Aktagold

Know Your Client (KYC), Anti-Money Laundering (AML), and Countering the Financing of Terrorism (CFT) Policy

UPDATED AS OF MAY 15, 2023

1. Aktagold Policy Statement

It is the policy of Aktagold Inc. ("Aktagold") to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the financing of terrorist or criminal activities. We will comply with all applicable requirements and regulations. Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the proceeds appear to have derived from legitimate origins or constitute legitimate assets. Generally, money laundering occurs in three stages. Cash first enters the financial system at the "placement" stage, where the cash generated from criminal activities is converted into monetary instruments, such as money orders or traveler's checks, or deposited into accounts at financial institutions. At the "layering" stage, the funds are transferred or moved into other accounts or other financial institutions to further separate the money from its criminal origin. At the "integration" stage, the funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses. Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal either the origin of the funds or their intended use, which could be for criminal purposes. Legitimate sources of funds are a key difference between terrorist financiers and traditional criminal organizations. In addition to charitable donations, legitimate sources include foreign government sponsors, business ownership and personal employment. Although the motivation differs between traditional money launderers and terrorist financiers, the actual methods used to fund terrorist operations can be the same as or similar to methods used by other criminals to launder funds. Funding for terrorist attacks does not always require large sums of money and the associated transactions may not be complex.

Our Anti-Money Laundering ("AML") and Countering the Financing of Terrorism ("CFT") policies, procedures and internal controls are designed to ensure compliance with all applicable regulations and will be reviewed and updated on a regular basis to ensure appropriate policies, procedures and internal controls are in place to account for both changes in regulations and changes in our business. U.S. regulations state that i) we may seek the services of a third party to apply measures of due diligence; ii) regardless of reliance on a third party, we remain liable for maintaining all such compliance and fulfilling AML and KYC obligations. Regulations also require us to collect all such data (Diligence Information) from the third party, without undue delay. The U.S. AML/CFT legislative framework is set out in the U.S. Bank Secrecy Act (31 U.S.C. 5311 *et seq.*), and the Code of Federal Regulations (C.F.R. Title 31, Subtitle B, Chapter X, Part 1027 "*Rules for Dealers in Precious Metals, Precious Stones or Jewels"*). It obliges organizations to put in place an effective risk-based AML/CFT framework which includes the application of a risk-based approach, Customer Due Diligence ("CDD") measures, reporting of suspicious

transactions, policies and procedures, record keeping and training. A dealer shall make its anti-money laundering program available to the Department of Treasury through FinCEN or its designee upon request.

2. AML/CFT Compliance Person Designation and Duties

Aktagold has a designated Chief Compliance Officer ("CCO"). The CCO has full responsibility for the Aktagold AML/CFT program. The duties of the CCO will include monitoring Aktagold compliance with AML/CFT obligations, overseeing communication and training for employees and overseeing Aktagold software modifications to ensure they comply with AML/CFT obligations. The CCO will also ensure that Aktagold keeps and maintains all of the required AML/CFT records and will ensure that any Suspicious Activity Reports ("SAR") generated by Aktagold software are filed with the U.S. Financial Crimes Enforcement Network ("FinCEN") when appropriate. The CCO is vested with full responsibility and authority to enforce Aktagold AML/CFT program. Aktagold will provide the company administrators, company secretary and associated financial institutions with contact information for the CCO, including: (1) name; (2) title; (3) mailing address; (4) email address; and (5) telephone number. Aktagold will promptly notify all parties of any change in this information and will review, and if necessary update, this information within 30 business days after the end of each calendar year. The annual review of this information will be conducted by the CCO and will be completed with all necessary updates being provided no later than 30 business days following the end of each calendar year. In addition, if there is any change to the information, the CCO will update the information promptly, but in any event not later than 30 days following the change.

3. Giving AML/CFT information to the U.S. government and authorities if requested

We will respond to a request ("Request") concerning accounts and transactions by immediately searching our records to determine whether we maintain or have maintained any account for, or have engaged in any transaction with, each individual, entity or organization named in the Request. We will designate one or more persons to be the point of contact ("POC") for Requests and will promptly update the POC information following any change in such information. (See Section 2 above regarding updating of contact information for the CCO.) Unless otherwise stated in the Request, we are required to search our files for each individual, entity or organization named in the Request. If we find a match, the CCO will consider any appropriate action. If the search parameters differ from searching through our entire database, for example, if limits to a geographic location apply, the CCO will structure our search accordingly. If the CCO searches our records and does not find a matching account or transaction, then the CCO will communicate that in the Request. We will maintain a register of Money Laundering and Financing of Terrorism Enquiries together with documentation that we have performed the required search by saving the logs, which will at all times be available on request.

4. Levels of Customer Due Diligence ("CDD")

4.1. People who have opened an account need to provide their full contact details (full name, address, email, and telephone number), prior to being allowed to deposit, trade and withdraw

currencies. This is known as Level 1 clearance, which allows deposits and withdrawals of USD 100 a day and USD 1,000 a month.

4.2. Level 2 clearance allows above USD 1,000 a day in deposits and withdrawals and USD 10,000 a month and for this a scanned copy of photographic ID and proof of address as explained in clause 5 is required.

5. Customer Due Diligence ("CDD") and Know Your Client Identification Program ("KYC")

We will collect sufficient information from each customer who has opened an account to enable the customer to be identified; utilize risk-based measures to verify the identity of each customer who has opened an account; record CDD information and the verification methods and results; provide the required adequate CDD notice to customers that we will seek identification information to verify their identities; and compare customer identification information with government-provided lists of suspected terrorists, once such lists have been issued by the government.

5.1 Required Customer Information

After opening an account, Aktagold will collect the following information for all accounts, if applicable, for any person, entity or organization that is opening a new account and whose name is on the account prior to activating the account for deposits and withdrawals of FIAT currencies (deposits, trading and withdrawing digital currencies does not require CDD verification):

- Full Name;
- Date and place of birth (for an individual);
- Nationality;
- Gender;
- Email;
- Phone number;
- Proof of a residential address (for an individual), or a principal place of business, local office, or other physical location (for a person other than an individual); and proof of identification with a photograph.

5.2 Customers Who Refuse to Provide Information

If a potential or existing customer either refuses to provide the information described above when requested, or appears to have intentionally provided misleading information, Aktagold will deactivate the account and, after considering the risks involved, consider closing any existing account. In either case, our CCO will be notified so that we can determine whether we should report the situation to the authorities.

5.3 Verifying Information

Based on the risk, and to the extent reasonable and practicable, we will ensure that we have a reasonable belief that we know the true identity of our customers by using risk-based procedures, and third-party KYC/AML providers, to verify and document the accuracy of the information we get about our customers, but in any case complying with

the statutory requirements. The CCO will analyse the information we obtain to determine whether the information is sufficient to form a reasonable belief that we know the true identity of the customer (e.g., whether the information is logical or contains inconsistencies). We will verify customer identity through documentary means, non-documentary means or both. We will use documents to verify customer identity when appropriate documents are available. In light of the increased instances of identity fraud, we will supplement the use of documentary evidence by using the non-documentary means described below whenever necessary. We may also use non-documentary means, if we are still uncertain about whether we know the true identity of the customer. In verifying the information, we will consider whether the identifying information that we receive, such as the customer's name, street address, postcode, email, telephone number, date of birth and photographic ID, allow us to determine that we have a reasonable belief that we know the true identity of the customer (e.g., whether the information is logical or contains inconsistencies).

Appropriate documents for verifying the identity of customers include the following:

5.4 For an Individual

- Proof of identity (passport copy or provisional or full driving license or Government issued National Identity Card (picture page is sufficient))
- Proof of residential address (utility bill* less than 3 months old or bank statement) *Electricity, gas, water, phone bill (not mobile phone)

5.5 For a Corporation

- Certificate of Incorporation.
- Memorandum and articles of Association.
- Identify the Beneficial Owner.
- For at least 2 directors of a Corporation - Proof of identity and proof of residential address.

The certifier must sign and date the copy document (printing his/her name clearly in capitals underneath) and clearly indicate his/her position or capacity on it and provide his contact details. The certifier must state that it is a true copy of the original. Any non-English documentation requires translation and certification as above. We are not required to take steps to determine whether the document that the customer has provided to us for identity verification has been validly issued and that we may rely on a government-issued identification as verification of a customer's identity. If, however, we note that the document shows some obvious form of fraud, we must consider that factor in determining whether we can form a reasonable belief that we know the customer's true identity.

We will use the following non-documentary methods of verifying identity: i) Confirming validity of email, ii) Confirming validity of telephone number. We will verify the information within a reasonable time after the account is opened. Depending on the nature of the account and requested transactions, we may refuse to complete a transaction before we have verified the information, or in some instances when we need more time, we may, pending verification, restrict the types of transactions or the monetary amount (Dollar, Euro, Swiss Franc) of transactions. If we find suspicious information that indicates possible money laundering, terrorist financing activity, or other suspicious activity, we will,

after internal consultation with CCO, report the activity to the FinCEN in accordance with applicable laws and regulations. We recognize that the risk that we may not know the customer's true identity may be heightened for certain types of accounts, such as an account opened in the name of a corporation, partnership or trust that is created or conducts substantial business in a jurisdiction that has been designated as a primary money laundering jurisdiction, a terrorist concern, or has been designated as a non-cooperative country or territory. We will identify customers that pose a heightened risk of not being properly identified. We will also take the following additional measures that may be used to obtain information about the identity of the individuals associated with the customer when standard documentary methods prove to be insufficient: 1. Obtain verification of beneficial owners of corporations 2. Obtain additional references from financial institutions

5.6 Lack of Verification

When we cannot form a reasonable belief that we know the true identity of a customer, we will do the following: (1) deactivate the account or keep it in deactivated status; (2) close an account after attempts to verify customer's identity fail; and (3) determine whether it is necessary to inform the FinCEN in accordance with applicable laws and regulations.

5.7 Recordkeeping

We will keep logs of our verification, including all identifying information provided by a customer, the methods used and results of verification, and the resolution of any discrepancies identified in the verification process. We will keep records containing a description of any document that we relied on to verify a customer's identity, noting the type of document, any identification number contained in the document, the place of issuance, and if any, the date of issuance and expiration date. With respect to non-documentary verification, we will retain logs that describe the methods and the results of any measures we took to verify the identity of a customer. We will also keep records containing a description of the resolution of each substantive discrepancy discovered when verifying the identifying information obtained. We will retain records of all identification information for five (5) years after the account has been closed; we will retain records made about verification of the customer's identity for five (5) years after the record is made.

5.8 Comparison with Government-Provided Lists of Terrorists

At such time as we receive notice that the authorities have issued a list of known or suspected terrorists and identified the list as a list for CDD purposes, we will, within a reasonable period of time after an account is opened (or earlier, if required by another law or regulation or directive issued in connection with an applicable list) determine, directly or by engaging the services of a third-party KYC provider, whether a customer appears on any such list of known or suspected terrorists or terrorist organizations issued by any government agency and designated as such by the authorities in consultation with the functional regulators. We will follow all directives issued in connection with such lists.

5.9 Notice to Customers

We will provide notice to customers that Aktagold is requesting information from them to verify their identities, as required by law. We will use the following method to provide notice to customers: Inform them by email and through Aktagold online platform when the customer wants to activate their account for depositing and withdrawing FIAT currencies, by using the text shown on section 5.10 below:

5.10 Important Information About Procedures for Activating a New Account

- *"To help the government fight the funding of terrorism and money laundering activities, Aktagold is required to obtain, verify, and record information that identifies each person who opens an account and wishes to deposit and withdraw FIAT currencies."*
- *"What this means for you: When you would like to deposit and withdraw FIAT currencies, we will ask for your name, address, date of birth and other information that will allow us to identify you. We may also ask to see photographic proof of your identification and proof of address."*

6. General Customer Due Diligence

It is important to our AML and KYC reporting program that we obtain sufficient information about each customer to allow us to evaluate the risk presented by that customer and to detect and report suspicious activity. When we open an account for a customer, the due diligence we perform may need to be enhanced. For each account meeting the following criteria and which could be deemed to be higher risk: i) Corporations in off shore jurisdictions; ii) Individuals from high risk countries; and iii) CDD documentation of questionable origin; we will take steps to obtain sufficient customer information to comply with our enhanced due diligence requirements. Such information may include: i) Identification of beneficial owners of corporations, ii) Reference from a financial institution, iii) Proof of source of funds.

7. Customer Due Diligence and Enhanced Due Diligence Requirements for Politically Exposed Persons ("PEP")

In the absence of explicit regulations, Aktagold utilizes the Enhanced Due Diligence measures for PEP and high-risk clients. For these cases, Aktagold screens, directly or through a third-party KYC provider, an individual's selected ID attributes of Name and DOB against watchlists of global regulatory authorities, foreign and domestic databases, compromised PEPs and sanctioned individuals.

8. Monitoring Accounts for Suspicious Activity

We will monitor account activity for unusual size, volume, pattern or type of transactions, taking into account risk factors and red flags that are appropriate to our business. (Red flags are identified in Section 8.b. below.) The CCO or his or her designee will be responsible for this monitoring, will review any activity that our monitoring system detects, will determine whether any additional steps are required, will document when and how this monitoring is carried out, and will report suspicious activities to the appropriate authorities. The CCO or his or her designee

will conduct an appropriate investigation and review relevant information from internal or third-party sources before the authorities are notified.

a) Emergency Notification to Law Enforcement by Telephone In situations involving violations that require immediate attention, such as terrorist financing or ongoing money laundering schemes, we will immediately call an appropriate law enforcement authority.

b) Red Flags that signal possible money laundering or terrorist financing include, but are not limited to: Customers – Insufficient or Suspicious Information – Provides unusual or suspicious identification documents that cannot be readily verified. – Reluctant to provide complete information about nature and purpose of business, prior banking relationships, anticipated account activity, officers and directors or business location. – Refuses to identify a legitimate source for funds or information is false, misleading or substantially incorrect. – Background is questionable or differs from expectations based on business activities. – Customer with no discernible reason for using Aktagold service. Efforts to Avoid Reporting and Recordkeeping – Reluctant to provide information needed to file reports or fails to proceed with transaction. – Tries to persuade an employee not to file required reports or not to maintain required records. – "Structures" deposits, withdrawals or purchase of monetary instruments below a certain amount to avoid reporting or recordkeeping requirements. – Unusual concern with Aktagold Operation´s compliance with government reporting requirements and Aktagold AML/CFT policies. Certain Funds Transfer Activities – Wire transfers to/from financial secrecy havens or high-risk geographic location without an apparent business reason. – Many small, incoming wire transfers or deposits made using checks and money orders. Almost immediately withdrawn or wired out in manner inconsistent with customer's business or history. May indicate a Ponzi scheme. – Wire activity that is unexplained, repetitive, unusually large or shows unusual patterns or with no apparent business purpose. Activity Inconsistent with Business – Transactions patterns show a sudden change inconsistent with normal activities. – Unusual transfers of funds or journal entries among accounts without any apparent business purpose. – Maintains multiple accounts, or maintains accounts in the names of family members or corporate entities with no apparent business or other purpose. – Appears to be acting as an agent for an undisclosed principal but is reluctant to provide information. Other Suspicious Customer Activity – Unexplained high level of account activity with very low levels of securities transactions. – Funds deposits for purchase of a long-term investment followed shortly by a request to liquidate the position and transfer the proceeds out of the account. – Law enforcement requests.

c) Responding to Red Flags and Suspicious Activity: When an employee of Aktagold detects any red flag, or other activity that may be suspicious, he or she will notify the CCO. Under the direction of the CCO, Aktagold will determine whether or not and how to further investigate the matter. This may include gathering additional information internally or from third-party sources, contacting the government, freezing the account and/or informing the authorities.

9. Suspicious Transactions Reporting

a) We will file a Suspicious Activity Report ("SAR") with the FinCEN, or the appropriate regulatory authority for any transactions (including deposits and transfers) conducted or attempted by, at or through Aktagold involving $10,000 or more of funds (either

individually or in the aggregate) where we know, suspect or have reason to suspect: (1) the transaction involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity as part of a plan to violate or evade law or regulation or to avoid any transaction reporting requirement under law or regulation; (2) the transaction is designed, whether through structuring or otherwise, to evade any requirements of the regulations; (3) the transaction has no business or apparent lawful purpose or is not the sort in which the customer would normally be expected to engage, and after examining the background, possible purpose of the transaction and other facts, we know of no reasonable explanation for the transaction; or (4) the transaction involves the use of Aktagold to facilitate criminal activity. We will also file a report and notify the appropriate law enforcement authority in situations involving violations that require immediate attention, such as terrorist financing or ongoing money laundering schemes. We may file a voluntary report for any suspicious transaction that we believe is relevant to the possible violation of any law or regulation but that is not required to be reported by us. It is our policy that all suspicious activities will be reported regularly to the Board of Directors and appropriate senior management.

b) Currency Transaction Reports. Aktagold only allows FIAT currency transactions once accounts are activated. Any transfers over $10,000 may be reported to the authorities.

c) Currency Transportation. Aktagold prohibits both the receipt of currency or other monetary instruments that have been transported, mailed or shipped to us. Aktagold only accepts currency transactions through financial institutions and internationally recognized payment platforms.

10. AML/CFT Recordkeeping

a) Responsibility for Required AML Records: Our CCO and his or her designee will be responsible for ensuring that AML/CFT records are maintained properly. In addition, as part of our AML/CFT program, Aktagold will create and maintain all relevant documentation on customer identity and verification (See Section 4 above) and funds transmittals. We will maintain all documentation for at least five (5) years.

b) AML/CFT Reporting Maintenance and Confidentiality: We will hold reports and any supporting documentation confidential. We will not inform anyone outside of the authorities or other appropriate law enforcement or regulatory agency about a report. We will segregate report filings and copies of supporting documentation from other firm books and records to avoid disclosing information. Our CCO will handle all requests for reports.

11. Clearing/Introducing Relationships

We will work closely with all collaborating institutions to detect money laundering. We will exchange information, records and data as necessary to comply with AML/CFT laws.

12. Training Programs

We will develop ongoing employee training under the leadership of the CCO and senior management. Our training will occur on at least an annual basis. It will be based on our firm's size, its customer base, and its resources and be updated as necessary to reflect any new developments in the law. Our training will include, at a minimum: (1) how to identify red flags and signs of money laundering and/or the financing of terrorism that arise during the course of the employees' duties; (2) what to do once the risk is identified (including how, when and to whom to escalate unusual customer activity or other red flags for analysis and, where appropriate, the filing of reports to the authorities; (3) what employees' roles are in Aktagold compliance efforts and how to perform them; (4) Aktagold record retention policy; and (5) the disciplinary consequences (including civil and criminal penalties) for non-compliance with these regulations. We will develop training in our firm, or contract for it. Delivery of the training may include educational pamphlets, videos, intranet systems, in-person lectures and explanatory memos. We will maintain records to show the persons trained, the dates of training and the subject matter of their training. We will review our operations to see if certain employees, such as those in compliance, and corporate security, require specialized additional training. Our written procedures will be updated to reflect any such changes.

13. Program to Independently Test AML /CFT Program

The testing of our AML/CFT program will be performed at least annually (on a calendar year basis) by the testing officer, personnel of Aktagold, who is not the CCO nor does he perform the AML/CFT functions being tested nor does he report to any such persons. His qualifications include a working knowledge of applicable requirements under the FinCEN rules and regulations. To ensure that he remains independent, we will separate his functions from other AML/CFT activities. Independent testing will be performed more frequently if circumstances warrant. After we have completed the independent testing, staff will report its findings to the CCO. We will promptly address each of the resulting recommendations and keep a record of how each noted deficiency was resolved.

14. Confidential Reporting of AML/CFT Non-Compliance

Employees will promptly report any potential violations of Aktagold AML/CFT compliance program to the CCO, unless the violations implicate the CCO, in which case the employee shall report to the testing officer. Such reports will be confidential, and the employee will suffer no retaliation for making them.

15. Additional Risk Areas

Aktagold has reviewed all areas of its business to identify potential money laundering and/or financing of terrorism risks that may not be covered in the procedures described above. The major additional areas of risk include future changes to regulations and hacking attempts on Aktagold servers. Additional procedures to address these major risks are maintaining constant contact with the FinCEN and consistently performing security checks on Aktagold server security.