



AML & KYC POLICY

October 2023

ANTI-MONEY LAUNDERING AND KYC POLICIES

INTRODUCTION

ONEBID ASSET LLC is a legal entity registered under the Limited Liability Companies Act, Chapter 151 of the Revised Laws of Saint Vincent and the Grenadines, 2009, with the following registration: Company Number 2432 LLC 2022.

Pursuant to the provisions of the Financial Services Authority of Saint Vincent and the Grenadines, the purpose of this policy is to set out the internal practices, policies, procedures and controls of ONEBID ASSET LLC (hereinafter referred to as "ONEBID ASSET", "the Company", "we", "our" or "us") regarding the prevention of money laundering (AML) and counter- financing of terrorism (CFT), as well as the Know Your Customer (KYC) policy.

GENERAL DEFINITION

Money laundering is the process of converting money or other material values obtained from illegal activities (terrorism, drug dealing, illegal arms trade, corruption, human trafficking, etc.) into money or investments that appear to be legitimate. Such activities are used to make it impossible to trace the illegal origin of money and other material values.

Money laundering also includes:

- conversion or transfer of property, especially money, if it is known that such property is obtained as a result of criminal activity or participation in such activity for the purpose of concealing or disguising the illegal origin of the property or assisting any person involved in the commission of such activity in order to avoid the legal consequences of the actions of that person or company;
- concealing or disguising the true nature, source, location, transfer of property rights or ownership of property, knowing that such property is obtained as a result of criminal activity or participation in such activity;
- acquisition, possession or use of property, if at the time of receipt, it is known that such property was obtained as a result of criminal activity or assistance in such activity;
- participating in, associating to commit, attempting to commit and aiding, instigating, assisting and advising in the commission of any of the acts mentioned in the paragraphs above.

Money laundering is considered such even if the activity as a result of which the laundered property was obtained was carried out on the territory of any state.

POLICY STATEMENT AND PRINCIPLES

The Company adopted the program taking into account:

- Saint Vincent and the Grenadines Anti-Money Laundering and Terrorist Financing laws and regulations;
- Recommendations of the FATF and Caribbean FATF.

The Company's anti-money laundering policy procedures include:

- ascertaining the source of the client's assets and income to ensure that they are consistent with his financial situation;
- understanding the client's likely trading patterns to identify inconsistencies;

- training of the staff responsible for approving new accounts, identification of additional accounts that may require enhanced customer identity verification.

This policy applies to all officers, employees, appointed producers, and the Company's products and services.

All business units and divisions of the Company will collaborate to create a cohesive effort in the fight against money laundering. Each business unit and division has implemented risk-based procedures that can be reasonably expected to prevent, detect and report transactions required by international anti-money laundering laws.

The Company will also appoint an AML/CFT compliance officer to monitor compliance with AML/CFT laws and regulations, as well as the Company's internal policies and procedures, and an AML/CFT reporting officer, as well as the relevant personnel subordinate to them, specially trained in accordance with legal requirements, responsible for identifying and reporting unusual transactions.

All efforts made will be documented and maintained in accordance with anti-money laundering legislation. The AML/CFT reporting officer provides reports to the Financial Intelligence Unit and acts as a liaison with service provider oversight authorities.

MANAGEMENT OF RISKS

ONEBID ASSET LLC has established policies, procedures and controls to detect and prevent money laundering, terrorist financing and other illegal activities. Risk management allows a Company to determine its initial approach to developing appropriate customer due diligence procedures for different types of customers.

A risk-based approach to client due diligence also requires conducting a client-specific risk assessment based on that client's individual circumstances. This will determine the amount of identifying and other customer information that will be requested, how it will be verified, and the extent to which the resulting relationships will be monitored.

Accordingly, before accepting a potential client, the Company applies KYC and due diligence to evaluate its risk factors, such as position, associated accounts, business activity and other indicators.

CUSTOMER IDENTIFICATION AND DUE DILIGENCE

The purpose of Customer Due Diligence (CDD) measures is to identify the customer and confirm his identity using reliable, independent source documents, data or information.

The Company recognizes the following documents as identification documents (the list is not exhaustive):

- valid passport;
- valid identification card issued by the national government; and
- valid driver's license.

For identification purposes, the Company requests the following information:

- full name;
- gender of the person;
- the primary address of residence of an individual;
- date of birth of an individual.

The Company also has the right, depending on the level of risk assessed by the Company in accordance with the applicable rules, to request from the client the following additional identification information:

- place of birth of the person;
- citizenship of the person;
- an official government-issued identification number or other government identifier.

When verifying a customer's identity, designated compliance officers will verify photo identification.

Legal entities must provide copies of their company registration, memorandum and/or articles of association, certificates confirming the legal powers of shareholders and directors, documents indicating the address of the registered office, as well as copies of passports of shareholders and directors.

The Company documents its inspection, including all identifying information provided by the customer, the methods used and the results of the inspection, including, but not limited to, the signature of the appointed producer on the appropriate photo ID.

If the customer either refuses to provide the information described above when requested, or appears to have intentionally provided misleading information, the designated agent must notify the Chief Compliance Manager and the Company will then reject the application.

Taking into account the risk assessment and in accordance with applicable rules, the Company has the right to conduct enhanced customer due diligence (ECDD).

These measures will almost certainly include obtaining additional identification and relationship information, including information about the source of funds, as well as a possible request for the following documents:

- a recent bank statement or utility bill;
- correspondence from a central or local government department;
- a letter of recommendation confirming the residential address from the regulated person or a foreign regulated person.

The Company will not provide services to a client if the funds in question are known or reasonably expected to be derived from corruption or misuse of public assets, without prejudice to any obligations of the Company under criminal law or other laws or regulations, or where the purpose of due diligence was not achieved.

PREVENTING FINANCING, TRANSFER AND WITHDRAWAL OF FUNDS BY THIRD PARTIES

The Company strictly does not allow financing by third parties. Any funds deposited into the account must come from the same account holder.

The Company strictly does not allow the transfer of trading funds between different trading accounts belonging to different account holders. This is done to prevent the possibility of money laundering.

The Company strictly enforces the policy that withdrawals should only be made through the same bank account, credit/debit card or digital wallets that the customer used to deposit funds.

MONITORING AND REPORTING SUSPICIOUS ACTIVITY

The main purpose of ongoing monitoring is to identify high-risk activities and business relationships so that money laundering and terrorist financing can be detected and, if possible, prevented.

The Company collects and verifies customer identification data and records and tracks detailed reports of all customer transactions. Particular attention is paid to complex or unusual transaction patterns that have no apparent economic or apparent legal purpose; and any other activity that the service provider considers to be particularly likely by its nature to pose a risk of money laundering or terrorist financing.

The Company does not accept cash deposits or pay out cash under any circumstances.

In addition, any bank deposit of \$10,000 or more may, at the Company's discretion, be subject to approval prior to acceptance of funds. The client may be required to complete an enhanced due diligence form requesting information regarding the source of funds. If approval is not received, funds may be rejected and returned at the customer's expense.

The Company reserves the right to refuse to process a transaction at any stage if it believes that the transaction is in any way related to money laundering or criminal activity. In accordance with international law, the Company is not obliged to inform the client that it has been reported to the appropriate governing authorities in connection with suspicious activity of the client.

PEP POLICY

Politically exposed person (PEP) is an individual who plays a prominent public role within a country or internationally.

The Company establishes, maintains and implements appropriate risk management systems to determine whether a customer, third party or beneficial owner is a foreign politically exposed person, and these risk management systems must take into account that a person may become a foreign politically exposed person once a business relationship is established.

It should be noted that this definition includes not only a person performing an important function in government, but also a person performing an important function in an international organization, as well as the immediate family members and close associates of these people.

While we welcome clients from all over the world, government restrictions along with our Company policy also prohibit the Company from opening accounts to citizens of the following countries with limited capacity and/or OFAC sanctions, as well as from high-risk and non-cooperative jurisdictions: Albania, Burkina Faso, Barbados, Botswana, Congo, Cuba, Ghana, Iran, Jamaica, Japan, Cambodia, North Korea, Cayman Islands, Libya, Morocco, Myanmar (Burma), Mauritius, Nicaragua, Panama, Pakistan, Singapore, Sudan, Senegal, Somalia, Syria, Uganda, US Minor Outlying Islands, USA, Virgin Islands (US), Yemen, Zimbabwe.

TRAINING

Company employees will perform manual controls during risk-based approval, for which they undergo special training. Its use reflects a training and awareness program:

- mandatory AML training program in accordance with the latest changes in legislation for all employees related to finance;
- Anti-money laundering training sessions for all new employees.

The content of this training program is established in accordance with the type of activity and positions held by employees.

DATA SECURITY



All data provided by any user/customer will be kept securely and will not be sold or transferred to third parties unless otherwise stated in the Privacy Policy/Customer Agreement. Data may only be transferred to the state anti-money laundering authority in cases provided for by law or for the purpose of preventing money laundering.

The Company will comply with all recommendations and regulations of the Data Protection Directive.