



ANTI-MONEY LAUNDERING (AML) PROGRAM AND PLAN OF ACTION: POLICIES, COMPLIANCE AND SUPERVISORY PROCEDURES

FinCEN – Financial Crimes Enforcement Network and OECD AML/CFT FAFT-GAFI guidelines

COMPANY POLICY

Thank you for reading **QUANTUM GROUP LLC** (hereon, “**QUANTUM**”) ANTI-MONEY LAUNDERING (AML) PROGRAM AND PLAN OF ACTION. Additionally, we have developed an internal procedural training course for contractors and employees and all parties associated with **QUANTUM** (Team Members) as well as those of its affiliate company, **QUANTUM CONSULTING, INC.**

It is the policy of **QUANTUM** to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities by complying with all applicable requirements under the Bank Secrecy Act (BSA) and its implementing 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. (1) 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. (2) 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. (3) 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 like 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.

To assist dealers in precious metals, precious stones, jewels, and finished goods (“Covered Goods”) in the fight against the financing of terrorism and money laundering, various resources have been made available.

Among the resources used to prepare this AML program are the following:

31 C.F.R. § 1010

<http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&SID=1d4b7666c253f04d69699bbde806fee&rgn=div5&view=text&node=31:3.1.6.1.2&idno=31>)



31 C.F.R. § 1027

(<http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&SID=1d4b7666c253f04d69699bbde806efee&rgn=div5&view=text&node=31:3.1.6.1.2&idno=31>)

FinCEN FAQs

(<https://www.fincen.gov/resources/statutes-regulations/guidance/frequently-asked-questions-0>)

Notice of Proposed Rulemaking (68 FR 8480), February 21, 2003

(<https://www.gpo.gov/fdsys/granule/FR-2003-02-21/03-4171/content-detail.html>)

Interim Final Rule, June 9, 2005

(<https://www.gpo.gov/fdsys/pkg/FR-2005-06-09/pdf/05-11431.pdf>)

“For most dealers, the requirements are (1) to establish an anti-money laundering program, (2) to file IRS/FinCEN Form 8300, (3) to file FinCEN Form TD F 90–22.1 [Report of Foreign Bank and Financial Accounts], and (4) to file FinCEN Form 105 [Report of International Transportation of Currency or Monetary Instruments].”

OECD AML/FT FAFT-GAFI guidelines (www.oecd.org) and (www.fatf-gafi.org):

- **Money Laundering and Terrorist Financing Awareness Handbook for Tax Examiners and Tax Auditors** – <https://www.oecd.org/ctp/crime/money-laundering-awareness-handbook.htm>
- **Bribery and Corruption Awareness Handbook for Tax Examiners and Tax Auditors** – <https://www.oecd.org/ctp/bribery-and-corruption-awareness-handbook-for-tax-examiners-and-tax-auditors-9789264205376-en.htm>
- **Report on Identity Fraud: Tax Evasion and Money Laundering Vulnerabilities** – <https://www.oecd.org/ctp/crime/identity-fraud-tax-evasion-and-money-laundering-vulnerabilities.htm>
- **FATF Standards – The FATF Recommendations, the international anti-money laundering and combating the financing of terrorism and proliferation (AML/CFT) standards, and the FATF Methodology to assess the effectiveness of AML/CFT systems.**
- **FATF Recommendations 2012 – amended October 2020** – <https://www.fatf-gafi.org/publications/mutualevaluations/documents/fatf-methodology.html>
- **Methodology 2013 – amended October 2019** – <https://www.fatf-gafi.org/publications/mutualevaluations/documents/fatf-methodology.html>
- **Procedures for the FATF Fourth Round of AML/CFT Mutual Evaluations – amended October 2019** – <https://www.fatf-gafi.org/publications/mutualevaluations/documents/4th-round-procedures.html>

- **Consolidated Processes and Procedures for Mutual Evaluations and Follow-Up (Universal Procedures) – amended October 2019 –**
<https://www.fatf-gafi.org/publications/mutualevaluations/documents/universal-procedures.html>

“Under an interim final rule by the Financial Crimes Enforcement Network (FinCEN), dealers in precious metals, stones or jewels are required to establish anti-money laundering programs. At a minimum, dealers must establish an anti-money laundering program that covers the following:

- Policies, procedures, and internal controls based on the dealer’s assessment of the money laundering and terrorist financing risk associated with its business.
- A compliance officer who is responsible for ensuring that the program is implemented effectively.
- Ongoing training of appropriate persons concerning their responsibilities under the program.
- Independent testing to monitor and maintain an adequate program.

“FinCEN is issuing this regulation to better protect those that deal in jewels, precious metals and precious stones from potential abuse by criminals and terrorists. “The characteristics of jewels, precious metals and precious stones that make them valuable also make them potentially vulnerable to those seeking to launder money,” said William J. Fox, Director of FinCEN. “This regulation is a key step in ensuring that the Bank Secrecy Act is applied appropriately to these businesses.”

“The interim final rule applies to ‘dealers’ that have purchased and sold at least \$50,000 worth of ‘covered goods’ during the preceding year”. The dollar threshold is intended to ensure that the rule only applies to persons engaged in the business of buying and selling a significant amount of these items, rather than small businesses, occasional dealers and persons dealing in such items for hobby purposes. ‘Covered goods’ include jewels, precious metals, and precious stones, and finished goods (including but not limited to, jewelry, numismatic items, and antiques) that derive 50 percent or more of their value from jewels, precious metals or precious stones contained in or attached to such finished goods. The interim final rule is final and binding.”

QUANTUM its team members, contractors and its related affiliate uses all its commercially reasonable efforts to comply with FinCEN regulations as well as with OECD AML/FT FAFT-GAFI guidelines. As a dealer in precious metals, **QUANTUM** uses its commercially reasonable efforts to only source its customers’ precious metals from companies that comply with FinCEN regulations and OECD AML/FT FAFT-GAFI guidelines as it is required, respectively. Additionally, **QUANTUM** has an express policy against aiding and abetting in the act of money laundering or facilitating any illegal acts governed by the USA Patriot Act or otherwise, as well as those that infringe the set rules of FAFT-GAFI AML/FT.

Because of our ironclad resolve and set in stone AML Program, **QUANTUM** is not a good target for the cleaning or disguising of criminal proceeds. We continually vow to do our absolute best to thwart any attempts to use our products to assist in any criminal activities including money laundering and terrorist financing.



By agreeing to **QUANTUM'S** terms and conditions and consummating a transaction, each customer represents and warrants to **QUANTUM** that:

- The customer is in compliance with the USA Patriot Act.
- The customer is in compliance with OECD AML/FT FAFT-GAFI guidelines.
- None of the funds being used to consummate the transaction were derived from or related or connected to money-laundering, terrorism or any other illegal or illicit activity.
- The transaction is not a scheme, or part of a scheme, involving or in support of terrorism, money-laundering or any other illegal or illicit activity.

QUANTUM, all times, reserves the right to require the customer to provide supporting information and documentation in support of the preceding representations and warranties or to ensure compliance with FinCEN regulations and OECD AML/FT FAFT-GAFI guidelines. **QUANTUM** maintains an active Anti-money Laundering Program and has designated one of its executive team members as a compliance officer, elected yearly, who actively monitors sales activity, trains staff, and monitors changes to regulations.

At least annually, there shall be an independent review and test for implementation and function of this program. Such independent review may be conducted by an employee of the Company, but must not work specifically for the AML Compliance Officer or be involved in the operation or oversight of the AML Compliance Program, in order to provide a fair and unbiased appraisal.

In summary, **QUANTUM** has an ironclad policy against aiding and abetting in the act of money laundering, terrorism financing or facilitating any and all illegal acts as governed by the United States Patriot Act, OFAC Office of Foreign Assets Control, FinCEN, OECD AML/FT FAFT-GAFI guidelines as well as forbidding the violation of any US state and or federal law.

RISK ASSESSMENT

Operating through **QUANTUM**, the Company is a precious metals dealer. All client dealings are internet and telephone based. **QUANTUM DOES NOT ACCEPT CASH PAYMENTS UNDER ANY CIRCUMSTANCES**. The Company currently accepts the following payment methods: bank wire, and in the future may considered certified credit card purchases with a third-party security merchant processor with AML/FT compliance and background check services. In assessing the money laundering risk exposure of the Company, we have considered all relevant factors including, but not limited to the following:

- **Products Bought and Sold:** As a precious metals dealer, the Company buys and sells gold and silver coins and bars. Our main business activity is to sell gold coins and bars to investors that want to diversify from their current assets to gold and silver in the form of coins or bars which are to be stored with a third-party depository service.
- **Customers:** Transactions with repeat customers do occur but are infrequent. For this reason, our customer base would typically be "non-established" under BSA regulations.

QUANTUM is not a click & buy online platform; in fact, all prospective clients must fill out a thorough **compliance questionnaire and client application, including completing a KYC form** (a copy individual and company entity KYC form is annexed to this document) in addition to going through a lengthy phone interview with a sales representative to find out the reason (legitimate intent) why they want to purchase precious metals, this initial interview gives **QUANTUM** the opportunity to assess the risk a prospective client might pose.

Here are some of the questions we ask:

- Are you looking to invest for long or short term?
- What is your main motivation for investing in gold or silver?
- Current presidential agenda?
- US Debt?
- Possible war?
- Falling dollar?
- Inflation?
- Deflation?
- At this point the prospective client is asked to expand on his thoughts about what he says is the reason why he wants to buy gold or silver.
- Where is the money that will be used to purchase precious metals coming from?
- Cash accounts? (bank accounts)
- Stocks?
- Bonds?
- IRA accounts?
- ETC.

Additional questions are asked to determine what he/she did or does for a living and conclude if the amount he/she has to invest matches the kind of income he/she has/had correlates to his/her skills.

As a further security measures, all calls may be monitored and recorded for compliance and training purposes.

We do not accept cash or cashier's checks as payments for a transaction, bank wires/ACHs as indicated above, and we do not accept orders from a third party.

Distribution Channels: Our business is conducted by telephone and over the internet from our websites. Covered Goods are typically shipped from the supplier to a depository transported by armored security transportation company such as Brinks.

Product Risk: **QUANTUM** intermediates gold and silver coins and bars only, but our focus is on premium numismatics and semi numismatics which carry a higher premium than its bullion counterpart. Such products are less desirable to money launderers as the cost is much higher than the metals melt down value.

Control for Higher Risk Situations: **QUANTUM** will continue to train its staff with focus on its sales team as they are the point of contact with the firm. We will have monthly meetings in which possible money laundering scenarios will be discussed and how to detect and report them. If we have reason to suspect that a prospective client is trying to hide his motives for purchasing gold or silver, we will take the following steps:

1. Ask for additional identification information such as:
 - a. Valid US ID or Passport
 - b. Proof of address such as telephone bill or bank statement
 - c. If still employed, letter of employment
 - d. If not employed, explanation of source of income
2. If the prospect client declines to provide the required information, we will decline the transaction and report it to the AML compliance officer.
3. The AML compliance officer will determine whether we need to file a SAR and or report it to FINCEN
4. AML officer will also submit all gathered information, including name, phone number, IP address and audio recording of the conversation with the prospective client, if applicable.

Note: We have every reason to believe that our clients that have US Dollars assets are deeply concerned with the massive US debt load economy and want to protect them from the resulting inflation.

Furthermore, to continue to aid AML policies, **QUANTUM** has the following clause in the firm's account agreement to deterred criminals and terrorists:

“Legitimate Monies & Intent: By authorizing this contract and funding an account the customer represent and warrant to **QUANTUM** that (i) this document has customer legal name and current address and(ii) That the customer is in complete compliance with the USA Patriot Act and with guidelines from OFAC Office of Foreign Assets Control, FinCEN, OECD AML/FT FAFT-GAFI, and (iii) none of the monies for this and subsequent purchases are derived from or in connection with money-laundering, terrorism or any other illegal or illicit activity(iii) the transaction is not part of a scheme, involving or in support of terrorism, money-laundering or any other illicit or illegal activity.”

Taking into account these and other considerations, we have developed and implemented the following policies, procedures and internal controls to prevent the Company from being used to facilitate money laundering and the financing of terrorist activities through the purchase and sale of Covered Goods.

AML COMPLIANCE PERSON DESIGNATION AND DUTIES

The Company has a designated Anti-Money Laundering Program Compliance Person (AML Compliance Person), with full responsibility for the Company's AML program.

The AML Compliance Person has a working knowledge of the BSA and its implementing regulations and is qualified by experience, knowledge, and training. The duties of the AML Compliance Person will include monitoring the firm's compliance with AML obligations and overseeing communication and training for employees.

The AML Compliance Person will also ensure that the firm keeps and maintains all of the required AML records and will ensure that Suspicious Activity Reports (SARs) are filed with the Financial Crimes Enforcement Network (FinCEN) if or when appropriate. The AML Compliance Person is vested with full responsibility and authority to enforce the firm's AML program. Duties important to mention:

- Develop, implement and update appropriate anti-money laundering and terrorist financing risk policies and procedures; including procedures for ensuring all required reports are made and all required records are maintained;
- Provide ongoing training of relevant employees, including senior officers;
- Prepare, review and file Form 8300; and
- Monitor the day-to-day operations and implementation of the Program.

When requested by FinCEN, the Company will provide FinCen with contact information for the AML Compliance Person including: (1) name; (2) title; (3) mailing address; (4) email address; (5) telephone number; and (6) facsimile (if any). Following the initial request from FinCEN, the Company will promptly notify FinCEN of any change in this information. (see 31 C.F.R. § 1010.520(a)(3)(iii)).

Questions about the BSA anti-money laundering laws, this Policy or the Program should be addressed to the AML Compliance Officer.

Transport Transactions Reporting

FinCEN Form 105. The Company shall file, when applicable, with FinCEN Form 105 under the following circumstances:

- When the Company physically transports, mails, or ships, or causes to be physically transported, mailed, or shipped currency or other monetary instruments in an aggregate amount exceeding \$10,000 at one time from the United States to any place outside the United States or into the United States from any place outside the United States.
- When the Company receives in the United States currency or other monetary instruments in an aggregate amount exceeding \$10,000 at one time which have been transported, mailed, or shipped to the Company from any place outside the United States.
- Such filing is not required for a transfer of funds through normal banking procedures, which does not involve the physical transportation of currency or monetary instruments.
- Any transactions conducted between a payer (or its agent) and the Company in a 24-hour period are related transactions.
- Transactions are considered related even if they occur over a period of more than 24 hours if the Company knows, or has reason to know, that each transaction is one of a series of connected transactions.

GIVING AML INFORMATION TO FEDERAL LAW ENFORCEMENT AGENCIES AND OTHER FINANCIAL INSTITUTIONS

a. FinCEN Requests Under USA PATRIOT Act Section 314(a)

As required by 31 C.F.R. § 1010.520(a)(3), “upon receiving an information request from FinCEN under section 1020.520, we will expeditiously search 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 FinCEN’s request.” If we find a match, our AML Compliance Person will report it to FinCEN via FinCEN’s Web-based 314(a) Secure Information Sharing System within 14 days or within the time requested by FinCEN in the request. If the search parameters differ from those mentioned above (for example, if FinCEN limits the search to a geographic location), our AML Person will structure our search accordingly.

When our AML Compliance Person searches our records and does not find a matching account or transaction, we will not reply to the 314(a) requests. We will maintain documentation that we have performed the required search by printing a search self-verification document from FinCEN’s 314(a) Secure Information Sharing System evidencing that that we have searched the 314(a)-subject information against our records. We will not disclose the fact that FinCEN has requested or obtained information from us, except to the extent necessary to comply with the information request. Our AML Compliance Person will review, maintain and implement procedures to protect the security and confidentiality of requests from FinCEN similar to those procedures established to satisfy the requirements of Section 501 of the Gramm-Leach-Bliley Act with regard to the protection of customers’ nonpublic information.

We will direct any questions we have about the 314(a) requests to the requesting federal law enforcement agency as designated in the request. Unless otherwise stated in the 314(a) request, we will not be required to treat the information request as continuing in nature, and we will not be required to treat the periodic 314(a) Requests as a government provided list of suspected terrorists for purposes of the customer identification and verification requirements.

b. National Security Letters

We understand that the receipt of a National Security Letter (NSL) is highly confidential. We understand that none of our officers, employees or agents may directly or indirectly disclose to any person that the FBI or other federal government authority has sought or obtained access to any of our records.

If we file a SAR after receiving an NSL, the SAR will not contain any reference to the receipt or existence of the NSL. The SAR will only contain detailed information about the facts and circumstances of the detected suspicious activity.

Resource: FinCEN SAR Activity Review, Trends, Tips & Issues, Issue 8 (National Security Letters and Suspicious Activity Reporting) (4/2005). – https://www.fincen.gov/sites/default/files/shared/sar_tti_08.pdf

c. Grand Jury Subpoenas

We understand that the receipt of a grand jury subpoena concerning a customer does not in itself require that we file a Suspicious Activity Report (SAR). When we receive a grand jury subpoena, we will conduct a risk assessment of the customer subject to the subpoena as well as review the customer's account activity.

If we uncover suspicious activity during our risk assessment and review, we will elevate that customer's risk assessment and file a SAR in accordance with the SAR filing requirements. We understand that none of our officers, employees or agents may directly or indirectly disclose to the person who is the subject of the subpoena its existence, its contents or the information we used to respond to it. If we file a SAR after receiving a grand jury subpoena, the SAR will not contain any reference to the receipt or existence of the subpoena. The SAR will only contain detailed information about the facts and circumstances of the detected suspicious activity.

Resources: FinCEN SAR Activity Review, Trends, Tips & Issues, Issue 10 (Grand Jury Subpoenas and Suspicious Activity Reporting) (5/2006). – https://www.fincen.gov/sites/default/files/shared/sar_tti_10.pdf

d. Voluntary Information Sharing with Other Financial Institutions Under USA PATRIOT Act Section 314(b)

We may share information with other financial institutions regarding individuals, entities, organizations, and countries for purposes of identifying and, where appropriate, reporting activities that we suspect may involve possible terrorist activity or money laundering.

The AML Compliance Person will ensure that the Company files with FinCEN an initial notice before any sharing occurs and annual notices thereafter.

We will use the notice form found at FinCEN's website. Before we share information with another financial institution, we will take reasonable steps to verify that the other financial institution has submitted the requisite notice to FinCEN, either by obtaining confirmation from the financial institution or by consulting a list of such financial institutions that FinCEN will make available. We understand that this requirement applies even to financial institutions with which we are affiliated, and that we will obtain the requisite notices from affiliates and follow all required procedures.

We will employ strict procedures both to ensure that only relevant information is shared and to protect the security and confidentiality of this information, for example, by segregating it from the firm's other books and records.

We also will employ procedures to ensure that any information received from another financial institution shall not be used for any purpose other than:

- identifying and, where appropriate, reporting on money laundering or terrorist activities;
- determining whether to establish or maintain an account, or to engage in a transaction; or
- assisting the financial institution in complying with performing such activities.



Rules: 31 C.F.R. § 1010.540. Resources: FinCEN Financial Institution Notification Form; FIN-2009-G002: Guidance on the Scope of Permissible Information Sharing Covered by Section 314(b) Safe Harbor of the USA PATRIOT Act (6/16/2009). – <https://www.fincen.gov/resources/advisories/fincen-guidance-fin-2009-g002>

e. Joint Filing of SARs by Company and Other Financial Institutions

If we determine it is appropriate to jointly file a SAR, we understand that we cannot disclose that we have filed a SAR to any financial institution except the financial institution that is filing jointly. If we determine it is not appropriate to file jointly, we understand that we cannot disclose that we have filed a SAR to any other financial institution or insurance company.

Rules: 31 C.F.R. § 1023.320; 31 C.F.R. § 1010.430; 31 C.F.R. § 1010.540. Resources: FinCEN’s BSA E-Filing System. – <https://bsaefiling.fincen.treas.gov/main.html>

IDENTITY VERIFICATION

We will verify the identities of all our customers and suppliers as follows. We shall use the following procedures to verify the identity of the supplier:

- For a business entity, we shall record the name, address, and tax identification number. We shall verify the identity of the business by reviewing documents that show the existence of the entity, such as certified articles of incorporation, a government-issued business license, or a partnership agreement. In addition, we will request a copy of the supplier’s written AML policies and procedures.
- For an individual, we shall record the name, address, tax identification number and birth date. We shall verify the individual’s identity by reviewing and maintaining a copy of an unexpired, government issued identification.

High Risk Sales

For any high risk (as defined below) sale of covered goods in any calendar year, we shall use the following procedures to verify the identity of the customer:

- We will record the name and address of the customer. We will also verify the individual’s identity by reviewing and maintaining a copy of an unexpired, government issued identification.
- For any high-risk sale made to a non-established business entity customer, we shall record the name, address, and tax identification number of the entity. We shall verify the identity of the business entity by reviewing documents that show the existence of the entity, such as certified articles of incorporation, a government-issued business license, or a partnership agreement

MONITORING FOR AND RESPONDING TO SUSPICIOUS ACTIVITIES

1. High Risk. We recognize a high-risk level and will exercise diligence in the following situations:
 - a. When conducting business with parties located in, or transactions for which payment or account reconciliation is routed through accounts located in, jurisdictions that have been identified as particularly vulnerable to money laundering or terrorist financing;

- b. Unusual payment methods, such as the use of multiple or sequentially numbered ACHs or wire transfer, as well as intending to request acceptance of money orders, traveler's checks, or cashier's checks, or payment from third parties as we DO NOT ACCEPT ANY OF THESE.
 - c. Unwillingness by a customer or supplier to provide complete or accurate contact information, financial references, or business affiliations;
 - d. Attempts by a customer or supplier to maintain an unusual degree of secrecy with respect to the transaction, such as a request that normal business records not be kept;
 - e. Purchases or sales that are unusual for the particular customer or supplier, or type of customer or supplier; and
 - f. Purchases or sales that are not in conformity with standard industry practice.
2. Company Policies and Procedures.
- a) Transaction and Customer Due Diligence. Each high-risk transaction will be reviewed by our AML Compliance Person. As part of this review, we will make reasonable inquiries to determine whether the transaction may involve money laundering or terrorist financing. If it is determined that a proposed transaction is likely to involve money laundering or terrorist financing, our AML Compliance Person will direct the Company to refuse to consummate, withdraw from, or terminate such transaction. If it is determined that the transaction is not likely to involve money laundering or terrorist financing, our AML Compliance Person will approve the proposed transaction. We will document our review of and our reasons for approving the transaction.
 - b) Supplier Due Diligence (see FinCEN FAQ #3, <https://www.fincen.gov/resources/statutes-regulations/guidance/frequently-asked-questions-0>)
 - c) We will take reasonable steps to determine whether a supplier of Covered Goods is a dealer as defined by 31 C.F.R. § 1027.100 or whether the supplier is eligible for the retailer exemption. Reasonable steps will depend on the nature of our relationship with the supplier. In most cases, verbal or written representations of the supplier will be sufficient. In other cases, additional due diligence will be required.
- 3) Reporting Suspicious Activities. FinCEN has explained that “[t]he interim final rule... does not require dealers to file reports of suspicious activity with FinCEN.” When we determine that a proposed transaction is likely to involve money laundering or terrorist financing, our AML Compliance Person will direct the Company to refuse to consummate, withdraw from, or terminate such transaction. In addition, if our AML Compliance Person believes that it would be appropriate to report the proposed transaction to law enforcement authorities, our AML Compliance Person may take any one or more of the following actions:

- a. Contact local or federal law enforcement authorities;
- b. File a suspicious activity report with FinCEN;
- c. Unwillingness by a customer or supplier to provide complete or accurate contact information, financial references, or business affiliations;
- d. Report suspected terrorist activities to FinCEN using its Financial Institutions Hotline (866-556-3974).
- e. If we file a SAR, no officer, director, employee, or agent of Company shall notify any person involved in the reported transaction that a SAR has been filed.

BSA REPORTING

- 1) Filing of FinCEN Form 8300 (31 C.F.R. § 1010.330). If, during our business, a company receives currency more than \$10,000 in 1 transaction (or 2 or more related transactions), it should file FinCEN Form 8300 to report the receipt of such currency. The company should file Form 8300 by the 15th day after the date the currency was received. Although we **DO NOT ACCEPT CASH TRANSACTIONS** and will not have the need to file form 8300, for informational purposes as part of AML/FT information dissemination, we still present what will pertain to a company that accepts cash transactions.
- 2) Foreign Bank and Financial Accounts Reports (31 C.F.R. § 1010.350). We will file a FinCEN Form 114, Report of Foreign Bank and Financial Accounts (“FBAR”), or any successor form, with the Department of Treasury for any financial accounts of more than \$10,000 that we hold, or for which we have signature or other authority over, in a foreign country.
- 3) Currency and Monetary Instrument Transportation Reports (31 C.F.R. § 1010.340). The Company prohibits both the receipt of currency or other monetary instruments that have been transported, mailed or shipped to us from outside of the United States, and the physical transportation, mailing or shipment of currency or other monetary instruments by any means other than through the postal service or by common carrier. We will file a CMIR with the Commissioner of Customs if we discover that we have received or caused or attempted to receive from outside of the U.S. currency or other monetary instruments in an aggregate amount exceeding \$10,000 at one time (on one calendar day or, if for the purposes of evading reporting requirements, on one or more days). We will also file a CMIR if we discover that we have physically transported, mailed or shipped or caused or attempted to physically transport, mail or ship by any means other than through the postal service or by common carrier currency or other monetary instruments of more than \$10,000 at one time (on one calendar day or, if for the purpose of evading the reporting requirements, on one or more days).

AML RECORDKEEPING

In its release of the interim final rule, FinCEN wrote: “The collection of information is the recordkeeping requirement in section [1027.210(a)]. The information will be used by Federal agencies to verify compliance by dealers with the provisions of sections [1027.100 and 1027.210]. The collection of information is mandatory.”

- 1) **Responsibility to Retain Required Records.** Our AML Compliance Person or designee will be responsible for ensuring that AML records are maintained properly. To satisfy BSA recordkeeping requirements, we will create and retain copies of SARs, FinCEN Form 8300s, FinCEN Form 114s (FBARs), CMIRs, training materials, lists of training recipients, identity verification documentation for new customers, identity verification documentation for non-regulated suppliers, reviews of high-risk transactions, and any other records required to be made under BSA regulations. We will retain these records and their accompanying documentation for at least five years.
- 2) **Confidentiality of SARs.** We will hold SARs and any supporting documentation confidential. We will not inform anyone outside of FinCEN or another authorized agency about a SAR. We will refuse any subpoena requests for SARs or for information that would disclose that a SAR has been prepared or filed and immediately notify FinCEN of any such subpoena requests that we receive. We will segregate SAR filings and copies of supporting documentation from other firm books and records to avoid disclosing SAR filings. Our AML Compliance Person will handle all subpoenas or other requests for SARs.

TRAINING PROGRAMS

We will develop ongoing employee training under the leadership of the AML Compliance Person and senior management. Our training will occur on at least an annual basis. It will be based on our Company'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. a review of BSA regulations governing the precious metals, precious stones, and jewels industry;
2. a description of the money laundering risks found in our business model; and
3. what to do when suspicious activity is encountered.

We will develop training in our Company, 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.

Rule: 31 CFR § 1023.210(b)(4)

PROGRAM TO INDEPENDENTLY TEST AML PROGRAM

- a. **Staffing** The testing of our AML program will be performed by an independent third party. We will evaluate the qualifications of the independent third party to ensure they have a working knowledge of applicable requirements under the BSA and its implementing regulations. Rules: 31 C.F.R. § 1023.210(b)(4).
- b. **Evaluation and Reporting.** After we have completed the independent testing, staff will report its findings to senior management. We will promptly address each of the resulting recommendations and keep a record of how each noted deficiency was resolved. Rules: 31 C.F.R. § 1023.210(b)(4)

CONFIDENTIAL REPORTING OF AML NON-COMPLIANCE

Employees will promptly report any potential violations of the firm’s AML compliance program to the AML Compliance Person, unless the violations implicate the AML Compliance Person, in which case the employee shall report to another member of senior management. Such reports will be confidential, and the employee will suffer no retaliation for making them. Rule: 31 C.F.R. § 1023.210.

SENIOR MANAGER APPROVAL

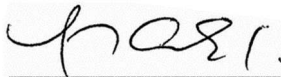
Senior management has approved this AML compliance program in writing as reasonably designed to achieve and monitor our firm’s ongoing compliance with the requirements of the BSA and the implementing regulations under it. This approval is indicated by signatures below. Rule: 31 C.F.R. § 1023.210.

Approved by the Board of Authorized Members,

Adopted: December 27, 2019
Updated: January 14th, 2026



Guillermo D. Ameglio
Co-Owner, Managing Partner
Republic of Panama



Argelis F. Ameglio
Co-Owner, Managing Partner
Republic of Panama



Carlos Ortega
CEO
Miami, FL

Acknowledgement

Company name: _____ a duly organized corporation in accordance with the laws of _____ [country] with headquarters in the city of _____ and duly represented in this act by (Name) _____ (Title) _____ declares to accept the principles contained in this Anti-Money Laundering and Combating the Financing of Terrorism (AML/FT) Policy, and to comply with the terms and conditions of this code.

_____ of _____ 20____

(Signature) _____