GLOBUS TRADING

Anti-Money Laundering Policy and Policy for combatting the financing of Terrorism

January 2025

GLOBUS TRADING

Contents

Introduction ..... **Error! Bookmark not defined.**

1. Introduction 4

1.1. Objective and purpose 4

Globus1.2. Policy Scope 5

1.3. Legal Requirements 6

1.4. Related Documents 6

1.6. Adoption and review of the Policy 7

1.6. Definitions 7

2. Governance and decision making 9

2.1. Governance 9

Management Board 9

Three lines of defense ..... **Error! Bookmark not defined.**

The first line of defence 10

The second line of defense 11

Internal audit, third line of defense ..... **Error! Bookmark not defined.**

2.2. Decision making 11

3. Risk based approach 12

3.1. Introduction 12

3.2. Globus business 12

3.3. Globus risk appetite 12

3.4. Risk classification of clients 13

3.5. Unacceptable risk and exit policy 13

3.6. Unacceptable risk: sanction hit 14

3.7. Periodic risk evaluation and assessment 14

4. Globus' measures against money laundering/terrorism financing and sanctions 15

4.1. Customer Due Diligence (CDD); onboarding and activating 15

4.1.1 Phase 1: CDD processes for all prospect clients: 15

4.1.2. Phase 2: CDD processes for higher-risk clients (EDD) 15

4.2. Continuous PEP and sanction lists check 16
4.2.1 Type of Hit 17
4.2.2. Adverse media review 17
4.2.3 Training and awareness 17
4.2.4. Record keeping and retention 17
4.3. Monitoring of Policy and CDD processes 18

GLOBUS TRADING

1. Introduction

1.1. Objective and purpose

Globus Trading Inc ("Globus") is incorporated in Comoros Union with registration number HT00324021, license number BFX2024059 , and registered address at Bonovo Road, Fomboni Island of Moheli, Comoros Union

The Anti-Money Laundering Policy which is targeted at combating laundering of money obtained through criminal activities is an integral part of Globus Trading's internal procedures. Anti-Money laundering measures are based on generally accepted standards and meet the requirements imposed on financial companies by regulators., specifically Central Bank of Comoros (BCC), Financial Investigation Unit (SFR/FIU), Ministry of Finance are followed by Globus, during the operations of the company.

As a licensed entity, Globus is part of the financial system and acting with integrity is of paramount importance for Globus and a central requirement of applicable legislation. An element of this requirement is that Globus identifies the integrity risks related to Globus' clients and that Globus takes appropriate measures to mitigate these risks.

The objective of this Anti-Money Laundering (**AML**) and Counter-Terrorism Financing (**CTF**) and Sanctions Policy (the "**Policy**") is to lay down Globus' approach, policy and principles on identifying the integrity risks – especially in relation to Money Laundering (**ML**), Terrorism Financing (**TF**) and violations of Sanctions - related to Globus' business activities and the clients of Globus and to take the appropriate measures to mitigate these risks.

ML, TF and violations of Sanctions are hereinafter together referred to as "**ML, TF and Sanctions Crime**"

The purpose of the Policy is twofold:

1. To prevent Globus and its services from being (mis)used for ML, TF and Sanctions Crime and to ensure compliance with applicable legal requirements.
2. To ensure that appropriate action is taken by Globus, to mitigate the risks associated with ML, TF and Sanctions Crime.

To this end, Globus conducts client due diligence (CDD), monitors transactions on ongoing basis and reports executed or anticipated 'unusual transactions' in accordance with AML Regulations (defined below).

This Policy outlines the applicable legal requirements as well as internal measures which are established by Globus, to ensure it complies with these legal requirements.

1.2. Policy Scope

The Policy covers all of Globus' business activities and applies to all natural persons working under responsibility of Globus, such as directors, employees, independent contractors and temporary workers (thus including all activities that Globus outsourced to third-party service providers and/or other entities).

The Policy applies in all jurisdictions where Globus is active at any given moment.

1.3. Legal Requirements

Globus must comply with Comoros laws and regulations relating to ML, TF and Sanctions Crime and, where applicable, additional ML, TF and Sanctions Crime requirements in other jurisdictions in which Globus operates. Based on Globus risk tolerance, Globus may adopt more strict standards.

  - Law No. 08-12/AU (2008) on transparency in public, economic, financial, and social activities
  - National Anti-Corruption Strategy (2012)
  - Establishment of the National Commission for the Prevention and Fight Against Corruption (CNPLC)
- The country has adopted specific anti-money laundering laws, such as:
  - Ordinance No. 03-002/PR (2003) on money laundering and confiscation
  - Law No. 12-008/AU (2012) on AML/CFT, with later amendments

And specifically, for CFD/Forex companies, requirements are laid out in:

  - Law No. 0 20-005/AU of June 23, 2020, on payment services and payment service providers

These laws and regulations will jointly be referred to as "**AML Regulations**"

Furthermore, Globus will make use of related guidelines of the competent regulatory authorities such as the EBA guidelines, Financial Action Task Force (**FATF**) recommendations and other international guidelines, Q&As and good practices on compliance with AML Regulations. Globus uses national and supranational risk assessments to keep this Policy up to date.

1.4. Related Documents

In addition to this Policy, Globus may adopt additional processes and procedures.

The following documentation has been established based on this policy and should be read in conjunction with this Policy:

- Privacy policy
- Vulnerable client policy

1.6. Adoption and review of the Policy

The Management Board of Globus (the **Management Board**) adopted this Policy and has the overall responsibility for compliance and management of risks associated with ML, TF and Sanctions Crime.

The Policy will be reviewed annually and when circumstances so require and may be amended at any time (after consultation with the MLRO) by the Management Board.

1.6. Definitions

Money Laundering	All activities aimed at legitimizing illegally obtained assets to conceal the illegal origin of those assets
Terrorism Financing	The use of capital and assets in order to facilitate, direct or indirect, terrorist activities (
Sanctions	Political instruments used to enforce foreign and security policies of the United Nations, the European Union and other jurisdictions in response to violations of international law or human rights, to encourage policy changes where legal or democratic principles are being violated or in combating terrorism.
Ultimate Beneficial Owner (UBO)	Any natural person(s) who ultimately (directly or indirectly) owns or controls more than 25% of a corporate client and/or the natural person(s) on whose behalf a transaction or activity is being conducted.[1]
Legal Representative (LR)	The natural person duly authorised to legally represent a corporate client vis-à-vis external party.
Politically Exposed Person (PEP)	a natural person who is or who has been entrusted with prominent public functions and includes the following: (a) heads of State, heads of government, ministers and deputy or assistant ministers.

1

	(b) members of parliament or of similar legislative bodies. (c) members of the governing bodies of political parties. (d) members of supreme courts, of constitutional courts or of other high-level judicial bodies, the decisions of which are not subject to further appeal, except in exceptional circumstances. (e) members of courts of auditors or of the boards of central banks. (f) ambassadors, chargés d'affaires and high-ranking officers in the armed forces. (g) members of the administrative, management or supervisory bodies of State-owned enterprises. (h) directors, deputy directors and members of the board or equivalent function of an international organisation. No public function referred to in points (a) to (h) shall be understood as covering middle-ranking or more junior officials. The AML Legislation in Comoros recognizes 3 types of PEP's: Foreign PEP , National (Comoros) PEP and PEP of international organizations .
Family of a PEP	(a) the spouse, or a person considered to be equivalent to a spouse, of a politically exposed person. (b) the children and their spouses, or persons considered to be equivalent to a spouse, of a politically exposed person. (c) the parents of a politically exposed person.
Person closely associated with a PEP	(a) a natural person known to be a joint UBO of a legal entity or legal arrangement with a PEP, or who has other close business relationships with a PEP. (b) a natural person who is the sole UBO of a legal entity or legal arrangement known to have been established for the benefit of a PEP.
business relationship	a business, professional or commercial relationship which relates to the professional activities of Globus and

	which is expected, at the time when the contact is established, to last for a certain duration.
Client	a legal or natural person with whom Globus enters a business relationship or who has a transaction executed. This includes clients and other business relationships.

2. Governance and decision making

2.1. Governance

With this Policy, the Management Board ensures that there is a robust approach within Globus, to prevent and combat ML, TF and Sanctions Crime and to report Suspicious Transactions, as defined in CIBA handbooks ("STR")

Management Board

It is the responsibility of the Management Board to ensure that Globus, complies with the measures set forth in this Policy.

MLRO/

In accordance with AML Legislation Appointment of an AML/CFT officer and SRF (FIU) correspondent (Art.14 of Law 12-008/AU), Globus designates an appointed Money Laundering Reporting Officer ("MLRO"). This person has as a specific area of attention and focuses on compliance with the AML legislation. As described in this policy, the MLRO is

- The main point of contact with the SRF(FIU), Central Bank of Comoros (BCC) in the handling of disclosures.
- Has unrestricted access to the CDD information of the financial institution's customers, including the beneficial owners thereof.
- Has sufficient resources to perform his or her duties.
- Is available on a day-to-day basis.
- Reports directly to, and has regular contact with, the Management Board of Globus and
- Is fully aware of both AML Legislation in Comoros , specifically the Law No. 12-008/AU (2012) on AML/CFT, with later amendments, and his/her personal obligations in lieu of the policies of Globus

The larger set of obligations of the MLRO also entails the covering of the Compliance Operations of Globus. These are:

1. Ensuring continued compliance with the requirements of the AML legislation, specifically Law No. 12-008/AU (2012) on AML/CFT, with later amendments subject to the ongoing oversight of the Board of the financial institution and senior management.
2. Undertaking day-to-day oversight of the program for combatting money laundering and terrorism financing.
3. Regular reporting, including reporting of non-compliance, to the Board and senior management; and
4. Contributing to designing, implementing and maintaining internal compliance manuals, policies, procedures and systems for combatting money laundering and terrorism financing.

The Management Board, where applicable, after having obtained the advice of the MLRO takes the following decisions:

1. The classification and approval of a client as high risk.
2. The decision to accept a PEP as a client,
3. The reporting of an unusual transaction to the FIU and/or equivalent in another jurisdiction.
4. Blocking of a client's account.
5. The decision (a) not to onboard and activate a client or (b) to terminate an existing relationship with a client if the risk is unacceptable.

Defence lines

Globus applies the defence risk management model in its efforts to identify, mitigate and handle ML, TF and Sanctions Crime risks.

The first line of defence

The business teams represent the first line of defence and are responsible for daily risk management. The onboarding team is responsible for :

- Prior to establishing the client relationship: Conduct client due diligence (CCD) measures and the full onboarding of clients,
- During the client relationship: Conduct ongoing monitoring (this includes periodic CDD reassessments and event driven CDD reassessments)
- During the client relationship: Conduct transaction monitoring activities,

- Escalate high risk clients to the CEO,
- Escalate alerts and potential unusual transactions to the CEO.
- The first line can obtain advice from the second line of defence: the MLRO.

Due to the limited size and complexity of its business, Globus has arranged its internal organisation such that the onboarding activities are headed by the MRLO This setup ensures oversight of CDD by an experienced professional. The onboarding team has no commercial targets or other incentives and focuses on CDD only. Globus considers this setup proportionate to its business.

The second line of defence

The MLRO/CO function, as the second line of defence, is responsible for the compliance cycle. This includes:

- Assessing, mitigating (e.g. providing guidance), monitoring and reporting.
- Proposing measures to mitigate integrity risks
- Conduct awareness and training,
- The MLRO also ensures that the required procedures are in place with regard to incident reporting of those risks.
- Monitoring developments and regulations, assess them and propose measures that have an impact on integrity risk.

The MLRO may advise the first line when asked or on its own initiative.

2.2. Decision making

The decisions taken by Globus regarding ML, TF and Sanctions Crime are based on strict rules stemming from AML Regulations, this Policy and Globus business rules (e.g., CDD Procedure, Onboarding Procedure). Globus considers adherence by these rules as crucial for ensuring that Globus business and service is not used for ML, TF and Sanctions Crime. These rules apply for every natural person working under responsibility of Globus.

Nevertheless, there are situations possible where strict adherence by legislation, this Policy and business rules may not result in the desired decision or outcome. Exceptions to the rules are possible but these deviations require written approval by the Management Board and after having received the advice of the MLRO.

All agreed exceptions to the rules, the nature and reasons for the exceptions and the advice of the MLRO are recorded in a register kept by the MLRO.

3. Risk based approach

3.1. Introduction

In executing this Policy and in complying with AML Regulations Globus adopts a risk-based approach. This means that Globus identifies and assesses the ML, TF and Sanctions Crime risks to which Globus is exposed. The exposure to these risks is related to Globus' business; its clients, products and services, distribution channels and countries where Globus is active. Based on this assessment, Globus takes mitigating measures proportionate to the risks and in conformity with Globus risk appetite.

The range, degree, frequency, or intensity of mitigating measures will be more comprehensive in situations assessed as posing a higher risk while these measures will be less comprehensive in situations assessed as posing a low risk. Applying a risk-based approach, thereby, allows Globus to target its resources in the most efficient and effective manner.

3.2. Globus business

Globus is an CFD / Forex broker that offers products to its clients via the website https://globustrading.co

Globus is a premier brokerage platform globally renowned for its dedication to delivering cutting-edge solutions through superior tools and analytics. Our paramount objective is to offer clients the ultimate trading experience, presenting a robust suite of user-friendly tools crafted to accommodate traders of every proficiency level. Globus operates as a fully licensed and regulated brokerage, guaranteeing utmost security and compliance.

3.3. Globus risk appetite

Globus has assumed a low appetite for integrity risks. For Globus this means as follows:

- No willingness for breaching regulations
- No willingness to damage the public trust and confidence in the financial system as a whole.

Globus will take appropriate measures if Globus has a reason to suspect that a (natural or legal) person has or will use Globus services for ML, TF and Sanctions Crime. These steps will include notifying supervisory authorities and/or suspending payments and services to the relevant clients.

3.4. Risk classification of clients

Based on Globus experience and its business as set out above, Globus considers the risk of ML, TF and Sanctions Crime for Globus in general as low/medium/high. Nevertheless, this risk is not fully absent, and Globus has, considering its risk appetite, established four risk categories for its clients. A client is classified as a low-risk client, medium-risk client, high-risk client or an unacceptable client.

The classification of each client in one of these categories is dependent on the outcome of Globus' CDD enquiries and the applicability of various criteria defined in the risk assessment Globus established to determine the risk a client may pose for ML, TF and Sanctions Crime.

The criteria for classifying a client as a high-risk or unacceptable client are updated yearly and when required due to new developments and changed or amended legislation and guidelines by supervisory authorities.

The findings on each client, as well as the risk classification, is documented by Globus in its database. If, for whatever reason, the CEO, after consulting the MLRO, decides in exceptional cases to deviate from the high-risk criteria and bases its decisions on other grounds, these grounds as well as the decision itself are documented properly in the database.

3.5. Unacceptable risk and exit policy

In addition to low, medium and high risk, Globus also acknowledges the category of unacceptable risk. If Globus is of the opinion that a client poses an unacceptable risk for ML, TF and Sanctions Crime, the client will not be onboarded and activated.

If a client is already onboarded and activated but if the periodic or event driven CDD reassessment or the results of the transaction monitoring indicates an unacceptable risk, Globus will terminate the relationship with that client with immediate effect or on the shortest possible notice.

The decision not to activate a client or to terminate an existing relationship is taken by the Management Board upon a proposal from the MLRO. This decision is only taken if there are indicators that result in an unacceptable high risk for ML, TF and Sanctions Crime. For example, if Globus is for whatever reason not able to successfully complete the CDD process , for example, because the required information is not obtained or appears to be incorrect.

Globus documents and registers all decisions not to onboard and activate a client and to terminate an existing client relationship, including the reasons for taking such decisions and the advice of the MLRO.

In case Globus cannot complete its CDD or in case Globus terminates a business relationship and there is an indication of ML/TF, Globus reports this to the Financial Intelligence Unit (**FIU**) in correspondence with its STR reporting procedure.

3.6. Unacceptable risk: sanction hit

Before a client is onboarded and activated and for clients already onboarded and activated, Globus checks the name(s) of client(s), LR(s) and UBO(s) against the names of individuals or entities included in international and national sanctions lists.

If there is a positive match, Globus not only immediately ceases all relationships with and stops making payments to/with that client or individual, but also immediately notifies supervisory authorities, and file a a suspicious transaction report under terms set by decree no . 19-051/MFBSB/CAB of the Minister of Finance, Budget and Sector Banking .

3.7. Periodic risk evaluation and assessment

Over time, the means and methods of ML, TF and Sanctions Crime change, also because of new technologies and new payment methods. Globus needs to ensure that it is aware of these new developments as well as of measures to counter these new potential risks. Globus

Globus not only has a training and awareness program that takes new developments in relation to ML, TF and Sanctions Crime into account, but Globus also periodically reviews its risks in this respect and the measures to mitigate these risks.

If Globus wants to introduce a new service or if it wants to change the existing services significantly, Globus will assess the risks related to ML, TF and Sanctions Crime of this proposed change in business and take appropriate mitigating measures.

In addition, Globus takes proper notice of the periodic national and international (EU) Financial crime risk evaluations and assessments as well as FATF guidelines. The guidance presented by these national and international analyses can result in changes of Globus risk assessment, changes in mitigating measures taken by Globus and/or modifications of Globus training and awareness program.

4. Globus' measures against money laundering/terrorism financing and sanctions

4.1. Customer Due Diligence (CDD); onboarding and activating

Before commencing a business relationship with a client (i.e., before a client will be onboarded and activated), Globus will perform the CDD onboarding activity. If it the client is a corporate entity with its owners/UBOs and legal representative (LRs) – Globus will perform the CDD process on the full entity. Globus in principle only commences a business relationship with a client after Globus has fully and successfully completed this CDD process.

4.1.1 Phase 1: CDD processes for all prospect clients:

1. Globus identifies and verifies the identity of the client, in the case of corporate client, the UBOs of the client and if applicable – the LR(s) of the client.
2. Globus determines the ownership and control structure of all its clients
3. Globus also determines whether the client is acting on its own behalf or for another person/entity. If the latter is the case, then that other person qualifies as Globus client and needs to be identified and his/her identity verified.
4. Globus verifies whether the client, UBO(s) and/or LR(s) are sanctioned parties as per international and national sanction lists.
5. Globus verifies whether the Client, or in case of corporate entity, the UBO(s) and/or LR(s) are PEP(s).
6. Globus determines the purpose and nature of the business relationship with the client and in case of higher-risk clients, investigates the source of wealth and the source of funds of the client.

4.1.2. Phase 2: CDD processes for higher-risk clients (EDD)

If as a result of this CDD process -, one or more criteria for high risk for ML, TF and Sanctions Crime is met, Globus will enquire further in order to obtain more information about the client, in the case of corporate entity, the UBO(s), LR(s) and, the nature and sources of funds of the assets of that client. With this additional information, Management Board can take an informed decision on the onboarding and activation of

the client. For the avoidance of doubt, if a client, or in case of a corporate entity, UBO and/or LR is a sanctioned party, Globus will not accept nor continue any business relationship with such a party. As per decree no · 19-051/MFBSB/CAB of the Minister of Finance, Budget and Sector Banking, a positive sanction hit will also trigger the STR reporting procedure.

The extent and nature of these additional enquiries depend on the obtained outcome of the CDD process thus far but may include an adverse media check of the client, as well as additional documents - whether via public sources - relating to the nature and sources of funds of the client and/or the position of persons connected to the client.

In cases that a client is qualified as higher risk (based on information received by the client or the type of products/services it receives from Globus), enhanced due diligence (**EDD**) is required. The following EDD measures will (at least, if not already) be taken:

- Adverse media check. Globus will carry out adverse media checks. These adverse media checks are effective to get better insight in the reputation and background of the client, On the basis thereof Globus assesses the level of risk of accepting such client or continuing doing business with such clients. This supports Globus in establishing whether clients affect the reputation of Globus or the financial industry in which it operates, nor lead to non-compliance with laws and regulations.
- collect additional information about the client
- collect information about the source of funds/wealth of the client,
- approval of Globus Management Board for establishing the relationship with the client,
- intensified monitoring of the client (this is achieved by annual reassessment of the client, and transaction monitoring activities).

4.2. Continuous PEP and sanction list check

PEP lists and sanction lists are screened daily through a third-party provider. Globus receives PEP lists from an external vendor and downloads the sanction lists from the authorities and screens these against available information regarding clients. The MLRO checks daily whether there are any positive hits. NameScan is used to check our portfolio of clients against sanction and PEP lists.

4.2.1 Type of Hit

For false hits payments are released and for positive hits, the Management Board is informed, and services will not be provided by Globus before investigating to understand the nature of the hit and take the appropriate measure such as filing STR, terminating the account and other connected activities.

4.2.2. Adverse media review

Reassessment will take place in case of adverse media with regard to the client. Globus will periodically perform an adverse media check on (high risk and/or medium) clients. The results will be reviewed by the MLRO and if needed, the risk classification of individual clients will be adjusted accordingly. In case of high risk, the Management Board or one of its members decide thereon

4.2.3 Training and awareness

Globus requires that all individuals active in Globus CDD and Transaction Monitoring processes have experience and possess an adequate and up-to-date awareness and knowledge of the risks of ML, TF and Sanctions Crime and applicable regulations. The MLRO offers training and keeps a training overview up to date. The MLRO also ensures that all employees who are considered part of the MLRO receive external training on the topic at least once every year.

4.2.4. Record keeping and retention

Globus has a robust and effective IT solution to cater for an effective administration and registration in the database with regard to its CDD process and ongoing monitoring of clients

This includes registration of all required information on natural persons and legal entities as well as all related documents in its internal database.

Records are kept in a manner making information and documents available to all individuals within Globus in a secure way that need access to this data for the purpose of their professional obligations (i.e., on a need-to-know basis). This means that Globus staff active in CDD has appropriate access to the client in question (within the database).

All data is kept during the lifetime of the client's relationship with Globus and at least five years after termination of the customer relationship or after the date of the last transaction of a client.

4.2.1 Type of Hit

For false hits payments are released and for positive hits, the Management Board is informed, and services will not be provided by Globus before investigating to understand the nature of the hit and take the appropriate measure such as filing STR, terminating the account and other connected activities.

4.2.2. Adverse media review

Reassessment will take place in case of adverse media with regard to the client. Globus will periodically perform an adverse media check on (high risk and/or medium) clients. The results will be reviewed by the MLRO and if needed, the risk classification of individual clients will be adjusted accordingly. In case of high risk, the Management Board or one of its members decide thereon

4.2.3 Training and awareness

Globus requires that all individuals active in Globus CDD and Transaction Monitoring processes have experience and possess an adequate and up-to-date awareness and knowledge of the risks of ML, TF and Sanctions Crime and applicable regulations. The MLRO offers training and keeps a training overview up to date. The MLRO also ensures that all employees who are considered part of the MLRO receive external training on the topic at least once every year.

4.2.4. Record keeping and retention

Globus has a robust and effective IT solution to cater for an effective administration and registration in the database with regard to its CDD process and ongoing monitoring of clients

This includes registration of all required information on natural persons and legal entities as well as all related documents in its internal database.

Records are kept in a manner making information and documents available to all individuals within Globus in a secure way that need access to this data for the purpose of their professional obligations (i.e., on a need-to-know basis). This means that Globus staff active in CDD has appropriate access to the client in question (within the database).

All data is kept during the lifetime of the client's relationship with Globus and at least five years after termination of the customer relationship or after the date of the last transaction of a client.

Globus database allows it to fully respond to requests from competent authorities (e.g. CIBA, FIU,) without delay, including on whether Globus has or had a business relationship with a client during the past 5 years and questions on the nature of the relationship with a client.

4.3. Monitoring of Policy and CDD processes

Globus periodically and regularly carries out quality checks in order to ascertain whether the measures and processes in relation to the prevention of ML, TF and Sanctions Crime are working properly. The quality checks are carried out monthly by the MLRO and the results are properly documented and are reported including possible recommendations to the Management Board of Globus.

Globus has a written process for carrying out quality checks in order to check whether the onboarding and risk classification of new clients is in conformity with Globus instructions. This process of quality checking is periodically reviewed.

GLOBUS TRADING

Document version control

Document Version	Type of revision	Date of publishing	Signing Off	MLRO	CEO
1.0	Initial drafting	01/10/2024	Board meeting		
1.1	Structural update	20/01/2025	Board meeting		