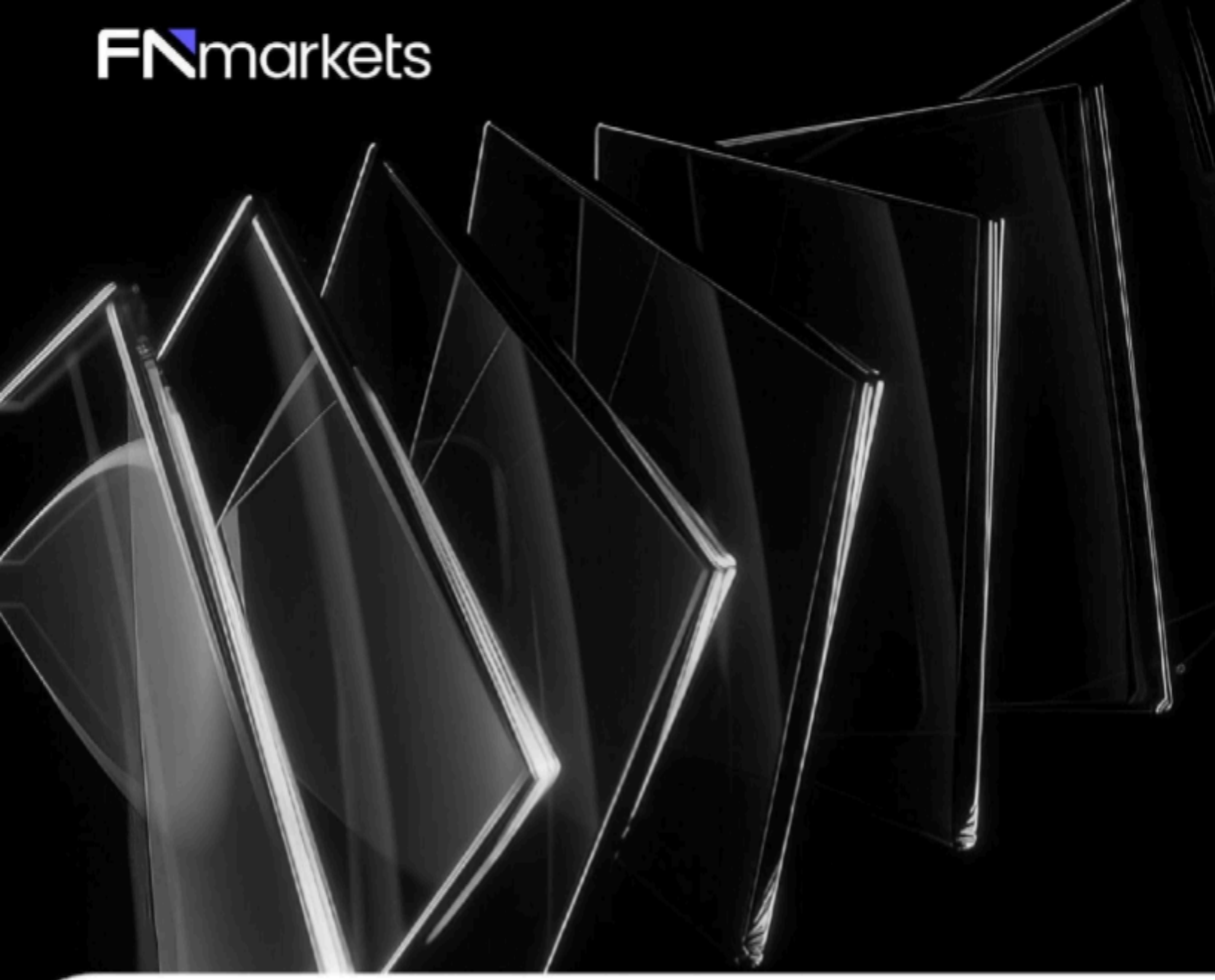
FNmarkets



AML Policy

AML/CTF Program

1. Customer Identification and Verification

The AML/CTF Program sets out the Customer identification and verification procedures (also referred to as “Know your Customer” or “KYC” procedures). The AML/CTF framework of the Union of the Comoros requires any Reporting Entity (such as the Company) to carry out procedures to verify a customer’s identity before providing a designated service to that customer, and ongoing due diligence of customers must be conducted.

Accordingly, the primary purpose of this AML/CTF Program is to set out the applicable customer identification and verification procedures for customers of the Company.

The level of information that must be collected is dependent on the identified ML/TF risk posed to the Company, having regard to the following factors:
Its customer types include:

- Beneficial owners of customers;
- Any Politically Exposed Persons (refer to paragraph 4.1.4);
- Its customers’ sources of funds and wealth;
- The nature and purpose of the business relationship with its customers, including, as appropriate, the collection of information relevant to that consideration;
- The control structure of its non-individual customers;
- The types of designated services provided;
- The methods by which the designated services are delivered.
- The foreign jurisdictions with which it deals.

The Company considers it important and seeks to assess the risk posed by each customer (as opposed to overall risks faced by the Company in respect to customers). This enables the Company to classify the risk posed by each customer as either low, medium, or high. If the risk cannot be clearly determined, then the Company will rely on the risk assessment performed generally with respect to its customers.

In addition, in developing this AML/CTF Program, compliance with the Anti-Money Laundering and Counter-Terrorism Financing laws of the Union of the Comoros and applicable FATF standards was considered.

Of note, there are different customer identification and verification procedures for different customer types.

2. Customers

Customers include the following:

- Individuals;
- Companies;
- Customers who act in the capacity of a trustee of a trust;
- Customers who act in the capacity of a member of a partnership;
- Incorporated associations;
- Unincorporated associations;
- Registered co-operatives;
- Government bodies.

3. Agents

The Company may authorise another person to be its agent for the purposes of carrying out applicable customer identification (and verification) procedures on its behalf. Clearly, these procedures must be carried out in accordance with the AML/CTF framework of the Union of the Comoros.

In this case, there must be a written agreement in place for the management of the customer identification (and verification) records whereby the Company has access to the records made by the agent and may request a copy of the records made by the agent.

4. Intermediaries

The company can accept that the customer identification procedure has been carried out in respect of the customer by the other Reporting Entity, i.e., the intermediary, if:

- An intermediary (that is, a Reporting Entity, being a licensed financial adviser) carried out the applicable customer identification procedures in respect of a particular customer to whom The Company provides (or proposes to provide) a designated service; and
- The customer identification procedure was carried out in accordance with the Anti-Money Laundering and Counter-Terrorism Financing laws of the Union of the Comoros and FATF standards; and
- The Company has obtained a copy of the records made by the intermediary (referring Reporting Entity); OR
- There is an agreement in place for the management of the customer identification records whereby the Company has access to the records made by the intermediary (or the referring Reporting Entity); and

- The Company has determined that it is appropriate for it to rely upon the applicable customer identification procedures carried out by the intermediary, having regard to the ML/TF risk faced by the Company relevant to the provision of its services to the customer; and
- Such other conditions set out in the Comoros AML/CTF laws (if any) are satisfied.

Then the company can accept that the customer identification procedure has been carried out in respect of the customer by the other Reporting Entity i.e., the intermediary.

Based on the nature of the Company's business, it is unlikely that it will seek to rely on another Reporting Entity to carry out the applicable customer identification procedures. However, the above is provided for information purposes.

5. Timing of Identification

5.1 New Customers

All new customers are to be identified and their identification verified, in accordance with the procedures set out in this AML/CTF Program, prior to the provision of any designated services.

5.2 Pre-commencement

Identification procedures may be required in respect of certain customers in certain circumstances (refer to paragraph 2.12 below).

5.3 Effective Date

All new customers are required to be identified and their identification verified BEFORE any designated service is provided to them.

Further, where a review of a customer, business line, or other circumstance results in a change in the risk profile of an existing customer, then the customer identification procedures described in this AML/CTF Program are required to be implemented according to the assessed risk.

5.4 Customer Identification and Risk Management

Customer identification (also referred to as Know Your Customer or "KYC") is an essential element in the ML/TF risk management process. The Company recognises that there is a risk to its business, including regulatory risks (of non-compliance with legislation) and a risk to its reputation should prospective or existing customers seek to utilise services offered by the Company for money laundering purposes or terrorism financing.

In accordance with the Anti-Money Laundering and Counter-Terrorism Financing laws of the Union of the Comoros and applicable FATF standards, the Company has adopted procedures (as set out in this AML/CTF Program) that are risk-based.

Representatives (or more generally, agents or intermediaries) will collect minimum KYC information from customers and perform risk assessment and verification procedures prior to accepting the customer.

Representatives (or agents or intermediaries) of the Company will record the KYC information, the verification methods used, and the results of such verification in a central depository.

Where further information is required from customers, representatives of the Company (or its agents or intermediaries) will make formal requests for additional information and will carry out a check of the customer against public data.

6. Who will be Identified

The Company has determined that it will identify and verify the person (or entity) who is the named "investor" (account holder), including beneficial owners and any person (or entity) that has control of “the account” (investment).

In other words, the Company considers that those people who can give instructions to it (such as an agent of the customer or a person who the customer has authorised to act on their behalf) as to the operation of the account, also need to be identified and verified.

7. Customer Identification and Verification

The Anti-Money Laundering and Counter-Terrorism Financing laws of the Union of the Comoros (in particular, relevant provisions on customer due diligence) are prescriptive as to the level of identification and verification procedures required.

Prior to establishing a relationship with a customer (i.e., opening an account), representatives (or the appointed agent of the Company or an intermediary) will collect the minimum KYC information and documents to verify the identity of the customer.

The information and supporting documentation will vary depending on the customer type and that customer’s risk profile.

The documented identification and verification procedures are mandatory and must not be deviated from. They are designed to ensure that the Company is reasonably satisfied as to the identity/existence of the customer, and in the case of non-individual customers, information is collected and verified in respect of beneficiaries, members of governing bodies, and beneficial owners.

Depending on the information obtained or the nature of the customer, additional information and/or verification may be required. Additional information may be required from the customer with regard to:

- The prospective customer type, including beneficial owners of the customer and whether the person is a Politically Exposed Person ("PEP");
- The customers' sources of funds and wealth;
- The nature and purpose of the business relationship with its customers, including, as appropriate, the collection of information relevant to that consideration;
- The control structure of its non-individual customers;
- The products and designated services to be provided;
- The delivery methods by which designated services will be provided;
- The foreign jurisdiction.

The Company seeks to determine the ML/TF risk posed by each customer as opposed to the overall risks faced by the Company with respect to customers for the provision of its designated services.

The risk ranking procedure must be utilised by representatives (or agents or intermediaries) to categorise (or rank) a new customer and assess that new customer's risk profile as being high, medium, or low.

8. How Information is Verified

Some of the information collected must be verified to ensure that the Company is reasonably satisfied as to the identity of its customer. This includes being reasonably satisfied that:

- The customer exists or is who he/she claim to be (for all customer types);
- The names and either the date of birth or address of each ultimate beneficial owner have been verified, excluding a customer, which is:
    - A domestic listed public company and its majority-owned subsidiary companies;
    - A licensed company subject to regulatory oversight of the Union of the Comoros or another FATF-equivalent jurisdiction;
    - A trust or managed investment scheme that is registered and subject to regulatory oversight under the laws of the Union of the Comoros or another FATF-equivalent jurisdiction;
    - A trust that is an unregistered managed investment scheme that only has wholesale clients;
    - A Government superannuation fund established under the laws of the Union of the Comoros or another FATF-equivalent jurisdiction;

    - A Government entity of the Union of the Comoros or another FATF-equivalent jurisdiction;
    - A customer who is a foreign listed public company subject to disclosure requirements (whether by stock exchange rules or by law or enforceable means) to ensure transparency of beneficial ownership that are, or are comparable to, FATF-recognised international standards.
- The name of each trustee and beneficiary or a description of each class of beneficiary is provided.
- The names and addresses of all partners are provided (for partnerships).
- The names of members of governing committees are provided (for associations). In the case of an unincorporated association, the person who has been identified in accordance with the KYC procedures for individuals is the customer of the Company, i.e., in his/her capacity as a member of the association.

Customer identity must be verified through:

- Believable and independent documentation;
- Reliable and independent electronic data; or
- Both of the above.

Reliable and independent documentation will generally be used to verify customer identity when appropriate documents are available, or alternatively, electronic means will be used (using a reputable vendor).

The Company has developed Customer Identification Procedures Checklists. In developing these Checklists, the Company has determined, using appropriate risk-based systems and controls:

With respect to individuals:

- That the Company is satisfied that any document from which it verifies KYC information collected from a customer has not expired (with the exception that a government-issued passport may be accepted if expired within the preceding two years, provided it is issued by the Union of the Comoros or another FATF-equivalent jurisdiction);
- What reliable and independent documentation will the Company require a customer to produce for the purpose of verifying the customer's name and date of birth, and/or residential address (as the case may be)?
- If any other KYC information collected from a customer is to be verified, what reliable and independent documentation may be used to verify that information?
- Whether, and in what circumstances, the Company is prepared to rely upon a copy of a reliable and independent document (rather than the original or a certified copy);

- In what circumstances the Company will take steps to determine whether a document produced by a customer may have been forged, tampered with, cancelled, or stolen, and, if so, what steps it will take to confirm whether or not the document has been forged, tampered with, cancelled, or stolen;
- Whether the Company will use any authentication service that may be available in respect of a document; and
- Whether and how to confirm KYC information collected from a customer by independently initiating contact with the person that the customer claims to be.

With respect to prospective customers other than individuals:

- What and how many reliable and independent documents the Company will use for the purpose of verification;
- Whether a document is sufficiently contemporaneous for use in verification;
- Whether, and in what circumstances, the Company is prepared to rely upon a copy of a reliable and independent document (rather than the original or a certified copy);
- In what circumstances will the Company take steps to determine whether a document produced by a customer may have been cancelled, forged, tampered with, or stolen, and, if so, what steps the reporting entity will take to confirm whether or not the document has been cancelled, forged, tampered with, or stolen;
- Whether the Company will use any authentication service that may be available in respect of a document; and
- Whether and how to confirm information about a customer by independently initiating contact with the customer.

Reliable and independent electronic data may also be obtained if a representative (or agent or intermediary) is still uncertain about the true identity of the customer (even after obtaining documentary evidence from the customer).

In verifying the customer's identity, any inconsistencies in the information obtained must be analysed.

In analysing the information (or documentation), the Company will consider whether there is a logical reason and consistent support (information) amongst the data provided, such as the customer’s name, street address, postcode, and date of birth, which appear to be consistent with verification independent checks.

9. Discrepancies

If a discrepancy exists between information collected and verifying documents, then the Company (or its agent or intermediary) will take steps to resolve the discrepancy (where possible) and will record the steps taken.

Where the discrepancy is material, the action to be taken will depend upon the discrepancy and will vary according to customer type and that customer's risk profile.

10. Disclosure Certificates

Where information is to be verified and it is not otherwise reasonably available from independent verification sources, a Disclosure Certificate may be provided by the customer (other than where the customer is an individual or a Government body established under the laws of the Union of the Comoros or another FATF-equivalent jurisdiction). This will constitute a reliable and independent document.

The Disclosure Certificates accepted by the Company are only for those customers who have been classified or ranked as low to medium risk.

A Disclosure Certificate will not be accepted as suitable evidence to verify information where factors exist that result in the elevation of the ML/TF risk and the customer receives a high risk classification (ranking).

In these circumstances where the identity cannot be readily verifiable to the reasonably satisfaction of The Company (or its agent or intermediary), the matter will be referred to a senior manager, who, in consultation with the AML/CTF Compliance Officer, will determine whether The Company will accept the transaction (i.e., enter into a customer relationship).

11. When will Additional KYC Information be Required

Based on an assessment of ML/TF risk, the Company has identified certain risk variables that will trigger the requirement for additional KYC information and verification procedures to be performed (these depend upon customer type and that customer's risk profile).

The risk variables are:

- Where the investor is physically present in, or is a corporation incorporated in, foreign jurisdictions identified as high-risk by the Union of the Comoros authorities, FATF-recognised lists, or credible international sources;
- Where the Company is entering into (or proposing to enter into a transaction) and the party to the transaction is physically present in, or is a corporation

incorporated in, foreign jurisdictions identified as high-risk by the Union of the Comoros authorities, FATF-recognised lists, or credible international sources;

- Where the prospective customer (natural person, director, member of governing body, beneficiary or beneficial owner) is named in a sanctions list issued by the Union of the Comoros, the United Nations, or another FATF-recognised authority;
- Where the risk of terrorism is identified;
- Where the customer or a beneficial owner is a PEP or an immediate family member or close associate of a PEP;
- Foreign jurisdiction risk (individuals and non-natural persons), i.e., the place where the customer is domiciled (located). In the case of a non-natural person, this includes officers and beneficial owners, and beneficiaries;
- In the case of a listed company, the foreign jurisdiction risk with respect to the location of the exchange on which the listed company is traded;
- The customer or beneficial owner has sophisticated activities and/or has links with high-risk foreign jurisdictions;
- The customer's or beneficial owner's business activities place it in a higher risk category;
- Where intermediaries exist that are not Reporting Entities;
- Where intermediaries exist that are Reporting Entities, and the Company does not have access to the record made by the intermediary, and/or there is no agreement in place for the management of the customer identification records with that Reporting Entity.

In addition to the above, based on an assessment of ML/TF risk, the Company has identified certain risk variables that may trigger the requirement for additional KYC information and verification procedures to be performed (these depend upon customer type and that customer's risk profile).

The risk variables are:

- Where the prospective customer is not physically present for identification purposes;
- Complex customer structures with numerous layers, e.g., trusts;
- The customer structure does not support the disclosed business of that customer, e.g., in the case of partnerships;
- Products & services risk;
- Services are provided via the internet.

12. Customer Refusing to Provide Information

If a prospective customer either refuses to provide information when requested or appears to have intentionally provided misleading information, the Company will not accept the Application Form (i.e., open the account) and will not do business with that prospective customer until the information has been provided and the customer identification and verification procedures as contained in this AML/CTF Program have been satisfactorily completed.

If an existing customer either refuses to provide information when requested or appears to have intentionally provided misleading information, then the Company, after considering the circumstances and ML/TF risks involved, will consider closing the account.

In either case, the AML/CTF Compliance Officer will be notified in order to determine whether the circumstances constitute a reportable matter and whether the risk classification of the customer should be increased.

13. Customer's True Identity

If a representative (or agent or intermediary) forms a reasonable belief that, based on the documentation provided, the prospective customer is not who he/she/they purports to be, then to be reasonably satisfied as to the customer's true identity the representative (or agent or intermediary) must, within 14 days of forming this belief:

- Collect additional KYC information with respect to the customer;
- Verify the KYC information already obtained from a reliable and independent electronic data source.

The AML/CTF Compliance Officer must be notified of the circumstances, and he will carefully consider the risk classification of the prospective customer.

14. Lack of Verification and Tolerances

The Company recognizes that there are prospective customers who are not able to provide the required verification documents or may not exist on electronic databases, such as the Land Titles Office, e.g., individuals who live in rented accommodation.

Where the Company cannot be reasonably satisfied as to the identity of the customer, then the Board has determined that it will not enter into a customer relationship with the person.

Such cases are to be referred to the AML/CTF Compliance Officer, who in turn, will also determine whether the circumstances are suspicious and may refer the matter to the

Compliance Committee and the Board and the Financial Intelligence Unit (FIU) of the Union of the Comoros or other relevant authorities as required by law.

15. Forgery

Representatives (or agents or intermediaries) responsible for the collection and verification of KYC information are not required to investigate whether a document provided by a customer has been validly issued. For example, representatives (or agents or intermediaries) can rely on documents issued by a governmental or statutory body as reliable and independent documentation and thus, verification of a customer's identity.

If, however, the document exhibits signs of fraud (tampering with the document), then the matter must be immediately reported to the AML/CTF Compliance Officer, and he will consider the factors in determining whether the Company can form a reasonable belief as to the customer's true identity.

16. Recording the Collection and Verification Procedure

Representatives (or agents or intermediaries) responsible for the collection and verification of customer identification will record the verification procedure, including all identifying information provided by a customer, details of the verification methods used, and the results of the verification.

Further, where a discrepancy arises (in the verification process), representatives (or agents or intermediaries) will record the method and result of the resolution of any discrepancy in identifying and verifying information.

Where reliance is placed on a document produced by the customer, a copy of that document is to be retained as part of the records. If representatives (or agents or intermediaries) obtain documents from electronic databases or from consumer agencies, copies of those documents are also to be retained.

Any additional information or verification procedures are to be documented, and copies of any supporting documents (evidence) provided by the customer or obtained electronically by representatives (or agents or intermediaries) are to be retained as part of the records.

All customer identification records and any records made in respect of the verification process must be retained for seven years after the closure of the customer account.

17. Requests for Information from Customers

If the Company determines that a prospective (or existing) customer has information that is likely to assist it in assessing, mitigating, and managing its ML/TF risk, then the Company will provide notice to the prospective (or existing) customer requesting that information from them in accordance with the laws of the Union of the Comoros. For example, a corporate customer may have a complex business structure for which the identification of the underlying beneficial owner is not readily identifiable. In this situation, requests will be made to the customer requesting clarity as to the structure.

The format for such requests will be as follows:

18. Customer Identification Procedure

Purpose

To ensure that every customer of the Company is properly identified and verified before services are provided, in line with the AML/CTF laws of the Union of the Comoros (2020) and FATF standards.

18.1 When this procedure applies

Customer identification is required when:

- A new account application is submitted;
- An individual requests to be added as a signatory or authorised user;
- There is a material change in ownership, control, or structure of an existing customer (e.g., new shareholder, director, trustee);
- Red-flags or risk triggers are detected, such as:
    - Customer linked to a high-risk jurisdiction,
    - Potential PEP involvement,
    - Complex or unusual transaction activity.

18.2 Information and documents to be collected

For Individuals:

- Government-issued photo ID (passport, national ID, driver’s licence);
- Proof of residential address (utility bill, bank statement, government letter, dated within last 3 months);
- Date of birth, nationality, and occupation.

For Companies:

- Certificate of Incorporation/Business Registration;
- Memorandum & Articles of Association (or equivalent);
- List of directors;
- Shareholder/beneficial owner details (anyone with ≥25% ownership or control);
- Proof of registered business address.

For Trusts/Partnerships/Associations:

- Trust deed or partnership/association agreement;
- Details of trustees/partners/committee members;
- Identification of all beneficiaries or classes of beneficiaries;
- Verification of beneficial owners.

18.3 Verification standards

- Documents must be current, valid, and independently issued.
- Where copies are provided, they must be certified or verified through an independent, reputable source.
- First payments must be made from a bank account in the customer's name at a bank regulated in Comoros or another FATF-equivalent jurisdiction.
- Where identity cannot be confirmed with certainty, the account will not be opened until the AML/CTF Compliance Officer approves.

18.4 Escalation and non-compliance

If required documents are not received within 14 calendar days:

- Account opening will be suspended;
- Existing accounts may be restricted until verification is complete;
- If refusal continues, the relationship will be terminated and the case escalated to the AML/CTF Compliance Officer.

Where identity cannot be established or suspicion of ML/TF exists:

- The matter will be escalated to senior management;
- A Suspicious Activity Report (SAR) may be filed with the Financial Intelligence Unit (FIU) of the Union of the Comoros.

18.5 Record keeping

All KYC information, documents, verification evidence, and correspondence must be stored securely for seven (7) years after account closure. Records must be easily retrievable in case of audit or regulatory inspection.

Template wording for customer notice

Subject: Request for Identification Documents

Dear [Customer Name],

In accordance with the Anti-Money Laundering and Counter-Terrorism Financing laws of the Union of the Comoros, FNmarkets is required to verify the identity of all customers.

Please provide the following documents within 14 days:

- [List documents needed – e.g., passport, proof of address, company registration, beneficial owner ID].

If we do not receive the required documents within the specified time, we may suspend or refuse to provide services until verification is completed.

Thank you for your cooperation.

Sincerely,
FNmarkets Compliance Team

19. Standard for Electronic Data

The Company considers that data obtained from official government sources of the Union of the Comoros or other FATF-equivalent jurisdictions (refer to paragraph 4.4 below) is reliable and independent and thus a suitable electronic data source to be used for verification purposes.

The Company has determined that it will also accept electronic data available from Authorized Service Providers (commercial carriers), provided the following criteria are met:

- The carrier is authorized to store personal data.
- The carrier uses a range of information sources that can be called upon to link an applicant to both current and previous circumstances.
- The carrier accesses negative information sources, such as databases relating to identity fraud and deceased persons.

- The carrier accesses a wide range of alert data sources.
- The process is transparent, i.e., what checks were carried out, details of the results, and the level of certainty as to the identity of the prospective customer.

20. Copies of Identification Documents

Where possible, identification documents provided by a prospective customer should be originals or certified copies. Where a customer provides copies of identification documents, there is a risk of identity fraud. As a result, additional information is to be collected and verified when copies of identification documents are only provided using one or more of the following methods:

- Contacting a customer by telephone prior to opening the account on a home or business number that has been verified (electronically or otherwise).
- Contacting the customer by telephone prior to them being authorised to transact to welcome them. One of the purposes of this call is to verify additional aspects of personal identity information that have been previously provided.
- Requiring that the first payment for a transaction be carried out from an account in the customer's name held in a bank regulated in the Union of the Comoros or another FATF-equivalent jurisdiction.

21. Electronic Identification

Where a customer provides identification information electronically, there is a risk of identity fraud. As a result, additional information is to be collected and verified when identification documents are only provided electronically using one or more of the following methods:

- Obtain verification of information from a reliable and independent electronic data source.

22. Verifying the Identity of Low to Medium-Risk Prospective Customers

Where the prospective customer is assessed as a low to medium risk and circumstances arise whereby a representative (or agent or intermediary) suspects on a reasonable ground that the customer is not who they claim to be, then the representative (or agent or intermediary) must, within 14 days of forming the suspicion, do one or more of the following:

- Carry out relevant KYC procedures depending on the customer type.
- Collect any additional KYC information in respect of the customer.
- Verify the information from a reliable and independent source.

The representative (or agent or intermediary) may forward a notice (in the format set out in paragraph 2.6 above) requesting the information from the customer.

If, after following the above procedure, the representative (or agent or intermediary) is satisfied as to the customer's true identity, then the procedure is to be recorded and retained in accordance with record-keeping procedures.

If after following the above procedure the representative (or agent or intermediary) is not reasonably satisfied that the customer is who they claim to be, then the Application Form will not be accepted and the account will not be opened until such time that the file has been reviewed by the AML/CTF Compliance Officer and senior management.

A full report is to be provided to the AML/CTF Compliance Officer, who, in consultation with senior management, will determine whether the account should be opened or whether the circumstances are suspicious enough to warrant the application being rejected and to determine whether it is a reportable matter.

23. Verifying the Identity of High-Risk Customers

The Company has implemented an enhanced Customer Due Diligence program to assess and collect further customer information in situations where it determines that:

- There is a high risk of ML/TF arising when providing a designated service to a customer.
- The customer is, or has a beneficial owner who is, a foreign PEP;
- The Company is entering into (or proposing to enter into a transaction) and the party to the transaction is physically present in, or is a corporation incorporated in, a foreign jurisdictions identified as high-risk by the Union of the Comoros authorities, FATF-recognised lists, or credible international sources; or
- One of the grounds for reporting a suspicious matter to the Financial Intelligence Unit (FIU) of the Union of the Comoros has been met.

Where the prospective customer is assessed (ranked) as a high risk and circumstances arise whereby a representative (or agent or intermediaries) suspects on reasonable grounds that the customer is not who they claim to be, then the customer will not be accepted and the account will not be opened.

A full report is to be provided to the AML/CTF Compliance Officer immediately, who, in consultation with senior management, will consider the circumstances and whether they are suspicious enough to confirm the application should be rejected and to determine whether it is a reportable matter.

24. Verification Procedures for Existing Customers

If at any time, in providing a designated service to an existing customer, a circumstance arises whereby:

- A representative suspects on reasonable grounds that the customer is not who they claim to be, or
- A suspicious matter reporting obligation arises for the Company in relation to that customer.

Then the representative must, within 14 days of forming the suspicion or the suspicious matter reporting obligation occurring, take one or more of the following actions:

- Carry out relevant customer identification procedures depending on the customer type and risk profile (unless these have already been carried out);
- Collect any additional KYC information in respect of the customer.
- Verify the information from a reliable and independent source.

The representative may forward a request (in the format set out in paragraph 2.6 above) requesting the information from the customer.

If, after following the above procedures, the representative is satisfied as to the customer's true identity, then the details of the procedures are to be recorded and retained in accordance with the record-keeping procedures.

If, after following the above procedures, the representative is not reasonably satisfied that the customer is who they claim to be, then the matter must be brought to the immediate attention of the AML/CTF Compliance Officer.

The AML/CTF Compliance Officer, in consultation with senior management, will determine whether the circumstances are suspicious enough to warrant the account being placed in suspense or rejected, and whether it is a further suspicious matter and thus reportable.

Reliance on due diligence carried out by intermediaries (where that intermediary is a licensed financial advisor only)

The Company may rely on the information collected and verified from an intermediary (acting as a referring Reportable Entity) in complying with its customer identification and verification obligations.

This will only be accepted in the following circumstances:

- The Company has determined that it is appropriate for it to rely upon the applicable customer identification procedures carried out by the intermediary,

having regard to the ML/TF risk faced by the Company relevant to the provision of its services to the customer.

- The intermediary is subject to AML/CTF obligations under the laws of the Union of the Comoros or another FATF-equivalent jurisdiction.
- Where the intermediary makes copies of all verification documents collected and provides such copies to the Company, or an agreement has been entered into whereby the Company has access to the records made by the intermediary.

Reliance on due diligence carried out by an agent (where that agent is another reporting entity)

The Company may authorise another person to be its agent for the purposes of carrying out applicable customer identification (and verification) procedures on its behalf. Clearly, these procedures must be carried out in accordance with the AML/CTF laws of the Union of the Comoros.

The Company may rely on the information collected and verified from an agent (another reportable entity) in complying with its customer identification and verification obligations.

This will only be accepted in the following circumstances:

- The Company has determined that it is appropriate for it to rely upon the applicable customer identification procedures carried out by the agent, having regard to the ML/TF risk faced by the Company relevant to the provision of its services to the customer.
- The agent is subject to AML/CTF obligations under the laws of the Union of the Comoros or another FATF-equivalent jurisdiction.
- Where the agent makes copies of all verification documents collected and provides such copies to the Company, or an agreement has been entered into whereby the Company has access to the records made by the agent.

25. Sharing Information with Agents and Intermediaries

The Company will share information about any customer seeking to utilise its services that it reasonably suspects of terrorist financing and/or money laundering with its appointed agents and any intermediary.

Information will be shared for the purposes of identifying and reporting activities that may involve acts of terrorism and/or money laundering activities, and to determine whether to establish or maintain a customer or engage in a transaction on behalf of that customer.

The Company will follow strict procedures and share only relevant information. The information will be protected, and it will remain confidential by being segregated from its other records.

26. Customer Types (Including Beneficial Owners and PEPs)

26.1 Where a prospective customer is named in a government list or a credible source

The United Nations and the Union of the Comoros are each able to designate persons and entities as being subject to financial sanctions.

Further, in some circumstances, persons and entities are subject to financial sanctions or measures similar to those issued by bodies such as the United Nations, FATF, or government-sanctioned bodies in FATF-equivalent jurisdictions.

Such sanctions and measures can include a prohibition on making funds available to the person or entity, or a more comprehensive asset freeze.

It is a criminal offence to make funds or financial services available to targets subject to an asset freeze either directly or via their agent (lawyer, accountant, or other authorized representative).

Representatives (or agents or intermediaries) responsible for account opening (identifying and verifying prospective customers) may use third-party software to determine whether the person or entity appears on a sanction list. Vendors will only be selected where all relevant lists are kept up to date and the vendors link to UN, Comoros national, and other FATF-recognised sanction lists.

Existing customers will also be screened at regular intervals relevant to the customer's ML/TF risk profile to determine whether the customer's name appears on the relevant lists.

The Company will adhere to all legislative directives issued in connection with such lists, including notification of information to the Financial Intelligence Unit (FIU) of the Union of the Comoros and any other competent enforcement authority.

Where a positive result is returned in respect of a customer (i.e. the name appears on the relevant list), the AML/CTF Compliance Officer must be notified immediately and is responsible for overseeing the ongoing treatment of the customer and, where applicable, making all reports, liaising with enforcement offices, and reporting to the Compliance Committee and the Board.

Any requests for third-party payments will require that the name of the third party be identified, verified, and checked. Where a positive result is returned in respect of a third party payee (i.e. the name appears on the relevant list), the AML/CTF Compliance Officer must be notified immediately and will be responsible for overseeing the ongoing treatment of the customer and, where applicable, making all reports, liaising with enforcement offices, and reporting to the Compliance Committee and the Board.

26.2 Terrorism risk

The Company implements the United Nations Security Council (UNSC) Resolutions 1267 and 1373 through the national counter-terrorism and asset-freezing regulations of the Union of the Comoros.

Assets must be frozen the moment a person or entity is placed on the UN or Comoros national list.

It is a criminal offence to deal with the assets of a person or entity named on a sanction list. The Company may utilise appropriate software in finding possible matches between customers and the names on the relevant lists (i.e., UN sanctions lists, Comoros national sanctions lists, or FATF-equivalent sanctions lists).

If a customer's name is matched to a person or entity named on the relevant lists, then the Company is under an obligation to freeze assets or economic resources.

If a match is found or if it is not clear if there is in fact a direct match, the AML/CTF Compliance Officer is to be notified immediately.

The AML/CTF Compliance Officer will coordinate, under Board supervision, the notification to the FIU of the Union of the Comoros and any other competent enforcement authority in respect of a possible match as the case may be.

27. Politically Exposed Persons (PEP)

A PEP is defined under the Anti-Money Laundering and Counter-Terrorism Financing laws of the Union of the Comoros and consistent with FATF guidance.

A PEP is:

- An individual who is or has been during the preceding three years, entrusted with a prominent public function in:
    - the Union of the Comoros; or
    - any other country; or
    - an international body or organisation.
- An immediate family member of a person referred to above; or
- A close associate of a person referred to above.

PEPs can pose a high money laundering risk as their position makes them vulnerable to bribery and corruption.

A PEP also includes a person who is an immediate family member or close associate to those described above.

27.1 Family members of a PEP include:

- A spouse;
- A de facto partner;
- A child and a child's spouse or de facto partner; or
- A parent.

Close associates of an individual who is a PEP means any individual who is known (having regard to information that is public or readily available) to have:

- Joint beneficial ownership of a legal entity or legal arrangement with a person who is a PEP; or
- Sole beneficial ownership of a legal entity or legal arrangement known to exist for the benefit of a person who is a PEP.

PEP status itself does not, of course, mean the individual should be rejected. It may, however, put a customer that is itself a PEP, or where a director or beneficial owner is a PEP, into a higher risk category, especially if domiciled abroad.

Business relationships with immediate family members or close associates of PEPs involve reputational risks similar to those with PEPs themselves. Furthermore, the definition is not intended to cover middle-ranking or more junior individuals in the foregoing categories.

27.2 Procedures to establish if a person is a PEP.

Whilst some individuals will be easily identified as PEPs due to widely available public documents or information, identifying a PEP is not always a straightforward exercise, particularly in the case of family members or close associates. Accordingly, it is first necessary to establish that the person is a PEP.

The Company has established procedures to assess whether a customer or beneficial owner is a PEP, as it has established a relationship with third-party service providers whereby they will perform checks to verify the identity of the customer or beneficial owner and other risk assessments, such as whether the person is a PEP (or lives in a high-risk jurisdiction).

27.3 Risk-based procedure where a customer is a PEP.

Approval from the AML/CTF Compliance Officer is required for accepting a PEP as a customer. The degree of scrutiny will depend on various risk factors, including, but not limited to, geographic risks, i.e., foreign jurisdiction risk as defined under Comoros AML/CTF laws, FATF-recognised lists, or credible international sources.

27.4 Customers' business activities and operations pose a significant risk.

Certain customers may present as high-risk because of their business activities, such as cash businesses, arms dealers, gaming establishments, and customers with financial links to high-risk jurisdictions.

27.5 Level and volume of trading are not logical given the customer's financial profile.

A customer may present with a certain financial profile, e.g., a salary earner. However, the anticipated or actual frequency and volume of trading or investment exceed the expected financial capability of the customer, or the level of investment in the account is significant.

27.6 High Net Worth Customers and Individual Investment Mandates

These are individualised services for high net worth customers, and the provision of these services is tailored to the customers' priorities. A wide range of products and services may be utilised, including:

- High-value transactions;
- Use of sophisticated products;
- Non-standard investment solutions;
- Business conducted across different jurisdictions; and/or
- Overseas companies, trusts, or personal investment vehicles.

27.7 The Customer’s Sources of Funds and Wealth

The Company must establish a customer’s sources of funds and wealth in order to assess the risk of the customer engaging in ML and/or TF. The sources of funds and wealth can be established during the risk assessment process.

27.8 The Nature and Purpose of the Business Relationship with Customers

Due to the nature of its activities, the Company is an issuer of OTC derivative products, and while transacting in the financial markets can result in losses, the risk of customers engaging in ML and/or TF through the Company’s business relationship with its clients is considered low.

27.9 The Control Structure of Non-Individual Customers

Some customers may present complex structures that have no commercial rationale or with numerous layers, resulting in difficulty in identifying the true beneficial owner.

27.10 Types of Designated Services

The risk of the customer engaging in money laundering and/or terrorism financing will differ depending on the nature of the designated service offered. For example, the risk of a person

laundering money by betting in a casino is greater than the risk of a person laundering money by trading financial products.

The Company has formed the view that the designated service it offers is a low ML/TF risk. This is on the basis that the designated service is an activity performed in well-regulated financial markets, i.e. the risk of a person using this type of product and/or service to launder money or finance terrorism is lower than other services such as the gaming industry or dealers in fine arts or commodities (such as gold and diamonds).

27.11 Methods by which we Deliver Designated Services

The way the designated service is delivered (e.g., over the internet as compared to face-to-face delivery) may impact the ability for a Reporting Entity to adequately assess and "know its customer."

The Company acknowledges that in most circumstances it is unlikely that it will physically meet with its customers. This, however, does not mean that the customer is high-risk.

To mitigate and manage the ML/TF risks, a higher risk weighting is attached to the provision of designated services where there is no direct contact with the customer AND where the identification documents provided cannot be readily verified.

27.12 No Face-to-Face Contact with Customer – Provision of Services via the Internet or Phone

A higher risk weighting may be attached to the provision of designated services where there is no direct contact with the customer and where the identification documents provided cannot be readily verified, i.e., where accounts are opened or correspondence is only via the telephone or internet (i.e., non-face-to-face).

Depending upon the ML/TF risk of that customer, this may trigger the requirement for more comprehensive searches and further due diligence to be performed for that particular customer.

In other words, caution is to be exercised, and more comprehensive searches (further due diligence) are required where the identity of the customer cannot be verified with confidence.

27.13 Agents of Customers

Where the customer is introduced by a person acting as the customer's agent, customer identification procedures are to be undertaken in respect of both the agent and the underlying customer, i.e., the Company considers both the investor and the agent as its customer. For example:

- If the agent is regulated and subject to AML/CTF obligations under the laws of the Union of the Comoros or another FATF-equivalent jurisdiction, then it will

have conducted its own collection and verification of information with respect to the customer.

- In this circumstance and in the absence of any other ML/TF risk variable (such as the customer being a PEP), representatives (or agents of the Company or intermediaries) may undertake the minimum KYC procedures relevant to the customer type and risk profile.
- If the agent is located in a foreign jurisdiction, both the intermediary and the customer will also undergo customer identification processes, having regard to their foreign jurisdiction risk as defined under Comoros AML/CTF laws and FATF standards.

28. Foreign Jurisdictions

Certain foreign jurisdictions pose higher ML/TF risks than others due to the activities being conducted in those regions.

The AML/CTF Compliance Officer, under the direction of the Board, will ensure that any government or FATF findings concerning the approach to money laundering and terrorism financing prevention in particular countries or jurisdictions is assessed and appropriate changes to the AML/CTF Program (and all compliance procedures) are made and communicated to all representatives, depending on their level of responsibility.

Reports on FATF mutual evaluations are obtained from www.fatf-gafi.org.

Procedures followed by the Company when determining if a foreign jurisdiction is of high risk include consideration of the following:

- Non-FATF members;
- Appear on the lists of credible sources as having high levels of corruption;
- Banking secrecy havens;
- Do not have a comparable AML/CTF regulatory environment to that of the Union of the Comoros or FATF-equivalent jurisdictions, or are otherwise designated as high-risk by credible international sources;
- Are subject to financial sanctions by the UN or are identified by the UN as providing funding or support for terrorist activities or which have terrorist organizations operating within them;
- Are subject to sanctions by bodies such as the UN, but which may not be universally acknowledged; and
- Are identified by credible sources as providing funding or support for terrorist activities, or that have terrorist organizations operating within them.