customer).
2. Riesgo Geográfico (Geographic Risk): país de residencia y de ciudadanía del Participante, país de origen de los fondos, coherencia de la dirección IP con los datos KYC, clasificación de la jurisdicción bajo las listas de la FATF, listas de Terceros Países de Alto Riesgo de la UE o listas de sanciones (sanctions lists) aplicables.
3. Riesgo del Producto (Product Risk): tipo de cuenta utilizada (Cuenta de Evaluación Financiada, Cuenta de Evaluación Exprés), importes agregados de pagos y de desembolsos del Programa de Beneficios, frecuencia y patrón de las transacciones, Nivel de Reconocimiento seleccionado.
4. Riesgo del Canal (Channel Risk): naturaleza de la interacción (a distancia / sin presencia física), uso de herramientas de anonimización (VPN, proxy, Tor) en infracción del §7.10.1(l) de los T&C, discrepancia entre la dirección IP y la jurisdicción declarada en el KYC.

5.3 Niveles de Diligencia Debida. Sobre la base de la evaluación agregada de los factores de riesgo, la Sociedad aplica uno de los tres niveles de diligencia debida:

1. Diligencia Debida Estándar del Cliente (Standard CDD) — para Participantes con un nivel de riesgo bajo o moderado. Incluye la verificación de identidad a través de Sumsub, el filtrado contra listas de sanciones y listas de PEP, y la evaluación del origen de los fondos.
2. Diligencia Debida Reforzada (EDD) — para Participantes de mayor riesgo. Se aplica en las circunstancias especificadas en el §7 del presente Marco. Incluye documentación adicional, una declaración de origen del patrimonio (source of wealth) y aprobación de la alta dirección.
3. Diligencia Debida Simplificada (SDD) — aplicada exclusivamente respecto de entidades jurídicas cotizadas en mercados regulados de jurisdicciones con un régimen AML adecuado, y respecto de organismos gubernamentales, en ausencia de cualquier indicador de riesgo.

5.4 Documentación. La evaluación de riesgo (risk assessment) de cada Participante se documenta en el expediente del cliente. Cualquier anulación manual de una evaluación de riesgo requiere justificación escrita y aprobación del Responsable de Cumplimiento de la Sociedad.

5.5 Revisión de la Evaluación de Riesgo. La evaluación de riesgo de cada Participante se revisa ante cualquiera de los siguientes hechos: cualquier cambio sustancial en el volumen o el

comportamiento de las transacciones; una solicitud de desembolso del Programa de Beneficios; la identificación de señales de alerta (red flags); y, en todo caso, no menos de una vez al año para los Participantes de mayor riesgo.

---

§6 Diligencia Debida del Cliente (CDD)

6.1 Desencadenantes del KYC. La Sociedad realiza o actualiza la verificación KYC (Conocimiento del Cliente, Know Your Customer) en las siguientes circunstancias:

1. al abrir una nueva cuenta o al efectuarse el primer pago por cualquier tipo de Cuenta Prop;
2. ante una primera solicitud de desembolso del Programa de Beneficios;
3. [Reservado intencionalmente];
4. ante la identificación de actividad inusual, señales de alerta o un cambio en el perfil de riesgo del Participante;
5. ante una solicitud dirigida al Participante al amparo del §7.10.1(m) de los T&C en relación con una posible implicación de terceros;
6. ante la revisión periódica programada del expediente del cliente (Participantes de mayor riesgo: cada 6 meses; riesgo medio: cada 12 meses; menor riesgo: cada 36 meses).

6.2 Datos Recogidos. Como parte de la Diligencia Debida del Cliente (CDD) estándar, la Sociedad recoge los siguientes datos y documentos:

1. documento de identidad: un pasaporte válido (página de la fotografía y de los datos biográficos), un documento nacional de identidad de la UE o un permiso de conducir (en jurisdicciones donde se acepte como documento de identificación satisfactorio);
2. verificación biométrica mediante selfie: una grabación de vídeo dinámica (liveness check) o un selfie estático con el documento de identidad, para evitar el uso de documentos de terceros y cuentas con deepfake;
3. prueba del domicilio: una factura de suministro, extracto bancario, carta oficial de la administración o contrato de arrendamiento emitido como máximo tres meses antes de su presentación;
4. Declaración de Origen de los Fondos (Source of Funds Declaration): obligatoria cuando el volumen agregado de pagos o desembolsos supere los umbrales fijados por la Sociedad (los umbrales específicos no se divulgan en esta versión pública del Marco de conformidad con los principios de confidencialidad de los controles AML de la Sociedad).

6.3 Proveedor de KYC/IDV. La Sociedad lleva a cabo la verificación de identidad y los controles biométricos a través de la plataforma Sumsub (Sum and Substance Ltd / Sumsub Group). Sumsub es el proveedor de KYC/AML de la Sociedad, referido en la categoría de destinatarios (ii) del §6 de la Política de Privacidad. Los datos personales se transfieren a Sumsub al amparo de un contrato escrito de tratamiento de datos que incorpora Cláusulas Contractuales Tipo (SCCs, Standard Contractual Clauses) de conformidad con la Commission Implementing Decision (EU) 2021/914. La lista completa de proveedores actuales de KYC/IDV está disponible previa solicitud en privacy@neomaaafunded.com.

6.4 Filtrado en Tiempo Real de PEP y Sanciones. En el momento del KYC, cada Participante es sometido a:

1. filtrado en tiempo real contra las listas vigentes de Personas Políticamente Expuestas (PEP) (Dow Jones Risk & Compliance, WorldCheck o bases de datos equivalentes integradas a través de Sumsub);
2. filtrado contra las listas de sanciones establecidas en el §9 del presente Marco;

3. filtrado de información adversa en medios (adverse media) contra las bases de datos pertinentes.

El filtrado se realiza tanto en la incorporación (onboarding) como de manera continua. Cuando se identifique una coincidencia o posible coincidencia, se aplicará el procedimiento descrito en el §9 del presente Marco.

6.5 Verificación del Número de Teléfono. De conformidad con el §6.1 de los T&C, el Participante debe completar la verificación del número de teléfono mediante código SMS en el plazo de siete (7) días naturales desde el primer pago o el registro de la cuenta. La falta de verificación dará lugar a un acceso restringido a las funcionalidades de la plataforma, incluida la creación de nuevas cuentas y las solicitudes de desembolso del Programa de Beneficios.

6.6 Cuentas de Sorteo (Giveaway Accounts). Los Participantes que hayan recibido cuentas a través de sorteos, rifas u ofertas de socios deberán completar la verificación KYC íntegra antes de que se tramite cualquier solicitud de desembolso del Programa de Beneficios, de conformidad con el §7.12(B)(v) de los T&C.

6.7 Clientes Corporativos. Cuando se registre una entidad jurídica, la Sociedad solicitará adicionalmente: un certificado de constitución, una escritura de constitución (Memorandum of Association), documentos que acrediten la facultad del representante autorizado y documentos de la estructura de titularidad que revelen a todos los Titulares Reales Últimos (UBO) que ostenten más del 25 % de las acciones o de los derechos de voto (de conformidad con la UAE Cabinet Decision No. 58 of 2020). No se aceptarán para prestación de Servicios las estructuras en las que el titular real no pueda identificarse.

6.8 Consecuencias del Incumplimiento del KYC. De conformidad con el §6.4 de los T&C y el §6.4.2 de los T&C, el incumplimiento por parte del Participante de la verificación KYC dará lugar a un acceso restringido a los Servicios y podrá dar lugar a la terminación con arreglo al §15 de los T&C.

---

§7 Diligencia Debida Reforzada (EDD)

7.1 Desencadenantes Obligatorios de EDD. La Diligencia Debida Reforzada (EDD, Enhanced Due Diligence) es obligatoria en las siguientes circunstancias:

1. condición de PEP (Persona Políticamente Expuesta, Politically Exposed Person) identificada o sospechada: el Participante es una PEP, un familiar de una PEP o un allegado conocido de una PEP;
2. el Participante es residente o ciudadano de una jurisdicción incluida en la lista de la FATF “Call for Action” o en la lista de la Comisión Europea de terceros países de alto riesgo;
3. se ha identificado una conexión o posible conexión con una persona o entidad sancionada;
4. se ha identificado un patrón de transacciones inusual: estructuración (structuring) de pagos, retirada inmediata de fondos tras su recepción, pagos desde datos de pago que no se corresponden con la información verificada del Participante;
5. discrepancia entre la dirección IP o la geolocalización y la jurisdicción declarada, conforme al §7.10.1(l) de los T&C;
6. un elevado valor agregado de desembolsos del Programa de Beneficios para un mismo Participante;
7. identificación de coordinación de la actividad de operativa entre múltiples cuentas conforme al §7.12 de los T&C;
8. cualquier otro factor que indique un mayor nivel de riesgo a juicio del Responsable de Cumplimiento.

7.2 Medidas Adicionales de EDD. La Diligencia Debida Reforzada (EDD) incluye las siguientes medidas adicionales por encima de la Diligencia Debida del Cliente (CDD) estándar:

1. obtención de la aprobación de la alta dirección con carácter previo al inicio o a la continuación de una relación de negocio con un Participante sujeto a EDD;
2. obtención de una Declaración de Origen del Patrimonio (Source of Wealth Declaration) con prueba documental de soporte (declaraciones tributarias, contrato de trabajo, documentos de operaciones inmobiliarias, etc.);
3. obtención de una Declaración de Origen de los Fondos detallada para cada transacción sustancial;
4. verificación de documentos a través de fuentes independientes adicionales;
5. monitorización continua reforzada de la relación de negocio con el Participante;
6. un ciclo de revisión periódica acortado del expediente del cliente (cada seis (6) meses en lugar de los 12 o 36 meses estándar).

7.3 Documentación de la EDD. Todas las medidas de Diligencia Debida Reforzada (EDD) se documentan en el expediente del cliente, registrando: la fecha en que se llevó a cabo la EDD; los motivos para aplicarla; los resultados de cada medida; el nombre del directivo que realizó la EDD; y la decisión adoptada tras la EDD, con la firma del Responsable de Cumplimiento.

7.4 Prohibición de Prestación de Servicios sin Completarse la EDD. Todos los desembolsos del Programa de Beneficios quedan suspendidos en tanto no se complete el procedimiento de EDD y se adopte una decisión positiva por el Responsable de Cumplimiento. Dicha suspensión no constituye incumplimiento de las obligaciones de la Sociedad frente al Participante.

---

§8 Jurisdicciones Prohibidas

8.1 Prohibición Absoluta. La Sociedad no presta Servicios a Participantes que sean residentes, ciudadanos de, o actúen por cuenta de, las siguientes jurisdicciones sometidas a sanciones globales o clasificadas por la FATF bajo “Call for Action”:

1. Cuba;
2. Irán;
3. República Popular Democrática de Corea (DPRK / Corea del Norte);
4. Myanmar (en la medida cubierta por la lista FATF Call for Action);
5. Siria;
6. Rusia;
7. Venezuela;
8. territorios sujetos a regímenes de sanciones globales a la Fecha de Entrada en Vigor: Crimea, República Popular de Donetsk, República Popular de Lugansk, Óblast de Zaporiyia, Óblast de Jersón (territorios anexionados/ocupados de Ucrania bajo sanciones de OFAC, UE y ONU);
9. Bielorrusia;
10. Libia, Sudán, Somalia, Iraq, Yemen, Malí, Líbano — en la medida exigida por los regímenes de sanciones aplicables de la ONU, la UE, OFAC y HMT del Reino Unido;
11. cualquier otro país o territorio sujeto a sanciones globales administradas por el UN Security Council, la European Union, OFAC o HM Treasury.

8.2 Lista Gris de la FATF — Cautelas Reforzadas. Respecto de los Participantes procedentes de jurisdicciones incluidas en las “Jurisdictions under Increased Monitoring” de la FATF (lista gris), se aplica obligatoriamente la Diligencia Debida Reforzada (EDD) conforme al §7 del presente Marco. La inclusión en la lista gris de la FATF no constituye, por sí sola, motivo de denegación automática

de los Servicios, siempre que la EDD se complete satisfactoriamente. La lista vigente se publica en el sitio web oficial de la FATF: https://www.fatf-gafi.org/.

8.3 Restricciones Adicionales Impuestas por la Sociedad. De conformidad con el §7.17 de los T&C, la Sociedad tampoco presta Servicios en las siguientes jurisdicciones por motivos comerciales o regulatorios: Estados Unidos de América — salvo permiso expreso de la Sociedad de conformidad con la legislación estatal aplicable; Canadá — salvo permiso expreso de la Sociedad. La lista completa y vigente de jurisdicciones restringidas figura en el §7.17 de los T&C, publicada en neomaaafunded.com.

8.4 Responsabilidad del Participante. De conformidad con el §7.17(d) de los T&C, el Participante asume la responsabilidad exclusiva del cumplimiento de la legislación aplicable de su jurisdicción. El registro o el uso de los Servicios desde una jurisdicción prohibida constituye un incumplimiento sustancial de los T&C y dará lugar a la suspensión inmediata de la cuenta sin previo aviso, de conformidad con el §7.17(d) de los T&C.

8.5 Monitorización y Actualizaciones. La Sociedad mantiene una monitorización continua de los acontecimientos en materia de sanciones y de regulación y actualiza la lista de jurisdicciones prohibidas ante cada modificación de los regímenes de sanciones de la ONU, la UE, OFAC y HM Treasury, así como tras cada sesión plenaria de la FATF (no menos de tres veces al año).

---

§9 Filtrado de Sanciones

9.1 Listas de Sanciones Aplicables. La Sociedad filtra a todos los Participantes contra las siguientes listas:

1. UN Security Council Consolidated List — todas las resoluciones de sanciones adoptadas en virtud del Capítulo VII de la Carta de la ONU;
2. EU Consolidated Sanctions List;
3. OFAC SDN List (Specially Designated Nationals and Blocked Persons List), junto con las OFAC Sectoral Sanctions Identifications (SSI);
4. UK OFSI Consolidated List (HM Treasury Financial Sanctions Consolidated List);
5. UAE Local Terrorist List, junto con las listas de sanciones administradas por la UAE Executive Office for AML/CFT.

9.2 Filtrado de PEP. El filtrado de la condición de Persona Políticamente Expuesta (PEP) se lleva a cabo utilizando Dow Jones Risk & Compliance, WorldCheck o bases de datos equivalentes integradas en la plataforma Sumsub, así como a través de fuentes públicas: registros oficiales de la administración, bases de datos de organizaciones internacionales y publicaciones en medios.

9.3 Frecuencia del Filtrado. El filtrado se realiza:

1. en cada incorporación de un nuevo Participante, con carácter previo a la concesión de acceso a los Servicios;
2. ante cada actualización de las listas de sanciones aplicables;
3. con carácter previo a cada desembolso del Programa de Beneficios;
4. ante cualquier cambio en los datos personales del Participante;
5. ante la adición de un nuevo método de pago o de datos de retirada.

9.4 Procedimiento ante la Identificación de una Coincidencia de Sanciones. Cuando se identifique una coincidencia o posible coincidencia con cualquier lista de sanciones aplicable:

1. la transacción y la cuenta se inmovilizan inmediatamente sin notificar al Participante;

2. el Responsable de Cumplimiento analiza la coincidencia en un plazo de 24 horas para determinar si se trata de una coincidencia verdadera o de un falso positivo;
3. cuando el resultado sea un falso positivo: la conclusión se hace constar en el expediente del cliente con justificación escrita;
4. cuando se confirme una coincidencia verdadera: los fondos permanecen inmovilizados; se presenta un informe a la autoridad de sanciones pertinente dentro del plazo legalmente prescrito; no se procederá a ninguna liberación sin la autorización escrita expresa de la autoridad de sanciones competente; el Responsable de Cumplimiento informa a la Alta Dirección.

9.5 Prohibición. Queda estrictamente prohibido liberar los fondos de una persona sancionada sin la autorización escrita de la autoridad de sanciones pertinente (OFAC, la UE o la autoridad competente correspondiente).

---

§10 Monitorización de Transacciones

10.1 Sistema de Monitorización. La Sociedad opera un sistema multinivel de monitorización de transacciones (transaction monitoring) que combina análisis automatizado con revisión manual por parte de miembros del equipo de cumplimiento.

10.2 Desencadenantes Automatizados. El sistema de monitorización genera alertas ante la identificación de, entre otros, los siguientes patrones:

1. Estructuración (Structuring): un patrón de pagos estructurado de modo que se mantenga por debajo de los umbrales establecidos o se eluda los requisitos de verificación.
2. Entrada/salida rápida (Rapid in/out): movimiento inmediato de fondos tras su recepción, sin finalidad económica aparente.
3. Desajuste geográfico (Geographic mismatch): transacciones de pago procedentes de jurisdicciones incompatibles con los datos KYC del Participante.
4. Pagos de terceros (Third-party payments): recepción de fondos de personas que no son el titular de cuenta verificado, o solicitudes de retirada a datos que no pertenecen al Participante.
5. [Reservado intencionalmente];
6. Datos de pago compartidos entre distintas cuentas: métodos de pago o destinos de retirada comunes compartidos entre distintas cuentas, de conformidad con el §7.12(C)(vi) de los T&C.
7. Uso de herramientas de anonimización: uso de VPN, Tor o servicios de proxy en infracción del §7.10.1(l) de los T&C.

10.3 Monitorización Comportamental de la Actividad de Operativa. Además de la monitorización de transacciones, la Sociedad realiza una monitorización comportamental de la actividad de operativa de los Participantes para identificar patrones que puedan indicar conductas coordinadas o fraudulentas con relevancia AML (Prevención del Blanqueo de Capitales): operaciones simétricas (matched trades), operativa en grupo / actividad coordinada, uso compartido de cuentas, e incoherencias de IP/geolocalización, de conformidad con el §7.10.1(l) y (m) de los T&C.

10.4 Umbrales. Los umbrales numéricos específicos de monitorización de transacciones no se divulgan en esta versión pública del Marco con el fin de preservar la confidencialidad de los controles AML de la Sociedad. Los desencadenantes se aplican de manera combinada: umbral Y conducta.

10.5 Revisión Manual. Todas las alertas del sistema de monitorización son objeto de revisión manual por parte de un miembro autorizado del equipo de cumplimiento. Los indicadores que no se justifiquen por motivos legítimos se escalan al Responsable de Cumplimiento (Head of

Compliance) para que evalúe si debe prepararse un Informe de Escalado de Actividad Sospechosa (SAER, Suspicious Activity Escalation Report) de conformidad con el §11 del presente Marco.

10.6 Señales de Alerta Típicas. Las señales de alerta (red flags) que requieren la atención inmediata del equipo de cumplimiento incluyen, entre otras:

- la negativa de un Participante a aportar documentación KYC sin explicación razonable;
- documentos con indicios de alteración o incoherencia;
- preocupación excesiva por parte de un Participante respecto de los procedimientos de monitorización;
- un perfil transaccional sustancialmente incoherente con el origen de los fondos declarado;
- la dirección IP del Participante al iniciar sesión no se corresponde con la jurisdicción declarada en el KYC;
- operaciones de mirror-trading entre cuentas seguidas de desembolsos del Programa de Beneficios a ambas cuentas;
- retrocesiones (chargebacks) o disputas de pago reiteradas seguidas de una nueva financiación de la cuenta.

---

§11 Escalado Interno de Actividad Sospechosa

11.1 Definición. Se considerará que una transacción o cuenta da lugar a motivos de actividad sospechosa cuando la Sociedad tenga conocimiento, sospecha o motivos razonables para sospechar que la transacción o los fondos están vinculados a actividad delictiva, blanqueo de capitales, financiación del terrorismo, elusión de sanciones o fraude, con independencia del importe de la transacción. Cuando la Sociedad determine posteriormente que surge cualquier obligación de información externa bajo la legislación aplicable, la Sociedad cumplirá dicha obligación de conformidad con los procedimientos de la autoridad competente.

11.2 Responsabilidades del Responsable de Cumplimiento. El Responsable de Cumplimiento (Head of Compliance) de la Sociedad asume la responsabilidad exclusiva de:

1. recibir las comunicaciones internas de actividad sospechosa procedentes de los empleados de la Sociedad;
2. evaluar cada comunicación interna y preparar un Informe de Escalado de Actividad Sospechosa (SAER) para la Alta Dirección (Senior Management) cuando se justifique el escalado;
3. evaluar si surge cualquier obligación de información externa bajo la legislación aplicable y, cuando surja tal obligación, cumplirla de conformidad con los procedimientos de la autoridad competente;
4. documentar todas las decisiones, incluidas las decisiones de no escalar o de no realizar ningún informe externo, con justificación escrita.

11.3 Proceso de Escalado Interno.

Paso 1 — Detección: un empleado o un sistema automatizado identifica una o varias señales de alerta.

Paso 2 — Escalado: dentro del plazo prescrito por los procedimientos internos, el empleado presenta al Responsable de Cumplimiento una comunicación interna escrita de actividad sospechosa que describa las señales de alerta identificadas y las medidas ya adoptadas.

Paso 3 — Revisión de Cumplimiento: el Responsable de Cumplimiento revisa los materiales presentados. Cuando sea necesario, el Responsable de Cumplimiento solicita información adicional a los empleados o al proveedor Sumsub.

Paso 4 — Decisión: el Responsable de Cumplimiento adopta una de dos decisiones: preparar un Informe de Escalado de Actividad Sospechosa (SAER) para la Alta Dirección, o abstenerse de hacerlo con justificación escrita.

Paso 5 — Escalado y reporte externo (en su caso): el Responsable de Cumplimiento escala el Informe de Escalado de Actividad Sospechosa (SAER) a la Alta Dirección y evalúa si surge cualquier obligación de información externa bajo la legislación aplicable. Cuando surja tal obligación, el Responsable de Cumplimiento asegurará el cumplimiento oportuno conforme a los procedimientos de la autoridad competente.

Paso 6 — Documentación: la totalidad del proceso se documenta. Los informes internos y la correspondencia se conservan durante un mínimo de cinco (5) años conforme al §12 del presente Marco.

11.4 Plazos. Un Informe de Escalado de Actividad Sospechosa (SAER) se prepara y se escala a la Alta Dirección sin demora indebida desde el momento en que el personal de la Sociedad supo, sospechó o tuvo motivos razonables para sospechar la concurrencia de motivos de escalado. Cualquier obligación de información externa que surja bajo la legislación aplicable se cumple dentro del plazo prescrito por dicha legislación.

11.5 Prohibición de Revelación (Tipping-Off). La Sociedad observa la prohibición de revelación (tipping-off) reflejada en el Artículo 25 del UAE Federal Decree-Law No. 10 of 2025 como buena práctica voluntaria. La Sociedad, sus empleados, administradores y agentes se abstendrán de divulgar al Participante o a cualquier tercero el hecho de que se ha producido un escalado interno de actividad sospechosa, o de que se ha realizado o pueda realizarse un informe externo, o de que se está llevando a cabo una investigación en relación con sospechas de blanqueo de capitales, financiación del terrorismo, fraude o elusión de sanciones, salvo cuando dicha divulgación sea exigida por la legislación aplicable.

11.6 Inmovilización de Activos por Actividad Sospechosa. Tras la preparación de un Informe de Escalado de Actividad Sospechosa (SAER) o tras la identificación de una coincidencia de sanciones, la Sociedad podrá inmovilizar la cuenta del Participante y suspender todos los desembolsos del Programa de Beneficios. Dicha inmovilización (asset freeze) no constituye incumplimiento de las obligaciones de la Sociedad frente al Participante; cualquier demora en los desembolsos derivada de requisitos legales AML o de sanciones no generará responsabilidad alguna por parte de la Sociedad, de conformidad con el §1.5(t)(v) de los T&C.

---

§12 Conservación de Registros

12.1 Principio General. De conformidad con el Artículo 16(1)(f) del AML FDL y las Financial Action Task Force (FATF) Recommendations (Recomendación 11), la Sociedad conserva todos los documentos y registros relativos a las relaciones de negocio con los Participantes y a todas las transacciones durante un mínimo de cinco (5) años desde el fin de la relación de negocio o la fecha de la transacción. Este período de conservación es coherente con el §8(a) de la Política de Privacidad.

12.2 Registros Sujetos a Conservación. Los siguientes registros están sujetos a conservación obligatoria, incluyendo:

1. documentos de identidad (KYC/CDD): pasaportes, documentos de identidad, documentos acreditativos del domicilio, resultados de verificación de Sumsub, capturas de pantalla de controles biométricos y resultados del filtrado de la condición de PEP;

2. documentos de EDD: declaraciones de Origen de los Fondos (SOF, Source of Funds) y de Origen del Patrimonio (SOW, Source of Wealth), pruebas documentales del origen de los fondos y decisiones de aprobación de la EDD por la alta dirección;
3. registros de transacciones: historial de pagos, historial de desembolsos del Programa de Beneficios y logs de procesamiento de pagos;
4. registros de filtrado de sanciones: resultados del filtrado automatizado y manual respecto de cada Participante y de cada transacción, incluidas anotaciones de coincidencias, posibles coincidencias y su resolución;
5. Informes internos de Escalado de Actividad Sospechosa (SAERs) y correspondencia de las investigaciones de cumplimiento;
6. cualesquiera informes externos presentados ante autoridades competentes bajo la legislación aplicable, cuando haya surgido tal obligación, y los acuses confirmando su presentación;
7. registros de las revisiones periódicas del expediente del cliente;
8. registros de la correspondencia con los Participantes relativa a procedimientos KYC/AML.

12.3 Requisitos Técnicos de Almacenamiento. Todos los registros se almacenan en un formato seguro (cifrado AES-256 en reposo, TLS 1.2 o superior en tránsito) de conformidad con el §29.9 de los T&C. Los registros deberán ser accesibles a las autoridades regulatorias y a la UAE FIU (Unidad de Inteligencia Financiera, Financial Intelligence Unit) a la primera solicitud. Queda prohibida la destrucción anticipada de registros antes del vencimiento del período de conservación aplicable. Tras la recepción de una solicitud de un regulador o de la UAE FIU, el período de conservación se suspende hasta la conclusión del procedimiento correspondiente.

12.4 Período de Conservación Extendido. Cuando estén en curso procedimientos judiciales, regulatorios o AML respecto de un Participante, el período de conservación de los registros correspondientes se extiende hasta la conclusión de dichos procedimientos más un (1) año.

12.5 Resumen de Períodos de Conservación:

- Registros KYC/AML: mínimo 5 años desde el fin de la relación de negocio o la fecha de la transacción (UAE FDL 20/2018 + FATF Rec. 11)
- Registros de transacciones: mínimo 7 años
- Registros SAER y cualesquiera informes externos: mínimo 5 años tras su preparación o presentación

---

§13 Formación y Sensibilización

13.1 Formación Anual Obligatoria. De conformidad con los requisitos del AML FDL y la buena práctica internacional, todos los empleados de la Sociedad con acceso a datos de clientes, operaciones de pago o procedimientos AML/CFT (Lucha contra la Financiación del Terrorismo, Combating the Financing of Terrorism) están obligados a completar formación AML/CFT/CPF (Lucha contra la Financiación de la Proliferación, Counter-Proliferation Financing) con periodicidad anual.

13.2 Programa de Formación. El programa de formación obligatorio comprende, entre otras materias:

1. el marco regulatorio AML/CFT/CPF (el AML FDL, la UAE Cabinet Decision No. 134 of 2025, las Financial Action Task Force (FATF) Recommendations);
2. las tipologías de blanqueo de capitales y financiación del terrorismo características del sector prop-trading;

3. los procedimientos KYC (Conocimiento del Cliente, Know Your Customer) / CDD (Diligencia Debida del Cliente) / EDD (Diligencia Debida Reforzada) de la Sociedad;
4. las señales de alerta y los procedimientos de escalado;
5. el cumplimiento de sanciones y los procedimientos de filtrado;
6. la prohibición de revelación (tipping-off) (cuando proceda) y los procedimientos del Informe de Escalado de Actividad Sospechosa (SAER, Suspicious Activity Escalation Report), incluida la evaluación de cualesquiera obligaciones de información externa bajo la legislación aplicable;
7. los canales internos de denuncia (whistleblowing);
8. las actualizaciones de la legislación aplicable y de la práctica regulatoria.

13.3 Formación Especializada. El equipo de Cumplimiento y el Responsable de Cumplimiento siguen un programa de formación especializada ampliado, que incluye formación sobre el uso de la plataforma Sumsub, la interpretación de los resultados del filtrado de sanciones y la evaluación de cualesquiera obligaciones de información externa que surjan bajo la legislación aplicable.

13.4 Documentación de la Formación. Todas las sesiones de formación se documentan (fecha, asistentes, contenido del programa, duración). Los registros de formación se conservan durante un mínimo de cinco (5) años. El Responsable de Cumplimiento mantiene un registro de la realización de la formación por cada empleado.

13.5 Empleados de Nueva Incorporación. Los empleados de nueva incorporación deberán completar la formación introductoria AML/CFT en el plazo de treinta (30) días desde su fecha de incorporación.

---

§14 Gobernanza y Contactos

14.1 Estructura de Gobernanza del Cumplimiento. La Sociedad ha establecido la siguiente estructura de gobernanza:

1. Responsable de Cumplimiento (Head of Compliance): coordina los procedimientos de diligencia debida del cliente, filtrado de sanciones y escalado de actividades sospechosas establecidos en el presente Marco; recibe y evalúa las comunicaciones internas de actividad sospechosa; prepara los Informes de Escalado de Actividad Sospechosa (SAERs) para la Alta Dirección (Senior Management); evalúa si surge cualquier obligación de información externa bajo la legislación aplicable y asegura el cumplimiento de la misma; organiza la formación del personal y las revisiones independientes.
2. Alta Dirección: aprueba el presente Marco y sus modificaciones; aprueba la incorporación (onboarding) de Participantes de mayor riesgo (EDD); recibe el informe anual del Responsable de Cumplimiento sobre la eficacia del Marco.
3. Consejo de Administración (Board of Directors): recibe los resultados de la revisión anual independiente del presente Marco directamente del revisor; asume la responsabilidad última del correcto funcionamiento del programa de cumplimiento de la Sociedad.

Cadena de rendición de cuentas: Responsable de Cumplimiento → Alta Dirección → Consejo de Administración.

14.2 Revisión Anual Independiente. La Sociedad encarga una revisión externa independiente del presente Marco no menos de una vez al año. El revisor deberá ser independiente de la dirección operativa de la Sociedad y deberá acreditar competencia demostrada en diligencia debida del cliente, cumplimiento AML/sanciones y protección al consumidor. Los resultados de la revisión se reportan directamente al Consejo de Administración. El Responsable de Cumplimiento está

obligado a desarrollar un plan de subsanación de las deficiencias identificadas en el plazo de treinta (30) días desde la recepción del informe de revisión.

14.3 Revisión Anual del Marco. El presente Marco se revisa no menos de una vez al año, y ante cada cambio sustancial en la legislación aplicable o en el modelo de negocio de la Sociedad.

14.4 Protección del Denunciante (Whistleblower). Los empleados de la Sociedad que de buena fe denuncien transacciones sospechosas o incumplimientos de cumplimiento, ya sea internamente o ante una autoridad competente, están protegidos frente a toda forma de represalia, acción adversa y discriminación, de conformidad con la legislación aplicable de los UAE.

14.5 Datos de Contacto. Para todas las consultas relativas al presente Marco, a los procedimientos de diligencia debida del cliente o al cumplimiento de sanciones, los Participantes y las partes interesadas podrán dirigirse a:

Consultas sobre diligencia debida del cliente, sanciones y cumplimiento: compliance@neomaaafunded.com

Consultas generales y soporte: support@neomaaafunded.com

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

Sitio web: neomaaafunded.com

14.6 Modificaciones del Marco. La Sociedad se reserva el derecho a modificar el presente Marco en cualquier momento. La versión vigente del Marco se publica en neomaaafunded.com. Las modificaciones sustanciales surten efecto conforme al procedimiento establecido en el §1.3 de los T&C.

El presente Marco de Diligencia Debida del Cliente y AML/Sanciones entra en vigor el 24 de septiembre de 2026. El presente Marco sustituye a todas las versiones previas de la Política AML / KYC o documento equivalente publicado por Neom Triple A Information Technology LLC bajo la marca NEOMAAA Funded.

Marco de Diligencia Debida del Cliente y AML/Sanciones v4.0.1 | Neom Triple A Information Technology LLC (NEOMAAA Funded) | Fecha de Publicación: 24 de septiembre de 2026