AML Policy

Last revised: 02/03/2021

This policy applies to all directors, officers and employees, as well as contractors of GGPlatform Limited.

GENERAL DEFINITIONS

For the purposes of this Manual, unless the context shall prescribe otherwise:

"Beneficial Owner" means an individual who ultimately owns or controls more than 25% of a company's shares or voting rights, or who otherwise exercises control over the company or its management.

"Business Relationship" the connections that exist between all entities that engage in commerce.

"User" means someone for whom Company is providing a service or doing some work.

"Company" means GGPlatform Limited (hereinafter "GGPLATFORM"), registered in Saint Lucia, registration number 2021-00017, legal address: Rodney Bayside Building, Rodney Bay, Gros-Islet, Saint Lucia.

"Money laundering" is defined as follows:
Money laundering involves transforming money acquired through crime into money that:

- has the appearance of coming from a legitimate source; and
- makes the criminal origin of the money difficult to trace.

Effective money laundering enables criminals to remove themselves from their criminal activities, making it harder to prosecute them, and confiscate their illegal proceeds.
There are three stages to laundering money:

1) **Placement:** During the first stage of this process the illegal money can enter into the financial system e.g. through deposits in a bank account. Illegal proceeds are easier to detect at the placement stage, when the physical currency enters the financial system.
2) **Layering:** Illicit proceeds trying to be anonymous and be separated from their source by creating some layers of financial transactions.
3) **Integration:** If the previous stage has gone successfully, the derived illegal wealth and income proceeds into the economy and all this money are used as normal business funds.

"Financing Terrorism" means the provision of financial services or accepting funds from customers with the knowledge that they are intended to finance a terrorist organization, preparation or committing of at least one of the acts defined by international law as crimes with a terrorist nature.

"Politically Exposed Persons (PEPs)" means an individual who holds or has ever held one of the following positions in or on behalf of a foreign country:

- a head of state or government;
- a member of the executive council of government or member of a legislature;
- a deputy minister (or equivalent);
- an ambassador or an ambassador's attaché or counselor;
- a president of a state owned company or bank;
- a head of a government agency;

- a judge;
- a leader or president of a political party in a legislature.

A politically exposed foreign person also includes the following family members of the individual described above:

- mother or father;
- child;
- spouse or common law-partner;
- spouse's or common-law partner's mother or father;

brother, sister, half-brother or half-sister (that is, any other child of the individual's mother or father)

Compliance means the company follows legal standards and legal acts adopted in this particular country.

AML/CFT means Anti-Money Laundering and Countering Financing of Terrorism

Due diligence means an investigation, audit, or review performed to confirm the facts of a matter under consideration.

Purpose of the guidance

The purpose of this guidance is to:

• outline the legal and regulatory framework for anti-money laundering/countering terrorist financing requirements and systems across the financial services sector;

• interpret the requirements of the relevant law and regulations, and how they may be implemented in practice;

• indicate good industry practice procedures through a proportionate, risk-based approach; and

• assist firms to design and implement the systems and controls necessary to mitigate the risks of the firm being used in connection with money laundering and the financing of terrorism.

This document sets out:

a) how accounts are monitored for suspicious behavior;
b) escalation processes for suspicious transactions within в GGPlatform Limited; and
c) how suspicious transactions will be reported to appropriate authorities.

Our compliance regime:

GGPlatform Limited has developed and formally approved a compliance regime to counter money laundering, terrorist financing or other criminal activities, including the appointment of a compliance officer, the preparation of appropriate policies and procedures, periodic analysis of their effectiveness and regular training of staff in the field of countering money laundering and the financing of terrorism.

GGPlatform Limited is committed to regularly update its electronic system for inspection of suspicious transactions and for verification of User identification records, in accordance with any new regulations as they are promulgated, as well as providing training for its employees on enhancements to anti-money laundering procedures that may be required by new regulations.

Scope of policy:

This policy applies to all GGPlatform Limited officers, employees, appointed producers and products and services offered by GGPlatform Limited.

All business units and locations within GGPlatform Limited will cooperate to create a cohesive effort in the fight against money laundering. Each business unit and location has implemented risk-based procedures reasonably expected to prevent, detect and cause the reporting of transactions required under the International Anti Money Laundering law.

All efforts exerted will be documented and retained in accordance with the Anti-Money laundering law. GGPlatform Limited guarantees full assistance to the authorities of different countries in the fight against money laundering and the financing of terrorism.

POLICY

It is the policy of GGPlatform Limited to prohibit and actively pursue the prevention of money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities.

GGPlatform Limited is committed to comply with AML/CFT in accordance with the best standards of international law, and it is expected that officials and employees will adhere to these standards in preventing the use of its products and services for money laundering purposes.

CUSTOMER IDENTIFICATION PROGRAM

GGPlatform Limited notifies customers about requested information to verify their identity, as required by the best standards of international law.

CUSTOMERS WHO REFUSE TO PROVIDE INFORMATION

If a customer either refuses to provide the information described above when requested, or appears to have intentionally provided misleading information, GGPlatform Limited will decline the application and notify authorities, if necessary.

1. Introduction

GGPlatform Limited has developed and formally approved an AML/CFT program to comply with the best practices of international law. The AML/CFT program must be supported by adequate and effective policies, procedures and controls to manage and mitigate money laundering and terrorist financing risks in our business operations.

All Directors, senior level management, staff employees, introducing agents and affiliated companies must fully understand the procedures set out herein and comply with the Company's policies and procedures with regards to Customer Due Diligence checks.

2. Policy Governance and Administration

The AML/CFT Compliance Officer is the administrator of this policy and is responsible for reviewing the policy at least annually. Furthermore, the AML/CFT Compliance Officer is responsible for initiating Suspicious Activity Reports or other required reporting to the appropriate law enforcement or regulatory agencies

3. Customer Due Diligence

To comply with AML/CFT best practices requirements, GGPlatform Limited must conduct a customer due diligence in order to determine the true identity of each User as well as to determine that customer behavior is in line with the customer profile. The customer profile shall be established when a customer due diligence is conducted at the outset of the business relationship with the customer. The level of customer risk is assessed in line with the customer profile.

3.1 Know Your User and Due Diligence for Individual Users

During the account opening process, GGPlatform Limited will require each User to submit specific personal information in order to fully identify the true identity of the User.

The User must provide the following information:

1. Full Name
2. Date of Birth
3. Place of Birth
4. Residential Address
5. Gender
6. Telephone Number

In addition, the User must provide in a good quality a copy of one of the following documents:
1. A valid passport with all necessary information.
2. Valid driver's license.
3. Valid Government Issued Identification Card

Note: The company reserves the right to request a photo of the owner of the document along with the document for identification.

The User is also required to provide in a good quality a copy of one of the following documents:
1. Utility bill
2. Bank statement

Note: The document must be valid, filed no later than 3 months from the date of its issue.

All documents uploaded by the User for the above purposes must be clear, in good quality and with proper format (pdf, jpg, tif). The company must have sufficient reason to recognize the identity of any of the downloaded documents.

4. Ongoing Account Monitoring in the personal account

GGPlatform Limited through its Compliance officer must undertake regular personal account monitoring to ensure that the business relationship and transactions are consistent with GGPlatform Limited knowledge about the customer, the customer's business and risk profile. In the case if there is a suspicion of money laundering, terrorist financing or other criminal activities, the compliance officer has the right to contact to the appropriate regulatory authorities.

Personal profile should be subject to more thorough verification in the case:

1. Any activity carried out on the personal profile that casts doubt over the true identity of a User;

2. Transfer of funds from countries that are known to be associated with drug trafficking or terrorism;

3. The unwillingness of the User to provide the requested documentation;

4. There are reasonable suspicions that the Personal Account carries out activities that, by their nature, may be related to money laundering or the financing of terrorism.

5. How do we monitor transactions?

Account Monitoring can be undertaken in several ways:

1. Front line staff vigilance and awareness
2. External Alerts.

Front Line Staff

The staff monitors transactions made by customers, identifies suspicious transactions based on their knowledge and experience. The staff passes proper, qualified training and warns of any suspicious actions of customers, in particular:

- Unusually large transactions or patterns of transactions
- Customers acting in a suspicious manner
- Transactions appear to be out of line with knowledge of the customer

Employees undergo regular AML/CFT training. Additional instructions and reference materials will be provided as needed.

External Alerts

Compliance Officer and company management can receive information from external sources:

- Notifications from the authority
- Media articles
- AML/CFT forums

The reaction to notifications from these sources of information may be to inform employees of suspicious information or to amend the relevant company policies.

6. Risk assessment

Due diligence includes checking the User for a number of risks:

a. Criminal risk;
b. Reputation risk;
c. Legal risk;
d. Credit risk;
e. Fiduciary risk;
f. Regulatory risk; and
g. Operational risk.

A relationship with a User can be exposed to any one or more of the above risks. There are several factors, which can expose us to such risks such as:

a. Identity and occupation of User;

b. Commercial purpose of the relationship;
c. Location of the User’s residence and his business interests;
d. Value and nature of the assets involved;
e. Source of funds

All the above factors need to be properly considered so that risks are limited. Users should be classified as high, medium or low risk.
In accordance with international requirements, the company applies risk assessment practices to counter money laundering and terrorist financing. By adopting a risk assessment practice, the Company reserves the right to suspend any User's operation, the movement of funds on the account, the activity of the user's personal account, which may be considered illegal or, in the opinion of employees, may be related to money laundering or terrorist financing for up to 6 months.

7. Record Keeping

Keeping records is important for monitoring and is useful in case of investigations. All records must be kept for at least 7 years.
Transaction Records by keeping supporting documents may include the following:
a. source of funds including full remitter details
b. volume of funds
c. destination of funds
f. counterparty details
i. date of transactions

In addition, Identity records will be required to keep copies of all verification documents.

8. Determining of information that can be transferred to authorities

The company, in cases where there is an attempt to make transactions that are suspected of money laundering or terrorist financing, informs the relevant authorities.

9. Policy Review

The policy must be approved annually by the owner of the policy.
Prepared, read and confirmed.