Anti-Money Laundering/Know Your Customer (AML/KYC) Disclosure

By agreeing to the General Terms and Conditions and Brit.Gold Contractual Documentation located at {_}, Members also acknowledge that the Company has implemented the AML/KYC program as described in this disclosure. All capitalized terms not defined herein shall have the meaning ascribed to them in the General Terms and Conditions and Brit.Gold Contractual Documentation, as applicable.

The Company protects itself from involvement in money laundering or suspicious activity by the following:

- A system of internal controls designed to assure ongoing AML compliance;
- Independent testing of AML compliance through an annual, independent AML audit;
- Designation of a Compliance Officer for managing AML Compliance; and
- AML training for all employees.

INTERNAL CONTROLS

The Company has established a set of AML/KYC policies and procedures which are approved by the Company's Board. The approved policies will be provided to all employees. All policies and procedures will be reviewed and updated or revised as needed, but no less often than annually.

The Company has developed and implemented internal controls for the purpose of ensuring that all of its operations comply with AML requirements and that all required reports are made on a timely basis.

INDEPENDENT TESTING

The Company's AML program will be subject to independent testing through an annual, independent AML audit. The audit will be conducted by an independent third party with working knowledge of AML requirements, or by Company personnel with working knowledge of AML requirements, none of whom work for or with the Compliance Officer. The Compliance Officer will develop corrective action plans for all issues that are raised in the audit, supervise the remediation performed, and report all updates to the corrective action plans to the Company's senior management.

COMPLIANCE OFFICER

The Company has appointed a Compliance Officer to be responsible for the management, coordination and monitoring of compliance with this policy and all applicable AML laws and regulations. The Compliance Officer will have working knowledge of all AML laws and be qualified by knowledge, experience and training. The Compliance Officer will be responsible for filing (if applicable) and keeping a record of suspicious transaction reports ("STR") and suspicious activity reports ("SAR"). The Compliance Officer will oversee all corrective action of any audit findings or other AML-related issues from the annual, independent AML audit. The Compliance Officer will be responsible for all record keeping requirements and provide reports on the effectiveness of the AML program to the Company's Board.

TRAINING

All of the officers and employees of the Company are required to receive AML training at least annually. The Company will track the training progress of all employees and maintain documentation of each employee, the date of the AML training as well as a description of such training. New employees will receive appropriate AML training within 30 days of their hire date. Training for all employees will include not only the legal elements of AML laws and regulations but will also cover job specific applications of these laws. Ongoing training will be provided and updated regularly to reflect current developments and changes to laws and regulations.

CUSTOMER IDENTIFICATION PROGRAM

Company has developed and implemented a Customer Identification Program ("CIP") that establishes procedures for verifying the identity of each customer that opens a new account on the Company's platform. It is the Company's policy to ensure that it has reasonably identified each customer who uses the Company's platform.

ACCOUNT OPENING PROCEDURES

Additionally, the Company will, as part of its account opening process: (i) cross-check the names of users against compliance databases such as the OFAC Specially Designated Nationals list and other governmental watch lists; (ii) require users to verify and validate their identity and identification documents presented at onboarding; and (iii) not permit any activity on platform with incomplete account opening information.

IDENTITY VERIFICATION

Individual

- Individual name
- Date of birth
- Residential address
- Identification number (e.g., National Insurance Number, State Id, Social security number)
- Acceptable and valid government-issued identification document (e.g., drivers license, passport, national identification card)

Institutions

- Institution name
- The address of the institution's principal place of business and, if different, the institution's mailing/registered address
- Identification number of the institution (e.g., employer identification number)
- Name of institution's representative/user for the account
- For institutions, the Company will collect the identifying information with respect to each beneficial owner and will use risk-based procedures to verify the identity of such beneficial owners, including:
    - Acceptable and valid government-issued identification document (e.g., drivers license, passport, national identification card) for each beneficial owner; and
    - Proof of residency (e.g., utility bills, government issued correspondence, documentation issued by recognized financial institutions).
- Customer due diligence procedures will include additional information regarding the institution including but not limited to the following:

- A description of the institution's business, including products and services, main customer types, and geographies served;
- Purpose of account; and
- Source of funds.

SUSPICIOUS TRANSACTION AND ACTIVITY REPORTING

The Company maintains a transaction monitoring program reasonably designed for the purpose of monitoring transactions for potential AML violations and suspicious activity reporting. Transactions that are unusual will be carefully reviewed to determine if it appears to be involved with money laundering, tax evasion, terrorist financing, or other illegal or criminal activity.

Upon identification of potential suspicious transactions or activity, the Compliance Officer will then consult with the Company's Chief Compliance Officer to determine whether to perform a filing for suspicious activity. The Compliance Officer will document any suspicious activity, the determinations made with regard to the activity and the determination as to whether a report of suspicious activity is required pursuant to applicable law or regulation. A filing and any information that would reveal the existence of a filing, are confidential.