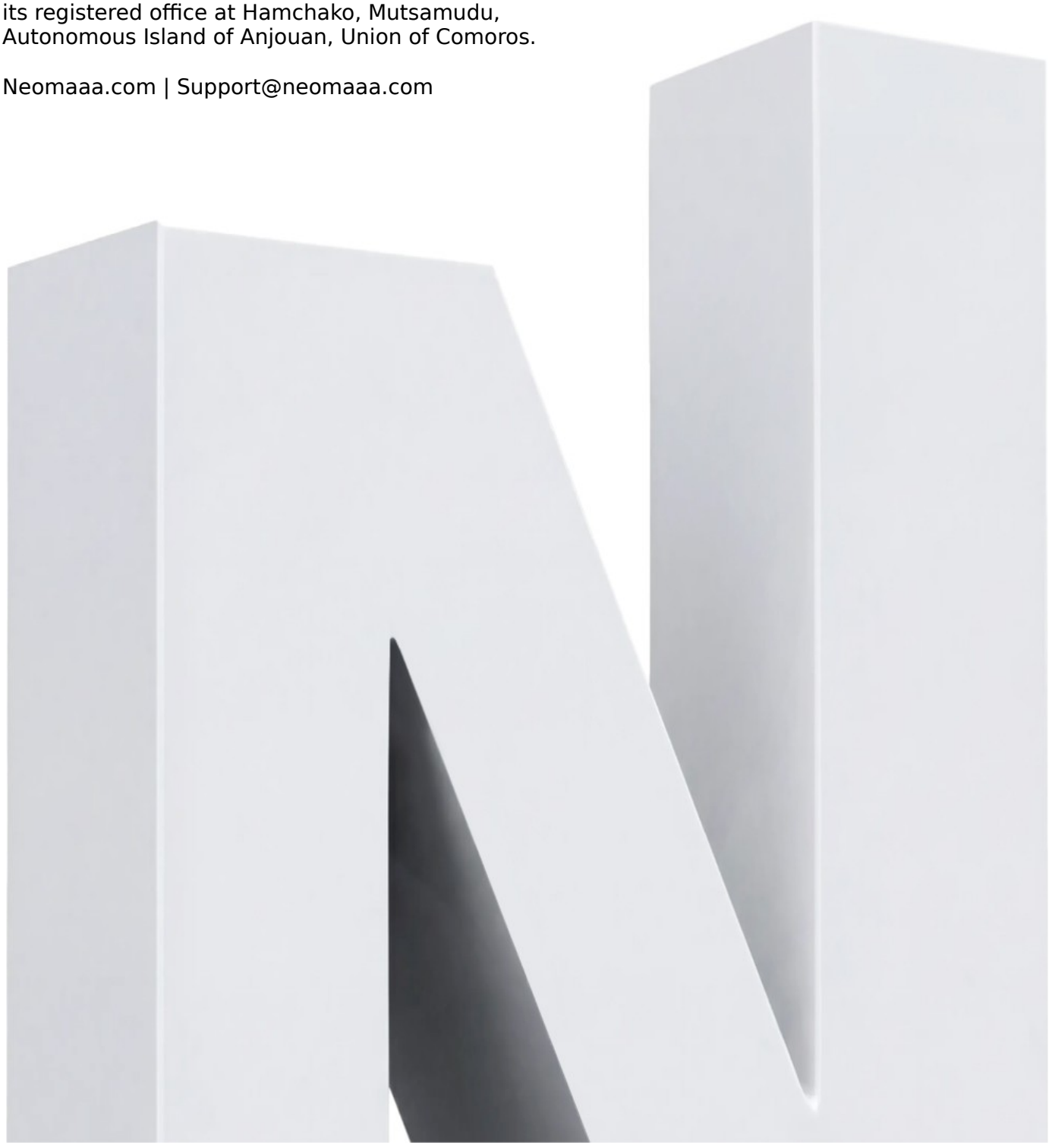
NEOMAAA

AML Policy

The Anjouan Offshore Finance Authority of the Union of Comoros with an Investment Dealer license 15968, having its registered office at Hamchako, Mutsamudu, Autonomous Island of Anjouan, Union of Comoros.

Neomaaa.com | Support@neomaaa.com



AML Policy

Version v.1.0 — 1 March 2026

Neomaaa Ltd
Registered as International Business Company No. 15968
Licensed under International Brokerage License Number L15968/N
Licensed and authorized by the Anjouan Offshore Finance Authority (AOFA), Union of Comoros
Hamchako, Mutsamudu, The Autonomous Island of Anjouan, Union of Comoros

Document Reference: NEOMAAA-AML-v1.0-2026
Created: 1 March 2026
Approved: 1 March 2026
Status: APPROVED • v.1.0

1. Introduction

1.1.

Neomaaa Ltd (hereinafter referred to as the ''Company''), is incorporated under the laws of The Autonomous Island of Anjouan, Union of Comoros with Registration 15968 having its registered office at Hamchako Mutsamudu, The Autonomous Island of Anjouan, Union of Comoros.

The Company is authorized as a Business Company under the Business Companies (Amendment and Consolidation) Act, of the Revised Laws of The Autonomous Island of Anjouan, Union of Comoros , 005 of 2005 (herein the "Law").

1.2.

The objects of the Company are all subject matters not forbidden by Business Companies (Amendment and Consolidation) Act, of the Revised Laws of The Autonomous Island of Anjouan, Union of Comoros, 005 of 2005, in particular but not exclusively all commercial, financial, lending, borrowing, trading, service activities and the participation in other enterprises as well as to provide brokerage, training and managed account services in currencies, commodities, indexes, CFDs and leveraged financial instruments.

1.3.

The Company is committed to combating money laundering and for this reason it has appointed a dedicated Anti-Money Laundering Compliance Officer (the "AMLCO") who is accountable to the Board of Directors and Senior Management of the Company. The AMLCO is further responsible for the training of employees with respect to the Anti-Money Laundering Law and any amendments thereof as well as for the preparation of the internal procedures of the Company.

2. Key Principal

2.1.

All of the Company's employees are required to read and acknowledge the Anti- Money Laundering Manual of the Company and shall at all times act under the 'Key Principles' set out therein.

a) Take appropriate steps to protect the Company and its domain from any activities which involve money laundering and terrorist financing.

b) The Company must maintain and implement written policies and procedures with respect to combating money laundering, a system of internal controls to ensure ongoing compliance with applicable laws which shall be reviewed and monitored by a designated person and to take appropriate action, once suspicious activity is detected, through the reporting of such transactions in line with the guidelines set out by Global Anti- Money Laundering regulations.

c) Comply with applicable anti-money laundering and terrorist financing laws and regulations as established by the Global Anti- Money Laundering guidelines.

d) All business units of the Company shall follow the AML policies and procedures.

e) Report all identified suspicious activities to the extent that it can do so under all applicable foreign and domestic laws.

f) Compliance with the Company's AML policies will be monitored through a combination of internal audit and regulatory reviews of compliance with relevant anti-money laundering legislation and/or regulations.

g) Retaining all the customer related documents for a period specified as per the Financial Services Authority The Autonomous Island of Anjouan, Union of Comoros.

h) The Company does not offer services of opening anonymous accounts.

i) Full cooperation with law enforcement and regulatory agencies to the extent that it can do so under all applicable laws.

j) Train staff on Know Your Customer and Anti-Money Laundering policies and new AML laws and regulations.

k) The AML Compliance Committee is responsible for initiating Suspicious Activity Reports ("SARs") or other required reporting to the appropriate law enforcement or regulatory agencies. Any contacts by law enforcement or regulatory agencies related to the Policy shall be directed to the AML Compliance Committee.

The committee shall:

– Receive internal reports of (suspicions of) money laundering.

– Investigate reports of suspicious events.

– Make reports of relevant suspicious events to the relevant authorities.

– Ensure the adequacy of arrangements made for the awareness and training of staff and advisers.

– Report at least annually to the firm's governing body on the operation and effectiveness of the firm's systems and controls.

– Monitor the day-to-day operation of anti-money laundering policies in relation to: the development of new products; the taking on of new customers; and changes in the firm's business profile.

3. Policy

It is the policy of Neomaaa Ltd to actively pursue the prevention of money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities. Neomaaa Ltd is committed to AML compliance in accordance with applicable law and requires its officers, employees and appointed producers to adhere to these standards in preventing the use of its products and services for money laundering purposes.

For the purposes of the Policy, money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the unlawful proceeds appear to have been derived from legitimate origins or constitute legitimate assets.

4. What is Money Laundering?

Money laundering is the process by which criminally obtained money or other assets (criminal property) are exchanged for "clean" money or other assets with no obvious link to their criminal origins. Criminal property may take any form, including money or money's worth, securities, tangible property and intangible property. It also covers money, which is used to fund terrorism.

Money laundering activity includes:

- Acquiring, using or possessing criminal property
- Handling the proceeds of crimes such as theft, fraud and tax evasion
- Being knowingly involved in any way with criminal or terrorist property
- Entering arrangements to facilitate laundering criminal or terrorist property
- Investing the proceeds of crimes in other financial products
- Investing the proceeds of crimes through the acquisition of property/assets
- Transferring criminal property.

There is no single stage of money laundering; methods can range from the purchase and resale of luxury items such as a car or jewelry to passing money through a complex web of legitimate operations. Usually the starting point will be cash, but it is important to appreciate that money laundering is defined in terms of criminal property. This can be property in any conceivable legal form, whether money, rights, real estate or any other benefit, if you know or suspect that it was obtained, either directly or indirectly, as a result of criminal activity and you do not speak up then you too are taking a part in the process.

The money laundering process follows three stages: 1. Placement Disposal of the initial proceeds derived from illegal activity e.g. into a bank account. 2. Layering The money is moved through the system in a series of financial transactions in order to disguise the origin of the cash with the purpose of giving it the appearance of legitimacy. 3. Integration Criminals are free to use the money as they choose once it has been removed from the system as apparently "clean" funds. No financial sector business is immune from the activities of criminals and Firms should consider the money laundering risks posed by the products and services they offer.

5. What is Counter Terrorist Financing (CTF)?

Terrorist financing is the process of legitimate businesses and individuals that may choose to provide funding to resource terrorist activities or organizations for ideological, political or other reasons.

Firms must therefore ensure that: i) customers are not terrorist organizations themselves: and ii) they are not providing the means through which terrorist organizations are being funded.

Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal the origin or intended use of the funds, which will later be used for criminal purposes.

6. Risk Based Approach

The level of due diligence required when considering anti-money laundering procedures within the firm, it should take a risk-based approach. This means the amount of resources spent in conducting due diligence in any one relationship that is subject risk should be in proportion to the magnitude of the risk that is posed by that relationship.

These can be broken down into the following areas:

Customer Risk

Different customer profiles have different levels of risks attached to them,a basic Know Your Customer (KYC) check can establish the risk posed by a customer.

For example, near-retired individuals making small, regular contributions to a savings account in line with their financial details poses less of a risk than middle-aged individuals making ad-hoc payments of ever-changing sizes into a savings account that does not fit into the profile of the customers' standing financial data.

The intensity of the due diligence conducted on the latter would be higher than that carried out on the former as the potential threat of money laundering in the second case would be perceived as being greater.

Corporate structures can be used as examples of customers that could carry a higher risk profile than the one just seen, as these can be used by criminals to introduce layers within transactions to hide the source of the funds, and like that, clients can be categorized into different risk bands.

Product Risk

This is the risk posed by the product or service itself. The product risk is driven by its functionality as a money laundering tool.

The Joint Money Laundering Steering Group has categorized the products with which Firms typically deal into three risk bands \-- reduced, intermediate and increased. Typically, pure protection contracts are categorized as reduced risk and investments in unit trusts as increased risk.

Additionally, a factor that will contribute to the classification of the risk category is the sales process associated with the product. If the transaction in the product takes place on an advisory basis as a result of a KYC, this will carry less risk than an execution only transaction, whereby you know significantly less about the customer.

Country Risk

The geographic location of the client or origin of the business activity has a risk associated with it, this stems from the fact that countries around the globe have different levels of risk attached to them.

A firm would determine the extent of their due diligence measure required initially and on an ongoing basis using the above four risk areas.

7. Customer Identification Program

Neomaaa Ltd has adopted a Customer Identification Program (CIP). We will provide notice that they will seek identification information; collect certain minimum customer identification information from each customer, record such information and the verification methods and results.

8. Notice to Customers

Neomaaa Ltd will provide notice to customers that it is requesting information from them to verify their identities, as required by applicable law.

9. Know Your Customers

When a business relationship is formed, in order to establish what might constitute normal activity later in the relationship, it is necessary for the company to ascertain the nature of the business a client expects to conduct.

Once an on-going business relationship has been established, any regular business undertaken for that customer can be assessed against the expected pattern of activity of the customer. Any unexplained activity can then be examined to determine whether there is a suspicion of money laundering or terrorist financing.

Information regarding a client's income, occupation, source of wealth, trading habits and the economic purpose of any transaction is typically gathered as part of the provision of advice. At the start of the relationship personal information is also obtained, such as, nationality, date of birth, and residential address. These pieces of information should also be considered in respect to the risk of financial crime (including AML and CTF). For high-risk transactions, it might be appropriate to seek verification of the information the client has provided.

10. Source of Funds

When a transaction takes place, the source of funds, i.e. how the payment is to be made, from where and by who, must always be ascertained and recorded in the client file (this would usually be achieved through retaining a copy of the cheque or direct debit mandate).

11. Identification

The standard identification requirement for customers who are private individuals are generally governed by the circumstances relating to the customer and the product type that is being dealt in, i.e. the level of risk attributed to the product whether it is a reduced risk, intermediate risk or an increased risk product. Taking that into account for reduced risk and intermediate risk products the following pieces of information are required as a standard for identification purposes:

– Full name

– Residential Address

12. Verification

Verification of the information obtained must be based on reliable and independent sources \-- which might either be documents produced by the customer, or electronically by the firm, or by a combination of both.

Where business is conducted face-to-face, firms should see originals of any documents involved in the verification.

If documentary evidence of an individual's identity is to provide a high level of confidence, it will typically have been issued by a government department or agency, or by a court, because there is a greater likelihood that the authorities will have checked the existence and characteristics of the persons concerned. In cases where such documentary evidence of identity may not be available to an individual, other evidence of identity may give the firm reasonable confidence in the customer's identity, although the firm should weigh these against the risks involved.

If the identity is to be verified from documents, this should be based on: Either a government issued document which incorporates:

– The customer's full name, and

– Their residential address

– Photographic Government issued documents or valid passport

– National identity card alternatively, this can be done by a non-photographic government issued document which incorporates the customer's full name, supported by a second document, which incorporates:

– The customer's full name, and

– Their residential address

13. Evidence of Address

– Current bank statements, or credit/debit card statements, issued by a regulated financial sector firm (but not ones printed off the internet and not less than 3 months old) \<!\-- \--\>

– Utility bills (not including mobile phone bills, not ones printed off the internet and not less than 3 months old) For increased risk level products, in addition to obtaining the standard information detailed above, the following know your customer information should be obtained and recorded:

– Employment and income details

– Source of wealth (i.e. source of the funds being used in the transaction)

14. Monitoring and Reporting

Transaction based monitoring will occur within the appropriate business units of Neomaaa Ltd. Monitoring of specific transactions will include but is not limited to transactions aggregating $5,000 or more and those with respect to which Neomaaa Ltd has a reason to suspect suspicious activity. All reports will be documented.

15. Suspicious Activity

There are signs of suspicious activity that suggest money laundering.

These are commonly referred to as "red flags." If a red flag is detected, additional due diligence will be performed before proceeding with the transaction. If a reasonable explanation is not determined, the suspicious activity shall be reported to the AML Compliance Committee.

Examples of red flag are:

– The customer exhibits unusual concern regarding the firm's compliance with government reporting requirements and the firm's AML policies, particularly with respect to his or her identity, type of business and assets, or is reluctant or refuses to reveal any information concerning business activities, or furnishes unusual or suspect identification or business documents.

– The customer wishes to engage in transactions that lack business sense or apparent investment strategy, or are inconsistent with the customer's stated business strategy.

– The information provided by the customer that identifies a legitimate source for funds is false, misleading, or substantially incorrect.

– Upon request, the customer refuses to identify or fails to indicate any legitimate source for his or her funds and other assets.

– The customer (or a person publicly associated with the customer) has a questionable background or is the subject of news reports indicating possible criminal, civil, or regulatory violations.

– The customer exhibits a lack of concern regarding risks, commissions, or other transaction costs.

– The customer appears to be acting as an agent for an undisclosed principal, but declines or is reluctant, without legitimate commercial reasons, to provide information or is otherwise evasive regarding that person or entity.

– The customer has difficulty describing the nature of his or her business or lacks general knowledge of his or her industry.

– The customer attempts to make frequent or large deposits of currency, insists on dealing only in cash equivalents, or asks for exemptions from the firm's policies relating to the deposit of cash and cash equivalents.

– For no apparent reason, the customer has multiple accounts under a single name or multiple names, with many inter-account or third-party transfers.

– The customer's account has unexplained or sudden extensive activity, especially in accounts that had little or no previous activity.

– The customer's account has many wire transfers to unrelated third parties inconsistent with the customer's legitimate business purpose.

– The customer's account has wire transfers that have no apparent business purpose to or from a country identified as money laundering risk or a bank secrecy haven.

– The customer's account indicates large or frequent wire transfers, immediately withdrawn by check or debit card without any apparent business purpose.

– The customer makes a funds deposit followed by an immediate request that the money be wired out or transferred to a third party, or to another firm, without any apparent business purpose.

– The customer makes a funds deposit for the purpose of purchasing a long-term investment followed shortly thereafter by a request to liquidate the position and transfer the proceeds out of the account.

– The customer requests that a transaction be processed in such a manner to avoid the firm's normal documentation requirements.

Know your customer \-- the basis for recognizing suspicions A suspicious transaction will often be one which is inconsistent with a customer's known, legitimate business or personal activities or with the normal business for that type of customer. Therefore, the first key to recognition is knowing enough about the customer's business to recognise that a transaction, or series of transactions, is unusual.

Questions you must consider when determining whether an established customer's transaction might be suspicious are:

– Is the size of the transaction consistent with the normal activities of the customer?

– Is the transaction rational in the context of the customer's business or personal activities?

– Has the pattern of transactions conducted by the customer changed?

Suspicious scenarios

Issues which should lead you to have cause for suspicion would include:

– Clients who are reluctant to provide proof of identity;

– Clients who place undue reliance on an introducer (they may be hiding behind the introducer to avoid giving you a true picture of their identity or business);

– Requests for cash related business, for example questions about whether investments can be made in cash, suggestions that funds might be available in cash for investment;

– Where the source of funds for investment is unclear;

– Where the magnitude of the available funds appears inconsistent with the client's other circumstances (i.e. the source of wealth is unclear). Examples might be students or young people with large amounts to invest;

– Where the transaction doesn't appear rational in the context of the customer's business or personal activities. Particular care should be taken in this area if the client changes their method of dealing with you without reasonable explanation;

– Where the pattern of transactions changes;

– Where a client who is undertaking transactions that are international in nature does not appear to have any good reason to be conducting business with the countries involved (e.g. why do they hold monies in the particular country that the funds are going to or from? Do their circumstances suggest that it would be reasonable for them to hold funds in such countries?);

– Clients who are unwilling to provide you with normal personal or financial information, for no apparent or rational reason. (Care should be taken not to include all distance relationships as suspicious, because most will be for genuine reasons. Suspicions will ordinarily be based upon

cumulative as opposed to stand alone issues) A money launderer is likely to provide persuasive arguments about the reasons for their transactions. Those should be questioned to decide whether a transaction is suspicious.

Reporting a Suspicion

Where, for whatever reason, we suspect that a client, or anybody for whom they are acting, may be undertaking (or attempting to undertake) a transaction involving the proceeds of any crime it must be reported as soon as practicably possible and in writing.

Internal reports must be made regardless of whether any business was, or is intended to be, actually written.

Investigation

Upon notification to the AML Compliance Committee an investigation will be commenced to determine if a report should be made to the appropriate law enforcement or regulatory agencies. The investigation will include, but not necessarily be limited to, review of all available information, such as payment history, birth dates, and address. If the results of the investigation warrant, a recommendation will be made to the AML Compliance Committee to file the SAR with the appropriate law enforcement or regulatory agency. The AML Compliance Committee is responsible for any notice or filing with law enforcement or regulatory agency.

Investigation

results will not be disclosed or discussed with anyone other than those who have a legitimate need to know. Under no circumstances shall any officer, employee or appointed agent disclose or discuss any AML concern, investigation, notice or SAR filing with the person or persons subject of such, or any other person, including members of the officer's, employee's or appointed agent's family.

Freezing of Accounts

Where we know that the funds in an account derive from criminal activity, or that they arise from fraudulent instructions, the account must be frozen. Where it is believed that the account holder may be involved in the fraudulent activity that is being reported, then the account may need to be frozen

15. Enquiries

For further AML enquiries please contact us at support@neomaaa.com

16. Enhanced Due Diligence (EDD)

The Company applies Enhanced Due Diligence measures to higher-risk Clients, including but not limited to:

– Politically Exposed Persons (PEPs) and their family members and close associates;

– Clients from high-risk jurisdictions as identified by the FATF, EU, or the Company's internal risk assessment;

– Clients with complex or unusual account structures;

– Clients engaging in unusually large or frequent transactions;

– Clients whose source of funds or source of wealth cannot be clearly established;

– Clients identified through adverse media screening.

EDD measures may include: additional identity verification, enhanced source of funds documentation, senior management approval for account opening and ongoing relationship, increased transaction monitoring, digital identity verification tools including device fingerprinting and browser analytics, and more frequent periodic reviews.

17. Sanctions Screening

The Company screens all Clients, beneficial owners, and counterparties against applicable sanctions lists, including but not limited to:

– United Nations Security Council consolidated sanctions list;

– European Union consolidated sanctions list;

– United States OFAC (Office of Foreign Assets Control) SDN list;

– United Kingdom HM Treasury sanctions list;

– And any other sanctions lists applicable to the Company's operations.

Sanctions screening is conducted at account opening, upon any change to Client information, and on an ongoing periodic basis. The Company will not establish or maintain a business relationship with any sanctioned person or entity.

18. Transaction Monitoring

The Company maintains automated and manual transaction monitoring systems to detect suspicious activity, including:

- Unusually large deposits or withdrawals;
- Frequent deposits followed by immediate withdrawal requests;
- Deposits from multiple payment methods or third-party sources;
- Transactions inconsistent with the Client's stated financial profile;
- Rapid movement of funds with minimal or no trading activity;
- Structuring of transactions to avoid reporting thresholds;
- Use of cryptocurrency or anonymizing payment methods.

Where suspicious activity is detected, the Company may freeze the Client's account, suspend withdrawals, file a Suspicious Activity Report (SAR), and report to relevant authorities without notifying the Client.

19. Record Keeping

The Company maintains records of all Client identification documents, transaction records, and correspondence for a minimum period of five (5) years after the termination of the business relationship or the completion of a transaction, whichever is later.

Records are maintained in a format that allows them to be made available to competent authorities upon request in a timely manner.

20. Staff Training

All Company employees receive regular training on AML/CTF obligations, including:

- Recognition of suspicious transactions and activity;
- KYC and CDD procedures;
- Reporting obligations and internal escalation procedures;
- Updates on new typologies, regulatory changes, and sanctions developments.

Training records are maintained and reviewed annually by the AMLCO.

21. Third-Party Deposits and Withdrawals

The Company does not accept deposits from, or process withdrawals to, third parties. All deposits must originate from accounts in the Client's own name, and all withdrawals must be directed to accounts in the Client's own name.

Where a third-party deposit is identified, the Company reserves the right to return the funds to the originating account and suspend the Client's account pending investigation.

22. Chargeback and Fraud Protection

Where the Company identifies a deposit that is subsequently subject to a chargeback, dispute, or fraud claim, the Company reserves the right to:

– Freeze the Client's account immediately;
– Suspend all withdrawals;
– Cancel or reverse any trades executed with the disputed funds;
– Reverse and withhold any profits derived from trading with the disputed funds;
– Deduct the chargeback amount, processing fees, and investigation costs from the Client's account;
– Report the matter to relevant law enforcement authorities;
– Terminate the Client's account permanently.

The Client acknowledges that the Company's determination regarding chargeback and fraud matters shall be made in accordance with the Company's procedures.

23. Politically Exposed Persons (PEPs)

The Company applies additional scrutiny to Clients identified as PEPs, their family members, and known close associates. PEP status is determined through screening against commercial PEP databases and through information provided by the Client.

Senior management approval is required for establishing or continuing a business relationship with a PEP. The Company conducts enhanced ongoing monitoring of PEP accounts.

24. Compliance with International Standards

The Company's AML/CTF policies and procedures are designed to comply with:

– Financial Action Task Force (FATF) Recommendations;
– Applicable laws of the Union of Comoros;
– Requirements of the Anjouan Offshore Finance Authority (AOFA);
– International best practices for anti-money laundering and counter-terrorist financing.

The Company reviews and updates its AML/CTF policies at least annually, or more frequently in response to regulatory changes, emerging risks, or identified deficiencies.

25. Client Risk Scoring and Classification

The Company operates a risk-based client classification system. Each Client is assigned a risk score upon account opening and throughout the business relationship based on the following factors:

– Country of residence and nationality (FATF high-risk, EU high-risk, or sanctioned jurisdictions);
– Transaction behavior (frequency, volume, deposit/withdrawal patterns);
– Deposit method (bank wire, card, e-wallet, cryptocurrency, prepaid);
– Trading patterns (consistency with stated profile, unusual activity);
– Sanctions and PEP screening results;
– Source of funds and source of wealth documentation;
– Adverse media and negative news screening results.

Clients are classified into the following risk categories:

25.1.

Low Risk: Clients from low-risk jurisdictions with verified identity, clear source of funds, consistent transaction behavior, and deposits via regulated bank transfers or major payment processors.

25.2.

Medium Risk: Clients from medium-risk jurisdictions, clients with moderate transaction volumes, clients using e-wallets or multiple payment methods, or clients where source of funds documentation requires additional review.

25.3.

High Risk: Clients from high-risk jurisdictions (FATF grey/black list), PEPs and their associates, clients with complex ownership structures, clients with large or unusual transaction patterns, clients using cryptocurrency or anonymizing payment methods, or clients flagged by adverse media screening.

25.4.

Prohibited Risk: Clients from sanctioned countries, sanctioned individuals or entities, clients who fail to provide required KYC documentation, clients with confirmed links to money laundering, terrorist financing, or other financial crime. The Company will not establish or maintain a business relationship with Prohibited Risk clients.

Risk classifications are reviewed periodically and may be updated at any time based on new information, changed circumstances, or regulatory developments. The Company reserves the right to escalate a Client's risk classification at any time without notice.

26. Right to Terminate for AML Risk

The Company reserves the right to suspend, restrict, or permanently terminate any Client account at any time, with or without prior notice, and without explanation, where the Company identifies or suspects:

– Money laundering or terrorist financing activity;
– Fraudulent or stolen deposits;
– Identity fraud or document forgery;
– Failure to provide requested KYC/AML documentation;
– Inconsistency between stated and actual source of funds;
– Structuring of transactions to avoid reporting thresholds;
– Any other AML/CTF risk identified by the Company.

Upon account termination for AML reasons, the Company may freeze all funds pending investigation, file a Suspicious Activity Report (SAR), report to relevant authorities, and withhold funds as required by law or regulatory guidance. The Client waives any claim arising from such termination.

27. Trading Abuse in Context of AML

The Company recognizes that certain trading practices may be used in conjunction with money laundering schemes. The following activities are specifically monitored and may trigger AML investigation:

– Depositing funds and requesting immediate withdrawal with minimal or no trading ("wash trading" for money laundering);
– Depositing via one payment method and withdrawing via another;
– Rapid cycling of funds between multiple accounts;
– Coordinated trading activity between related accounts;
– Use of the trading platform to convert currencies through round-trip transactions;
– Depositing large amounts inconsistent with the Client's stated financial profile.

The Company reserves the right to void trades, cancel profits, suspend accounts, and report activity to authorities where trading abuse with potential AML implications is detected.

28. Payment Method Risk Classification

The Company classifies payment methods by risk level for AML purposes:

28.1. Low Risk Payment Methods

– Bank wire transfer from a regulated bank in a low-risk jurisdiction;
– Payments from regulated and licensed payment service providers (PSPs).

28.2. Medium Risk Payment Methods

– Credit and debit card payments;
– E-wallet payments (Skrill, Neteller, and similar);
– Payments from banks in medium-risk jurisdictions.

28.3. High Risk Payment Methods

– Cryptocurrency deposits (Bitcoin, Ethereum, USDT, and other digital assets);
– Prepaid cards or vouchers;
– Payments from unregulated or unlicensed payment processors;
– Payments from banks in high-risk jurisdictions;
– Cash deposits (not accepted by the Company).

The Company applies enhanced verification procedures to deposits made via High Risk payment methods. The Company reserves the right to refuse deposits from any payment method at its sole discretion.

29. Internal AML Escalation Workflow

The Company follows a structured internal escalation process for suspected AML/CTF activity:

Step 1. Detection: Suspicious activity is identified through automated transaction monitoring systems, manual review, staff observation, or external notification.

Step 2. Internal Report: The detecting employee or system generates an internal suspicious activity report and forwards it to the AMLCO.

Step 3. AMLCO Review: The AMLCO conducts a preliminary investigation, reviews all available information, and determines whether the suspicion is substantiated.

Step 4. Account Action: If the suspicion is substantiated, the AMLCO may order account freezing, withdrawal suspension, position closure, and enhanced monitoring.

Step 5. SAR Filing: If the investigation confirms reasonable grounds for suspicion, the AMLCO files a Suspicious Activity Report (SAR) with the relevant Financial Intelligence Unit (FIU) or regulatory authority.

Step 6. Ongoing Monitoring: The account remains under enhanced monitoring. The Company cooperates fully with any subsequent investigation by law enforcement or regulatory authorities.

Step 7. Resolution: Based on the outcome of the investigation, the Company may permanently terminate the account, release funds, or take any other action deemed appropriate.

The Company maintains detailed records of all escalation actions, AMLCO decisions, and SAR filings for a minimum of five (5) years.

30. Internal AML Investigation Framework

When conducting an internal AML investigation, the AMLCO has the authority to:

– Access all Client account records, trading history, and communication logs;
– Request additional documentation from the Client;
– Engage external compliance consultants or forensic specialists;
– Coordinate with other entities in the Company's group;
– Share information with relevant regulatory authorities and law enforcement;
– Make binding decisions regarding account status, fund disposition, and reporting.

All internal investigations are conducted confidentially. The Company is not obligated to inform the Client that an investigation is underway ("tipping off" is prohibited under AML regulations). Investigation records are maintained for a minimum of five (5) years after the investigation is concluded.

31. Client Indemnification

The Client agrees to indemnify, defend, and hold harmless the Company, its directors, officers, employees, agents, and affiliates from and against any and all claims, losses, damages, liabilities, costs, and expenses (including reasonable legal fees) arising from or in connection with:

– Fraud, misrepresentation, or identity theft committed by or attributed to the Client;
– Deposits made with stolen, fraudulent, or unauthorized payment methods;
– Chargebacks, payment reversals, or disputed transactions initiated by or on behalf of the Client;
– Money laundering, terrorist financing, or any other financial crime committed by the Client;
– The Client's breach of any representation, warranty, or obligation under this AML Policy, the Client Agreement, or Terms & Conditions;
– Any third-party claim arising from the Client's use of the Company's services.

This indemnification obligation survives the termination or closure of the Client's account indefinitely.

32. Right to Refuse Service

The Company reserves the right to refuse to establish a business relationship, decline to open an account, reject a deposit, or refuse to provide any service to any person or entity, at any time, with or without explanation. The Company is not obligated to disclose the reasons for any refusal.

The Company may exercise this right based on AML risk assessment, KYC deficiencies, sanctions screening, adverse media results, internal risk policies, or any other factor at the Company's sole discretion.

33. Execution-Only Service

The Company provides execution-only brokerage services. The Company does not provide investment advice, portfolio management, fiduciary services, or personal recommendations. No communication from the Company, including market analysis, research, or educational content, shall be construed as investment advice.

The Client is solely responsible for all trading decisions and acknowledges that the Company bears no responsibility for the outcome of any trade or investment decision made by the Client.

34. Client Representations on Source of Funds

The Client represents and warrants that:

– All funds deposited with the Company are derived from lawful sources;

– The Client is the legal and beneficial owner of all deposited funds;

– No funds deposited originate from criminal activity, money laundering, terrorist financing, tax evasion, fraud, or any other illegal source;

– The Client's trading activity does not constitute an attempt to launder money, finance terrorism, or evade sanctions.

The Client agrees to provide documentary evidence of source of funds and source of wealth upon request by the Company. Failure to provide such documentation may result in account suspension, fund freezing, and account termination.

35. Platform Abuse and AML

The Company recognizes that platform and trading abuse may be associated with money laundering activity. The Company reserves the right to void, cancel, or reverse any trades and reverse and withhold any profits where trading activity involves:

– Systematic exploitation of pricing errors, latency, or execution delays;

– Manipulation of platform functionality, APIs, or trading systems;

– Arbitrage abuse across accounts, brokers, or platforms;

– Use of automated tools or algorithms designed to exploit system vulnerabilities;

– Any activity the Company determines is inconsistent with legitimate trading.

The Company may report such activity to regulatory authorities and law enforcement where it suspects a connection to financial crime.

36. Information Sharing with Financial Institutions

The Company may share Client information, including personal data, trading data, KYC documents, transaction records, and AML investigation findings, with:

– Banks and financial institutions;
– Payment service providers (PSPs) and card processors;
– Regulatory and supervisory authorities;
– Financial Intelligence Units (FIUs);
– Law enforcement agencies;
– Courts, arbitrators, and legal advisors;
– Other entities within the Company's corporate group.

Such sharing may occur without prior notice to the Client where required by law, regulatory obligation, or the Company's AML/CTF procedures. The Client consents to such sharing as a condition of using the Company's services.

37. Governing Law and Jurisdiction

This AML Policy and all matters arising from or in connection with it shall be governed exclusively by the laws of the Union of Comoros.

Any dispute arising from this AML Policy or the Company's AML/CTF procedures shall be subject to the exclusive jurisdiction of the courts of the Union of Comoros. The Client irrevocably submits to such jurisdiction and waives any objection to the exercise of jurisdiction by the courts of the Union of Comoros.

The Client waives any right to bring claims related to the Company's AML/CTF actions in any jurisdiction other than the Union of Comoros.

38. FATF Compliance

The Company's AML/CTF framework is designed to comply with the Financial Action Task Force (FATF) standards, including:

– The FATF 40 Recommendations on combating money laundering and terrorist financing;
– The FATF Risk-Based Approach to AML/CTF supervision and compliance;
– The FATF Travel Rule (Recommendation 16), where applicable to virtual asset transfers, requiring the collection and transmission of originator and beneficiary information;
– FATF guidance on virtual assets and virtual asset service providers (VASPs).

The Company monitors FATF publications, mutual evaluation reports, and updates to the FATF grey list and black list, and adjusts its risk assessments and procedures accordingly.

39. AML Monitoring Tools and Technology

The Company deploys automated AML monitoring tools and technology to ensure effective detection and prevention of financial crime, including:

– Sanctions screening software integrated into the onboarding process and ongoing monitoring;

– Automated transaction monitoring systems with rule-based and behavioral detection capabilities;

– Fraud detection systems analyzing deposit patterns, withdrawal behavior, and trading activity;

– Behavioral monitoring tools tracking platform usage, login patterns, and device characteristics;

– Name matching and fuzzy logic screening against global watchlists and PEP databases;

– Case management systems for internal investigations and SAR preparation.

The Company continuously evaluates and upgrades its AML technology infrastructure to maintain compliance with evolving regulatory standards and emerging financial crime typologies.

40. PEP Approval and Monitoring Procedure

The Company applies a structured approval and monitoring procedure for Politically Exposed Persons (PEPs), their family members, and known close associates:

– Step 1: PEP status is identified through automated screening against commercial PEP databases during onboarding and on an ongoing basis;

– Step 2: Enhanced Due Diligence (EDD) is conducted, including verification of source of funds, source of wealth, and the nature of the business relationship;

– Step 3: Senior Compliance Officer or AMLCO approval is required before the account is opened or the business relationship is continued;

– Step 4: The account is placed under continuous enhanced monitoring with lower transaction thresholds for alerts;

– Step 5: Periodic review of the PEP relationship is conducted at least annually, or more frequently if risk indicators change.

The Company reserves the right to decline to establish or to terminate a business relationship with any PEP where the risk is deemed unacceptable.

41. Cryptocurrency and Virtual Asset AML Procedures

The Company recognizes that cryptocurrency and virtual asset transactions present elevated AML/CTF risks. The following additional procedures apply to all cryptocurrency-related deposits and withdrawals:

– Blockchain analysis: The Company utilizes blockchain analytics tools (such as Chainalysis, TRM Labs, Elliptic, or equivalent providers) to trace the origin and destination of cryptocurrency transactions;

– Wallet screening: Client cryptocurrency wallet addresses are screened against known sanctioned, darknet, mixer, and high-risk wallet databases;

– Enhanced source of funds: Clients depositing via cryptocurrency are required to provide additional source of funds documentation, including proof of cryptocurrency acquisition;

– Transaction monitoring: Cryptocurrency transactions are subject to heightened monitoring thresholds and may trigger additional verification requirements;

– Conversion tracking: Where cryptocurrency is converted to fiat currency or vice versa, the Company maintains records of all conversion details.

The Company reserves the right to refuse, delay, or reverse any cryptocurrency transaction where blockchain analysis or wallet screening identifies risk indicators.

42. Cooperation with Financial Institutions and Authorities

The Company is committed to full and transparent cooperation with:

– Correspondent banks and banking partners;
– Payment service providers (PSPs) and card processors;
– The Anjouan Offshore Finance Authority (AOFA), Union of Comoros;
– Financial Intelligence Units (FIUs) in relevant jurisdictions;
– Law enforcement agencies conducting financial crime investigations;
– Regulatory authorities and supervisory bodies;
– Courts, arbitrators, and legal counsel.

The Company will respond to information requests, production orders, and regulatory inquiries promptly and in full compliance with applicable law. The Company may share Client data, transaction records, KYC documentation, and investigation findings with any of the above entities without prior notice to the Client where required by law or regulatory obligation.

The Company maintains a designated point of contact for law enforcement and regulatory communications within the Compliance Department.

43. Money Laundering Reporting Officer (MLRO)

The Company has designated a Money Laundering Reporting Officer (MLRO) in addition to the Anti-Money Laundering Compliance Officer (AMLCO). The MLRO and AMLCO functions may be performed by the same individual where appropriate for the size and complexity of the Company's operations.

The MLRO is responsible for:

– Receiving and evaluating internal Suspicious Activity Reports (SARs) from Company employees;
– Making the decision on whether to file external SARs with the relevant Financial Intelligence Unit (FIU);
– Maintaining the SAR register and ensuring timely filing;
– Acting as the primary point of contact for law enforcement and regulatory authorities on AML matters;
– Reporting to the Board of Directors on AML/CTF matters.

The MLRO has the authority to freeze accounts, suspend transactions, and escalate matters independently of the Company's commercial operations.

44. KYC Verification Technology

The Company utilizes industry-leading automated identity verification and KYC technology providers to ensure accurate, efficient, and compliant client onboarding. The Company may use one or more of the following providers (or equivalent alternatives):

– Sumsub --- automated identity verification, document verification, liveness detection, and AML screening;
– Veriff --- AI-powered identity verification and biometric analysis;
– Jumio --- document verification, facial recognition, and identity proofing;

– Onfido --- document and biometric verification;

– Or any other provider meeting the Company's compliance standards.

KYC verification technology is integrated into the Company's onboarding workflow and may also be used for ongoing verification, re-verification, and enhanced due diligence purposes.

45. AML Compliance Technology Stack

The Company deploys a comprehensive AML compliance technology stack, which may include one or more of the following tools and providers (or equivalent alternatives):

– Chainalysis / TRM Labs / Elliptic --- blockchain analytics and cryptocurrency transaction monitoring;

– Dow Jones Risk & Compliance --- sanctions screening, PEP screening, and adverse media monitoring;

– Refinitiv World-Check --- global risk intelligence and screening;

– ComplyAdvantage --- real-time AML data and transaction monitoring;

– LexisNexis Risk Solutions --- identity verification and fraud prevention;

– Internal proprietary monitoring systems --- rule-based and behavioral transaction monitoring.

The Company continuously evaluates its technology stack and may add, replace, or upgrade providers to maintain compliance with evolving regulatory requirements and industry best practices.

46. Independent AML Audit

The Company conducts an independent AML/CTF audit at least annually. The audit is performed by an external compliance consultant, auditor, or specialized AML advisory firm independent of the Company's operations.

The scope of the annual AML audit includes:

– Review of the Company's AML/CTF policies and procedures;

– Assessment of KYC/CDD and EDD processes;

– Evaluation of transaction monitoring effectiveness;

– Review of SAR filing procedures and timeliness;

– Assessment of sanctions screening processes;

– Review of staff training and awareness programs;

– Testing of AML technology and systems;

– Identification of gaps, deficiencies, and recommendations for improvement.

Audit findings and recommendations are reported to the AMLCO, MLRO, and Board of Directors. Corrective actions are implemented within agreed timelines and tracked to completion.

47. AML Training Program

All Company employees, contractors, and relevant third parties receive mandatory AML/CTF training:

– Initial training: within 30 days of joining the Company;

– Annual refresher training: mandatory for all staff, conducted at least once per calendar year;

– Ad-hoc training: when significant regulatory changes, new typologies, or identified deficiencies require immediate attention;

– Role-specific training: enhanced training for compliance staff, senior management, and employees in client-facing or high-risk roles.

Training covers: recognition of suspicious activity, KYC/CDD procedures, internal reporting obligations, sanctions compliance, PEP handling, cryptocurrency AML risks, and regulatory updates.

Training completion is documented and records are maintained for a minimum of five (5) years. The AMLCO monitors training compliance and reports to the Board annually.

48. Banking and Correspondent Relationship Cooperation

The Company is committed to maintaining transparent and cooperative relationships with its banking partners, correspondent banks, payment service providers, and financial intermediaries.

The Company will:

– Respond promptly and fully to information requests from banking partners;
– Provide KYC documentation, transaction records, and AML compliance information as requested;
– Facilitate on-site visits or remote due diligence reviews by banking partners;
– Notify banking partners of material changes to the Company's AML/CTF policies or risk profile;
– Cooperate in joint investigations where suspicious activity affects shared clients or transaction flows;
– Maintain a designated banking relationship contact within the Compliance Department.

The Company recognizes that maintaining strong banking relationships is essential to its operations and is committed to exceeding the AML/CTF expectations of its financial partners.

49. Contact

For any questions regarding this AML Policy or to report suspicious activity, please contact:

AML Compliance Officer: compliance@neomaaa.com Email: support@neomaaa.com Address: Hamchako, Mutsamudu, The Autonomous Island of Anjouan, Union of Comoros Neomaaa Ltd Trading as NEOMAAA International Business Company No. 15968 International Brokerage License Number L15968/N *© 2025--2026 Neomaaa Ltd. All rights reserved.* Contact Information Company: Neomaaa Ltd Email: support@neomaaa.com Compliance: compliance@neomaaa.com Website: neomaaa.com Address: Hamchako, Mutsamudu, The Autonomous Island of Anjouan, Union of Comoros Licensed and authorized by the Anjouan Offshore Finance Authority (AOFA), Union of Comoros.

Acknowledgement

By using the Company's services, the Client acknowledges having read, understood and accepted the AML Policy.

Neomaaa Ltd
Trading as NEOMAAA
International Business Company No. 15968
Regulated by the Anjouan Offshore Finance Authority (AOFA), Union of Comoros

Contact Information

Company: Neomaaa Ltd
Email: support@neomaaa.com
Compliance: compliance@neomaaa.com
Website: neomaaa.com
Address: Hamchako, Mutsamudu, The Autonomous Island of Anjouan, Union of Comoros