

**SEASIF PACIFIC, LLC**

**Anti-Money Laundering (AML)  
Policies and Procedures  
(AML Manual)**

**May 2021**



**Table of Contents**

1. Introduction and Background
2. Company's Internal Policy
3. Minimum Requirements of the AML Program
4. Risk Assessment
5. AML Compliance Officer Designation and Duties
6. Giving AML Information to Federal Law Enforcement Agencies
7. Checking Government Lists
8. Customer Identification and Verification (Know Your Customer – KYC)
  - a. Required Customer Information
  - b. Verification Procedures
  - c. Evaluating Customer Information
  - d. Customers Who Refuse to Provide Information
  - e. Lack of Verification
  - f. Recordkeeping
  - g. Notice to Customers and Request for AML Certification
9. Employee Background
10. Monitoring Accounts for Suspicious Activity
  - a. When to File a SAR
  - b. Red Flags
  - c. Responding to Red Flags and Suspicious Activity
11. BSA Reporting
  - a. Filing a SAR
  - b. Currency Transaction Reports (CTR): Form IRS 8300
  - c. Money Transfers
12. AML Recordkeeping
  - a. SAR Maintenance and Confidentiality
  - b. Company Liability for Reporting Suspicious Criminal Activities
  - c. Records Required
13. Training Programs
14. Testing the AML Program
15. Confidential Reporting of AML Non-Compliance
16. Senior Manager Approval

**APPENDICES:**

- I. Anti-Money Laundering Contacts
- II. Gramm-Leach-Bliley Act-Section 501-a
- III. Red Flags
- IV. Notice to Customers - Confirmation Letter of AML Written Compliance Procedures
- V. Supply Chain Policy for a Responsible Global Supply Chain of Mineral from Conflict Affected and High-Risk Areas
- VI. Site Visits to Key Customers in Domestic and International High-Risk Geographies (HRG)
- VII. Anti-Bribery AND Anti-Corruption Policy
- VIII. The Anti-Money Laundering Act of 2020

## **1. Introduction and Background**

The purpose of this manual is to set forth **SEASIF PACIFIC, LLC** (hereinafter referred as the Company) policies and procedures that ensure compliance with the requirements of various laws, regulations and acts relative to anti-money laundering and counter-terrorism financing (AML/CFT). It is the Company's policy and practice to comply with this laws and regulations. As regulatory changes occur, this manual will be revised and submitted for approval to the Board of Directors.

This manual provides guidance for daily operations and it is a training tool for new staff members. In addition, it may be used as a vehicle for periodic review of the policies and procedures contained herein to ensure that they are in compliance with the applicable AML/CFT laws and regulations.

This Manual will be revised from time to time and replacement pages will be provided to document any new regulations, laws and/or procedures as they are adopted. It is the responsibility of the company to provide copies of this Manual to each Officer, Employee, and/or a Staff member and keep the text and exhibits current by immediately inserting the new, revised pages in the appropriate Section and Page sequence.

### **Background**

The Financial Crimes Enforcement Network (FinCEN) was created in 1990 to support federal, state, local, and international law enforcement by analyzing the information required under the Bank Secrecy Act (BSA), one of the nation's most important tools in the fight against money laundering. The BSA's recordkeeping and reporting requirements establish a financial trail for investigators to follow as they track criminals, their activities, and their assets. Over the years, FinCEN staff has developed its expertise in adding value to the information collected under the BSA by uncovering leads and exposing unknown pieces of information contained in the complexities of money laundering schemes.

Dirty money can take many routes-some complex, some simple, but all increasingly inventive-the ultimate goal being to disguise its source. The money can move through banks, check cashers, money transmitters, businesses, casinos, and even be sent overseas to become clean, laundered money. The tools of the money launderer can range from complicated financial transactions, carried out through webs of wire transfers and networks of shell companies, to old-fashioned currency smuggling.

FinCEN researches and analyzes this information and other critical forms of intelligence to support financial criminal investigations. The ability to link to a variety of databases provides FinCEN with one of the largest repositories of information available to law enforcement in the country.

FinCEN provides a networking process designed to facilitate information sharing between agencies with shared investigative interests.

FinCEN's mission is to safeguard the financial system from illicit use, combat money laundering, and promote national security through the strategic use of financial authorities and the collection, analysis, and dissemination of financial intelligence.

Since its establishment in 1990, FinCEN has played a significant role in the U.S. Government's efforts to combat transnational organized crime. FinCEN carries out its mission by providing investigative support to law enforcement, intelligence, and regulatory agencies, cooperating globally with counterpart

financial intelligence units (FIUs), and using its regulatory authorities to make it more difficult for organized criminal groups to move money through the financial system. FinCEN supports the Department of the Treasury's efforts to promote the adoption of international standards involving AML/CFT, including through the Financial Action Task Force (FATF) where FinCEN led the delegation from 1994 through 1998. The National Security Council identified FinCEN as one of 34 Federal entities that it considered as having a significant role in the fight against international crime as noted in an August 2001 Government Accountability Office report.

FinCEN serves as the FIU of the United States; an FIU is the central agency within a jurisdiction responsible for collecting, analyzing, and disseminating financial information in furtherance of law enforcement investigations and prosecutions. FinCEN revolutionized the international tracking of transnational criminals through data sharing by joining with several other jurisdictions' FIUs to create the Egmont Group in 1995. At its founding, the Egmont Group focused on the establishment of FIUs. Today's Egmont Group is concentrating on the operational exchange of information to help law enforcement officials investigate and prosecute transnational organized crime. The important role that FIUs play has been recognized in the United Nations Convention Against Transnational Organized Crime, which recommends that every country establish an FIU.

FinCEN also exercises its authority under Section 311 of the USA PATRIOT Act, which allows for the imposition of special measures for jurisdictions, financial institutions, or international transactions of primary money laundering concern. The section allows for identifying customers using correspondent accounts, including obtaining information comparable to information obtained on domestic customers and prohibiting or imposing conditions on the opening or maintaining in the United States of correspondent or payable-through accounts for a foreign banking institution. Section 311 actions are only used after careful consideration and research. These actions are always well founded and the consequence of egregious financial crime sometimes involving terrorist finance and transnational organized crime. As these actions have shown, Section 311 has proven to have a very significant impact on targeted financial institutions.

The Currency and Foreign Transactions Reporting Act of 1970 (which legislative framework is commonly referred to as the "Bank Secrecy Act" or "BSA") requires U.S. financial institutions to assist U.S. government agencies to detect and prevent money laundering. Specifically, the act requires financial institutions to keep records of cash purchases of negotiable instruments, file reports of cash transactions exceeding \$10,000 (daily aggregate amount), and to report suspicious activity that might signify money laundering, tax evasion, or other criminal activities. It was passed by the Congress of the United States in 1970. The BSA is sometimes referred to as an "anti-money laundering" law ("AML") or jointly as "BSA/AML." Several AML acts, including provisions in Title III of the USA PATRIOT Act of 2001, have been enacted up to the present to amend the BSA.

On March 1, 2011, FinCEN transferred its regulations from BSA statute 31 CFR Part 103 to 31 CFR Chapter X as part of an ongoing effort to increase the efficiency and effectiveness of its regulatory oversight. 31 CFR Chapter X is organized by generally applicable regulations and by industry-specific regulations. This Manual was created following Chapter X of the BSA.

## **2. Company's Internal Policy**

It is the company's policy to prohibit and actively prevent money laundering and the funding of terrorist or other criminal activities. We define money laundering as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so unlawful proceeds appear to have been derived from legitimate origins or constitute legitimate assets.

Generally, money laundering occurs in three stages.

- **Placement:** the illegitimate funds are furtively introduced into the legitimate financial system. It could be cash, metal or stones first enter the financial system at the "placement" stage, where the gains generated from criminal activities are converted into monetary instruments, such as money orders or traveler's checks; or deposited into cash accounts or metals pool accounts at financial institutions or at companies dealing in precious metals or stones.
- **Layering:** At the "layering" stage, to further separate the money from its criminal origin, funds or metals are transferred or moved into other accounts or other financial institutions or into other companies dealing in precious metals or stones.
- **Integration:** At the "integration" stage, funds, metals or stones 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 the origin or intended use of the funds, which will later be used for criminal purposes.

Money laundering and terrorist finance are illegal. They undermine the security of our society and the viability and success of our business. Non-compliance risks business interruption, fines up to \$1 million, prison terms up to 20 years per count, forfeiture of assets, heavy legal expenses, and damage to individual and company reputation that may be irretrievable.

It is our policy to encourage all employees to report suspicious activity to the AML Compliance Officer. We have adopted this policy to help employees avoid involvement in money laundering and to encourage them to detect and report transactions as required by law. Employees who observe suspicious activity but are uncomfortable discussing it with the AML Compliance Officer should feel free to discuss the information with a senior manager, confidentially and without fear of retaliation.

The company management is committed to prevent any money laundering or terrorist finance scheme.

### **3. Minimum Requirements of the AML Program**

Institutions are required to establish and maintain a program to assure and monitor compliance with the requirements of the BSA and the Department of the Treasury regulations implementing the act. The program developed by an institution must:

- provide for the continued administration of policies and procedures;
- be reasonably designed to assure and monitor compliance with the record keeping and reporting requirements;
- be in writing

At a minimum, the AML program shall:

- Incorporate policies, procedures, and internal controls based upon the company's assessment of the money laundering and terrorist financing risks associated with its line(s) of business.
- Designate an AML Compliance Officer.
- Provide on-going education and training of appropriate persons concerning their responsibilities under the program.
- Provide independent testing to monitor and maintain an adequate program. The scope and frequency of the testing shall be commensurate with the risk assessment conducted by the company. Such testing may be conducted by an officer or employee of the company, so long as the tester is not the person designated as the AML Compliance Officer or a person involved in the operation of the program.

## **4. Risk Assessment**

### **Overview**

Although attempts to launder money, finance terrorism or conduct other illegal activity can emanate from many different sources, services, and customers, some geographic locations may be more vulnerable and have been historically abused by money launderers and criminals. Depending on the specific characteristics of the particular service or customer, the risks are not always the same.

Various factors, such as a number of transactions and dollar volume, and geographic location should be considered when making a risk assessment. In formulating a risk-based AML/BSA compliance program, management has identified the significant risk to the company and developed a risk assessment tailored to the company's unique circumstances. An effective AML/BSA compliance program controls risks that may be associated with the company's unique products, services, customers, and geographic locations. As new products and services are introduced, existing products and services change, the Company will institute appropriate policies, procedures, and processes to address those changes.

### **Customers, Service and Entities**

Although any type of product, customer, or service is potentially vulnerable to money laundering or terrorist financing activity, by the nature of their business, occupation or anticipated transactions activity, certain customers and entities may pose specific money laundering risks. However, the AML Compliance Department follows a risk-based approach and neither defines nor treats all members of a specific category of customers as posing the same level of risk. In assessing customer risk, the Company factors many variables, such as services sought, source of funds, nature of the business, products and services offered, target market, and geographic location.

Within any category of business there will be customers that pose varying levels of risk of money laundering.

For purposes of making the risk assessment required by the BSA, the Company will take into account all relevant factors including, but not limited to:

- The type(s) of products the Company buys and sells, as well as the nature of the Company's customers, suppliers, distribution channels, and geographic locations;
- The extent to which the Company engages in transactions other than with established customers or sources of supply, or other dealers; and

### **Geographic Locations**

Identifying geographic locations that pose a higher risk is essential to the Company's AML/BSA compliance program. The AML Compliance Department understands and evaluates the specific risks associated with doing business in or facilitating transactions involving certain geographic locations. However, geographic risk alone does not always determine an entity's or transaction's risk level, either positively or negatively.

High-risk geographic locations can be categorized as either international or domestic. International high-risk geographic locations generally include:

- Countries subject to OFAC sanctions, including state sponsors of terrorism.
- Countries identified as supporting international terrorism under section 6(j) of the Export Administration Act of 1979, as determined by the Secretary of State.
- Jurisdictions determined to be “of primary money laundering concern” by the Secretary of the Treasury, and jurisdictions subject to special measures imposed by the Secretary of the Treasury through FinCEN, pursuant to section 311 of the USA Patriot Act.
- Jurisdictions/countries identified as non-cooperative by the Financial Action Task Force on Money Laundering (FATF).
- Major money laundering countries and jurisdictions identified in the U.S. Department of State’s annual International Narcotics Control Strategy Report (INCSR), in particular countries which are identified as jurisdictions of primary concern.
- Other countries identified by the Company as high-risk because of its prior experiences, transaction history, or other factors (e.g., legal considerations, or allegations of official corruption).

Domestic high-risk geographic locations may include businesses doing business within, or having customer located within, a U.S. Government-designated high-risk geographic location. Domestic high-risk geographic locations include:

- High Intensity Drug Trafficking Areas (HIDTAs).
- High Intensity Financial Crime Areas (HIFCAs).

The Company’s primary service area is located in a HIDTA and HIFCAs. Do to this, the company primarily accepts business applications from customers who have a personal business history with the owner of the Company or have been referred by existing customers.

### **Account Opening Risk Assessment**

All accounts at the Company are reviewed by the AML Compliance Department. The risk assessment process is consulted with the owner. Should the customer be categorized high risk due to geographical location and type of business, the AML Compliance Department and the owner might consider onsite verification or rejecting the application. If the customer meets the following criteria, the customer will be considered high risk:

1. The business is organized outside the U.S.A.
2. The business has international operations from a high-risk country or territory.
3. The owner of the business or one of the principals is foreign government official or a close associate of a foreign government official, also know as Politically Exposed Person (PEP).
4. The business is one of the following:
  - a. Nontraditional Jewelry entities such as:
    - i. Currency exchange houses, also known as Giros or Casas de Cambio.
    - ii. Money transmitter.
    - iii. Check cashing facilities.



Because of the risk associated with the types of customers, products and services, and geographical locations, Enhanced Due Diligence beyond the minimum Customer Identification Program requirements may be necessary for certain customers. The AML Compliance Officer will determine if the resources offered by third-party vendors of doing onsite verification is necessary with these customers.

It is important to mention that new hires at the Company will be screened prior to hiring to insure we know the true identity of our employees via a police report, third-party vendors, and work history.

## **5. AML Compliance Officer Designation and Duties**

The Company designates Antoanela Chiritescu as its AML Compliance Officer, with full responsibility for the Company's AML program.

The AML Compliance Officer will be responsible for:

- ensuring that the AML program is implemented effectively, and it is updated as necessary to reflect changes in the risk assessment, requirements of the AML laws/regulations, and further guidance issued by the Department of the Treasury,
- assessing the company's exposure to money laundering,
- monitoring the firm's compliance with AML obligations,
- overseeing communication and training for employees,
- arranging for regular testing of AML systems and precautions,
- ensuring that proper AML records are kept and
- making sure Suspicious Activity Reports ("SARs") are filed accordingly, when necessary.

The Company will provide all employees with current contact information for the AML Compliance Officer, including name, title, mailing address, e-mail address, telephone number and facsimile number, along with contact information for regulatory and law enforcement officers (See Appendix I).

## **6. Providing and Sharing AML Information to Federal Law Enforcement Agencies**

Management has designated the AML Compliance Officer to coordinate with Government agencies on matters involving money laundering, terrorist finance and suspicious activity.

Employees should refer all Government regulatory or enforcement agency requests for information to the AML Compliance Officer.

The Company will respond to and cooperate with FinCEN and other Federal or State law enforcement and regulatory agencies. Contact with law enforcement and regulatory agencies and responses to requests for information about accounts or transactions will be handled through the AML Compliance Officer or other designated person.

That response will begin by immediately searching the Company's records, to determine whether we maintain or whether we have maintained any account or engaged in any transaction with an individual, entity, or organization named in the law enforcement request. Upon receiving an information request, we will designate one person to be the point of contact regarding the request and to receive similar requests in the future.

Unless otherwise stated in the request, we will search:

- Any current account maintained for a named suspect,
- Any account maintained by a named suspect during the preceding 12 months, and
- Any transaction conducted by or on behalf of or with a named subject during the preceding six months.

If the Company identifies an account or transaction identified with any individual, entity, or organization named in a request from FinCEN, it shall report to FinCEN, in the manner and in the time frame specified in FinCEN's request, the following information:

- A. The name of such individual, entity, or organization;
- B. The number of each such account, or in the case of a transaction, the date and type of each such transaction; and
- C. Any Social Security number, taxpayer identification number, passport number, date of birth, address, or other similar identifying information provided by the individual, entity, or organization when each such account was opened, or each such transaction was conducted.

If the request was made by FinCEN, we will respond accordingly, by calling its Hotline, 866-556-3974 or by completing FinCEN's subject information form. This information can be sent to FinCEN at [www.fincen.gov](http://www.fincen.gov). If the search parameters differ from those mentioned above (for example, if FinCEN requests longer periods of time or limits the search to a geographic location), the Company will adapt its search accordingly. If the Company searches its records, and does not uncover a matching account or transaction, the Company will reply that it has no records.

The Company will not disclose the fact that information has been requested, except to the extent necessary to comply with the information request. The Company will maintain procedures to protect the security and confidentiality of information requests from, such as those established to satisfy the requirements of Section 501 of the Gramm-Leach- Bliley Act (See Appendix II).

The Company will direct any questions to the requesting Federal law enforcement agency as designated in the request.

Unless otherwise requested in the information request, the Company will not be required to treat the information request as continuing in nature, and it will not be required to treat the request as a list for purposes of the customer identification and verification requirements.

The Company will not use information provided to a Government agency for any purpose other than (1) to report as required under the AML regulations; (2) to determine whether to establish or maintain an account, or to engage in a transaction; or (3) to assist the Company in complying with any requirement of the AML regulations.

## **7. Screening Government Lists**

Before an account is opened (or when required by another State or Federal law, regulation or directive issued about an applicable list), the Company will determine whether a customer or vendor appears on a list of known or suspected money-launderers, terrorists or terrorist organizations issued by any State or Federal government agency. The Company will follow all directives issued in connection with such lists.

The regulations apply to customers, suppliers and vendors alike, so the term "customers" when used in these AML Compliance and Supervisory Procedures will include customers, suppliers and vendors.

Before opening an account, the company will check to ensure that a customer does not appear on the Office of Foreign Assets Control ("OFAC") List of "Specifically Designated Nationals and Blocked Persons" (SDN or OFAC List), and is not from, or engaging in transactions with people or entities from embargoed countries and regions listed on the OFAC Web Site. OFAC, within the US Department of the Treasury, administers and enforces economic and trade sanctions based on US foreign policy and national security goals against targeted foreign countries and regimes, terrorists, international narcotics traffickers, those engaged in activities related to the proliferation of weapons of mass destruction, and other threats to the national security, foreign policy or economy of the United States. Since the OFAC Web Site is updated frequently; the Company will check the list on a regular basis. The company will also review other such lists made available by United States Government agencies, as well as lists of non-cooperative countries issued by international bodies such as the FATF and the United Nations (UN).

The Company may access these lists through various software programs to ensure speed and accuracy. The Company will also review existing accounts against these lists when they are updated, and the company will document its review.

If the Company determines a customer, or someone with whom the customer is doing business with, is on the SDN List or is engaging in transactions with a person or entity located in an embargoed country or region, the company will not proceed with the transaction pending clarification and instructions from FinCEN.

## **8. Customer Identification and Verification (Know your Customer – KYC)**

It is the Company's policy to abide by Know Your Customer (KYC) principles and guidelines generally accepted, and widely used, by the banking and non-banking community.

The Company has clear and comprehensive KYC policies and procedures to abide exposing the Company to criminal activity as well as a mean of detecting suspicious activities by its customers in a timely manner.

The Company's KYC policies and procedures have not been instituted to and shall not be used to interfere with the Company's commitment to foment lasting and profitable relationships with its customers, but rather to protect and ensure the Company's soundness as well as its good name and reputation in our community.

As a matter of general policy, the Company shall abide by the KYC principles in its daily business practice:

- a) Make a reasonable effort to determine the true identity of all customers requesting any Company services;
- b) Take particular care to identify the ownership of all accounts;
- c) Obtain valid and current identification from all new customers;
- d) Business account relationships shall not be established until the legal identity of the potential customer (the business) and principals of such a business are established;
- e) Obtain identification from customers seeking to conduct significant business transactions;
- f) Become aware of the transactions carried out by Company customers through KYC procedures;
- g) Become aware of any unusual transaction or activity that is disproportionate to the customer's known business;
- h) Obtain enough information from the customer to develop a "profile" of the customer;
- i) Once established, monitor "profiles" and update them as necessary;
- j) If a potential customer refuses to produce any of the requested information, the relationship shall not be established;
- k) If requested follow up information of a material nature is not produced by the customer, the relationship, if already established, shall be terminated;
- l) Maintain ongoing contact with the customer, including but not limited to correspondence, telephone calls and visits to the customer;
- m) Immediate contact shall be established with a customer whenever warranted, or when there is sufficient reason to believe the account relationship is no longer desirable for the Company; all instances of contact must be fully documented, and evidence retained in the customer's file.

The Company will use risk-based measures to ascertain, document and verify the identity of each customer. The Company will record customers' identification information and the verification methods and results; and compare customer identification information with government-provided lists of suspected terrorists.

#### INTERNATIONAL CUSTOMERS

1. The Company will establish and maintain systems and controls that will allow to manage effectively the risks involved in obtaining and establishing new international customers.
2. An international customer for the purpose of this AML Manual is defined as a legal corporate or natural person that does not reside nor is registered to do business in the United States of America and its territories.
3. The Company shall establish systems and controls that will allow the identification and delineation of a complete customer profile including the identification of the beneficial owners of the account. Similarly, appropriate controls must be in place to establish profiles for the owners/principals and signers in accounts of all business customers.
4. It is the Company's goal to ensure that the systems and controls established capture, monitor, and provide adequate reporting that will facilitate review of account activities of each customer.
5. The Company shall develop policies and procedures to detect, investigate and report suspicious transactions involving the Company's international customers.
6. International accounts will comply with the Know Your Customer Rules (KYC). No International relationship will be established if it does not comply with the KYC Rules and include all required documentation.

#### DOMESTIC CUSTOMERS

1. The Company will establish and maintain systems and controls that will allow to manage effectively the risks involved in obtaining and establishing new domestic customers.
2. A domestic customer is defined as a legal corporate or natural person with their legal residence or registered within the United States of America and its territories.
3. The Company shall establish systems and controls that will allow the identification and delineation of a complete customer profile. Similarly, appropriate controls are in place to establish profiles for the owners/principals of all business customers.
4. It is the Company's goal to ensure that the systems and controls established capture, monitor and provide adequate reporting that will facilitate review of activities of each customer.
5. The Company has developed policies and procedures to detect, investigate and report doubtful or suspicious transactions involving the Company's domestic customers.

6. Domestic accounts will comply with the Know Your Customer Rules (KYC). No Domestic relationships will be established if it does not comply with the KYC Rules and includes all required documentation.

**a. Required Customer Information**

Prior to opening an account, the Company will collect the following information for all accounts, if applicable, for any person, entity or organization who is opening a new account and whose name is on the account:

- name;
- date of birth (for an individual) or date of incorporation (for entities);
- address, which will be a residential or business street address, an Army Post Office ("APO") or Fleet Post Office ("FPO") number, or residential or business street address of next of kin or another contact individual (for an individual who does not have a residential or business street address), or a principal place of business, local office or other physical;
- an identification number, which will be a taxpayer identification number (for U.S. persons) or one or more of the following:
  - a taxpayer identification number,
  - passport number and country of issuance,
  - alien identification card number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or other similar safeguard (for non-U.S. persons).
  - If a customer has applied for, but has not received, a taxpayer identification number, we will request a copy of the application, and contact the appropriate U.S. governmental agency to confirm that the application was filed before the customer opens the account and to obtain the taxpayer identification number within a reasonable period after the account is opened.

**GENERAL REQUIREMENTS**

- Verify that all the information provided in the identification documents and the account opening documents matches. Ensure there are no inconsistencies.
- Verify that the identification documents are not expired and are reliable, to the best of your ability.
- Ensure that copies made for the file are clear, legible, and complete.

Contents

It is the Company's policy to incorporate the following principles within the Company's business practices:

- Determine the true identity of all customers requesting the Company's services. Company employees should be especially careful with new customers and those customers seeking to conduct significant business transactions.
- Detect and report any unusual transaction activity, i.e., any suspicious activity being conducted by the customer.



In order to detect and report suspicious transactions, the following procedure is implemented and will be followed:

- Collect sufficient information to develop a transaction profile of each customer to enable the Company to project with relative certainty the types of transactions that a customer is likely to transact.
- Include in the Company's employee education program, examples of customer behavior, or activity that may warrant investigation.

#### Standards and Procedures

The Company's Know Your Customer Standard consist of three tiers of guidelines for:

1. Opening new accounts, domestic and international;
2. Compare all information provided by client with the designated systems;
3. Keep a record of all information acquired in the process;

#### Taxpayer Identification Account (TIN)

The Bank Secrecy Act requires the Company to obtain the taxpayer identification number of the person who holds the account. For new accounts, the Company must obtain the appropriate number within 30 days of the account opening. If the account is in the name of two or more individuals, the Company must obtain the tax identification number of all persons who have a financial interest in the account.

The Company is not liable when a person who opens an account has applied for a social security or taxpayer ID number on Forms SS-4 or SS-5 but does not receive the number within 30 days. The time is extended for another 30 days for the applicant to have a reasonable opportunity to receive the number and supply it to the Company. If the TIN is not supplied in a timely manner, it is important that the account officer, or designee, follow up with the customer. Accounts should be closed within 90 days in which the applicants have not provided the Company their taxpayer's identification number.

#### ID Numbers That Must Be Obtained

The Company must obtain the number of:

- Sole Proprietorship: Social Security number of the owner or the Employer ID number;
- Employer ID number of the Entity, for an Association, Partnership or Corporation;
- Company Certificate of Registration.

#### Verification Procedures

In order to verify the identity of the account applicant(s), the staff must:

- Maintain copies of customer identification;
- Perform a screening against government lists and maintain a copy of the results in the file; and

The Compliance Officer is responsible for reviewing the identification provided by the account holder to ascertain that they refer to the prospective account holder.

- a. For International Customers request two banking references from the customer. Any deviation from obtaining two banking references will be reviewed by the Compliance Department on a case by case basis. Depending on the research conducted and the comfort level established, the Compliance Department may accept or waive the requirement of the two banking references.
- b. A referral alone from a Company employee, Director, Shareholder or from one of the Company's accepted customer is not sufficient to identify the customer; however, in most instances, it should warrant less vigilance than otherwise required.

#### **BUSINESS ACCOUNT REQUIREMENTS**

Prior to opening a business account, the Business Application must be completed. The following information must be obtained as applicable:

##### **CORPORATIONS**

- Articles of Incorporation;
- Trade Name Certificate (if corporation also operates under a trade name);
- Tax Identification Number; and
- Corporate Resolution

##### **PARTNERSHIPS**

- Certificate of Registration and/or Articles of Limited Partnership with Secretary of State;
- Partnership Agreement evidencing the identity of the partners;
- Trade Name Certificate (if also operating under a trade name); and
- Tax Identification Number.

##### **SOLE PROPRIETORSHIPS**

- Trade Name Certificate or similar document; and
- Tax Identification Number (or proprietor's social security number).

##### **LIMITED LIABILITY COMPANIES**

- Articles of Incorporation;
- Trade Name (Fictitious Name if applicable);
- Tax ID;
- Operating Agreement; and
- Do not use a Corporate Resolution Form to obtain authorization; use an LLC form.

In addition, all Businesses must provide:

- Street address (P.O. Box may be used as secondary address only);
- Business telephone number, fax number and e-mail address;
- Nature of Business (must be SPECIFIC).

Obtain from all Authorized Signers:

- Acceptable picture identification;

- Taxpayer identification number or Social Security Number; and
- Home street address, telephone number and e-mail address of account signers and major owners (10% or more).

**BSA Compliance Officer must approve ALL International Businesses prior to opening an account. If approved, obtain the:**

- Country of the business with appropriate authorization to do business (equivalent to corporate articles, partnership agreements, etc.)
- Business license;
- Two (2) bank references;
- Certificate of Good standing from appropriate government authority; and
- One reference letter.

To verify the identity of the business account applicant(s) and owners/principals, the Customer Service staff must:

- Perform a screening against government lists (like OFAC) on the business and each owner/authorized signer and maintain a copy of the results in the file;
- Verification in the Department of State website (like Sunbiz for Florida or other State's equivalent) and maintain a copy in the file;
- Obtain a "Certificate of Good Standing" from appropriate government authority from the respective country.

#### **b. Verification Procedures**

In addition to collecting the required information discussed above, the Company will verify the identity of the customer using that information. The required verification will occur before the account is opened. If additional verification is needed, verification will occur within a reasonable time after the account is opened.

Based on the risk, and to the extent reasonable and practicable, the Company will ensure that it has a reasonable belief to know the identity of its customers by verifying and documenting the accuracy of the information collected.

The Company will verify customer identity through documentary evidence, non-documentary evidence, or both. The Company will use Government-issued documents to verify customer identity when appropriate documents are available. The Company will supplement the use of documentary evidence by using the non-documentary means described below whenever possible. In analyzing the verification information, it will consider whether there is a logical consistency within the identifying information provided, such as the customer's name, street address, zip code, telephone number, date of birth, and social security number.

#### Verification through Documents

One or more of the following documents will be used to verify a customer's identity. The company may use other documents to establish that it has reasonable belief that it knows the true identity of the customer. Given the availability of the counterfeit or fraudulently obtained documents, the Company is encouraged to obtain more than a single document to ensure that it has reasonable belief that it knows the customer's true identity.

For Individuals:

- An unexpired government issued identification evidencing nationality or residence and bearing a photograph or similar safeguard, such as driver's license, passport or military ID.

For an Entity other than an Individual (such as corporation, sole proprietorship, partnership, limited liability company, or trust):

- Documents showing the existence of the entity, such as certified articles of incorporation, corporate or partnership resolutions, an unexpired government-issued business license, a partnership agreement, or a trust instrument (in its entirety).

For business accounts, the Company will also consider utilizing one or more of the following methods:

- Conduct a site visit of the place of business; and/or
- Visit the business website or send a confirming electronic message to the business e-mail address.

The Company is aware that it is not required to take steps to determine whether the document that the customer has provided for identity verification has been validly issued and that it may rely on government-issued identification as verification of a customer's identity. If the document shows some obvious form of fraud, the Company will consider this as a factor in determining whether it can form a reasonable belief as to the customer's identity.

Non-documentary verification

The Company might use any of the following non-documentary methods of verifying identity:

- Contacting a customer;
- Independently verifying the customer's identity through the comparison of information provided by the customer with information obtained from a consumer reporting agency, public database, or other source;
- Checking references with other company's financial institutions; or
- Obtaining a financial statement.

The Company will use non-documentary methods of verification in the following situations:

- (1) when the customer is unable to present an unexpired government-issued identification document with a photograph or other similar safeguard;
- (2) when the firm is unfamiliar with the documents the customer presents for identification verification;
- (3) when the customer and firm do not have face-to-face contact; and
- (4) when there are other circumstances that increase the risk that the firm will be unable to verify the true identity of the customer through documentary means.

Depending on the nature of the account and requested transactions, the Company may refuse to complete a transaction before it has verified the information, or in some instances when the Company needs more time, the Company may restrict the types of transactions or dollar amount of transactions.

**c. Evaluating Customer Information**

The Company will perform an initial risk assessment of each new customer. A questionable assessment will be treated as an internal "red flag." The account opening application will be annotated for ongoing consideration by the AML Compliance Officer.

**RED FLAGS**

By following the "Know Your Customer" procedures, the Company employees may encounter one or more of the following "RED FLAGS":

- The customer provides unusual or suspicious identification documents;
- The customer is reluctant or refuses to provide personal background information, and/or references, other banking relationships, details concerning business activities;
- References cannot be verified or contacted;
- Home or business telephone number is disconnected;
- The customer's background is inconsistent with business activities;
- Recent ownership changes of the business, however the background of the new owners is inconsistent or incompatible with the nature of the business;
- The business financial statements are inconsistent with the type of business.

If the Company finds suspicious information that indicates possible money laundering or terrorist financing activity, the Company may file a SAR in accordance with applicable law and regulation.

The Company recognizes the risk of not knowing the customers. 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 designated by the U.S. as a primary money laundering concern or one that has been designated as non-cooperative by an international body. The Company will identify customers that pose a heightened risk if not properly identified, and may take the following additional measures to obtain information about the identity of the individuals associated with the customer when standard documentary methods prove to be insufficient:

1. Confirm the beneficial ownership of the account
2. Verify the identity of individuals with control or authority over the account

**d. Customers Who Refuse to Provide Information**

If a prospective or existing customer refuses to provide the information described above when requested, the Company may obtain this information from other sources. If a prospective or existing customer provides deliberately misleading information, it will be investigated and will not open the account or, after considering the risks involved, may consider closing any existing account. In either case, the AML Compliance Officer will be notified so that he can determine whether we should report the situation to FinCEN.

**e. Lack of Verification**

When the Company is unable to know the identity of a customer, it will do the following:

- (A) not open an account;
- (B) impose terms under which a customer may conduct transactions while the Company attempts to verify the Customer's identity;
- (C) close an account after attempts to verify customer's identity have failed; or
- (D) after consultation with the Company's Compliance Officer or Management, file a SAR.

**f. Recordkeeping**

The Company will document the verification, including all identifying information provided by a customer, the methods used and results of verification, and the resolution of any discrepancy in the identifying information. It will keep records containing a description of any document that the Company 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, the Company will retain documents that describe the methods and the results of any measures taken to verify the identity of a customer. The Company will maintain records of all identification information for five years after the account has been closed; as well as the records made about verification of the customer's identity for five years after the record was made.

**g. Notice to Customers and Request for AML Certification**

The Company will explain to its customers that the information requested from them is to verify their identities, as required by Federal law. In addition, the Company will require confirmation from its counterparties that they either have anti-money laundering programs or are exempt by completing the AML Certification form on the company's letterhead. (See Appendix IV)

If any counterparties are required to comply with the USA Patriot Act, Bank Secrecy Act and other legislation and regulations to prevent money laundering and terrorist financing, the Company will request, in addition to the AML certification form, that they have available a written AML program of compliance and supervisory procedures. (See Appendix IV).

## **9. Employee Background**

To protect the Company from employee complicity in money laundering or terrorist financing activity, the Company will collect and review background information prior to hiring every employee. The areas investigated depend on the sensitivity and seniority of an employee's position and may include but it is not limited to credit, criminal records and motor vehicle, prior employment and, in certain instances, drug tests. Certain of these checks will be done periodically after employment.

## **10. Monitoring Accounts for Suspicious Activity**

A suspicious transaction is a transaction where the Company has reason to believe, knows with certainty, or suspects:

1. The material being sold was obtained from an illegal activity (such as drug trafficking) or;
2. A person is structuring the transaction in such a manner as to evade the currency transaction reporting requirements.

By following proper "Know Your Customer" procedures, Company employees may encounter transactions that will trigger their suspicion. In these instances, Company employees are expected to follow the Company's Compliance Procedures to identify and report suspicious transactions.

The Company is firmly committed to the goal of full compliance with the laws and regulations promulgated to prevent money laundering and terrorist financing activities and other types of criminal activities. Therefore, the Company will assist and cooperate, in every way possible with the U.S. authorities (F.B.I., U.S. Attorney's office, Federal Deposit Insurance Corporation, State and Local Law Enforcement Authorities, etc.) in the discovery of suspected violations and will take whatever measures are necessary to report any suspicious activities or any known violations and to aid in the prosecution of those individuals responsible for the criminal conduct.

As a matter of policy and as a matter of law, the Company will report the detection of any suspected violation, known or suspected crimes.

All employees have the responsibility of referring to the AML Compliance Officer and/or the President and their department manager any type of suspicious activity that the staff member may encounter during the performance of his/her duties.

The Company will use sales management reports and manually monitor enough account activity to identify unusual size, volume, pattern or type of transactions, geographic factors such as whether jurisdictions designated as "non-cooperative" are involved, or any of the "red flags" identified in this AML Manual. The Company will review transactions, including trading and wire or metal transfers, in the context of other account activity to determine if a transaction lacks financial sense or is suspicious because it is an unusual transaction or strategy for that customer.

The AML Compliance Officer or his designee will be responsible for this monitoring, will document when and how it is carried out and, at the discretion of the AML Compliance Officer, will report suspicious activities to the appropriate authorities.

Included in the information the Company will use to determine whether to file a Form SAR are exception reports that include transaction size, location, type, number, and nature of the activity. The Company will create employee guidelines with examples of suspicious money laundering activity and will note high-risk clients whose accounts may warrant further scrutiny. The AML Compliance Officer will conduct an investigation before a SAR is filed.



**a. When to file a SAR**

The Company shall file a SAR if any known or suspected Federal criminal violation or pattern of criminal violations committed or attempted against the Company is discovered, or involving a transaction or transactions conducted through the Company, where the Company believes that it was either an actual or potential victim of a criminal violation, or series of criminal violations, or that the Company was used to facilitate a criminal transaction regardless of amount involved in the violation.

This applies also if any transaction conducted or attempted to go through the Company is suspicious, or has reason to suspect:

- The transaction involves funds derived from illegal activities or is conducted to hide or disguise funds from illegal activities as part of a requirement under Federal Law.
- The Transaction is designed to evade any regulations promulgated under the Bank Secrecy Act.
- The transaction has no business or apparent lawful purpose or is not the sort in which a particular customer would normally be expected to engage, and the Company knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction.

Filing a SAR serves as a mean to inform the regulatory authorities and law enforcement agencies of known or suspected criminal activities or patters of criminal violations perpetrated against the Company.

This form is used to report a variety of criminal activities and its use is not limited to money laundering.

All appropriate employees should be involved in identifying unusual or suspicious activities being on the alert for transactions that do not match the profile and business activities of the client. The following are the steps for reporting unusual or suspicious activities:

- Suspicious activities when detected or suspected should be reported to the employee's supervisor.
- The referral/escalation of the unusual or suspicious activity must take place in such a way to avoid "tipping off" the customer.
- If after completing more due diligence and investigation, the employee suspects that the activity is suspicious or unusual, the employee should in turn notify the AML Compliance Officer.
- The AML Compliance Officer, where warranted, will then carry out an analysis of the unusual suspicious activities.

Results of such investigation May Require the Company:

- To continue the relationship with enhanced monitoring if the customer is providing information that can be reviewed and confirmed to be authentic;
- To cancel all business relationship with the customer, if the customer refuses to provide the information requested, or if the unusual or suspicious activity continues to occur; and/or;
- To report the suspicious activity by way of filing a SAR to law enforcement and/or regulatory agencies.

The designated AML Compliance Officer is responsible for the filing of the SAR. The SAR is filed through the [www.FINCEN.gov](http://www.FINCEN.gov) website. The AML Compliance Officer is responsible for:

- a. Completing, signing, and maintaining a copy of the SAR and maintaining all the original supporting documentation;
- b. All communications pertaining to suspicious activities with the regulatory authorities;
- c. Following-up and investigating any suspicious activities reported to the President; and
- d. Advising staff members on all aspects of compliance with this reporting requirement.

**b. Red Flags**

The filing of suspicious activity will be limited to the AML Compliance Officer and his designees.

Employees will be instructed to watch for the behavior patterns that the Treasury Department summarizes as being symptomatic of money laundering situations:

- A. Unusual payment methods, such as large amounts of cash, multiple or sequentially numbered money orders, traveler's checks, or cashier's checks, or payment from third parties.
- B. Unwillingness to provide complete or accurate contact information, financial references or business affiliations.
- C. Attempts to maintain a high degree of secrecy, such as a request that normal Business records not be kept.
- D. Purchases or sales unusual for the particular customer or supplier or type of customer or supplier.
- E. Purchases or sales that do not conform to standard industry practice.

For specific examples of red flags, see Appendix III.

**c. Responding to Red Flags and Suspicious Activity**

When a member of the Company detects any red flag, he or she will report it to the AML Compliance Officer and will provide all necessary support to investigate the activity. This may include gathering additional information internally or from third-party sources. The AML Compliance Officer may choose to file a SAR. Suspicious activity and red flags, whether reported or not, will be detailed in a written report.

## **11. BSA Reporting**

### **a. Filing a SAR**

FinCEN recommends filing a SAR for any account activity (including deposits and transfers) conducted or attempted through the Company involving (or in the aggregate) \$5,000 or more offends or assets where the Company knows, suspects, or have reason to suspect:

- 1) the transaction involves funds or precious metals derived from illegal activity or is intended or conducted in order to hide or disguise funds, metals or assets derived from illegal activity as part of a plan to violate or evade federal law or regulation or to avoid any transaction reporting requirement under federal law or regulation,
- 2) the transaction is designed, whether through structuring or otherwise, to evade the requirements of the BSA 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 the Company knows, after examining the background, possible purpose of the transaction and other facts, of no reasonable explanation for the Transaction, or
- 4) the transaction involves the use of the Company to facilitate criminal activity.

The Company would not base its decision on whether to file a SAR solely on whether the transaction falls on the above set threshold. The AML Compliance Officer might file a SAR to notify law enforcement of transactions that raise an identifiable suspicion of criminal, terrorist, or corrupt activities. In high-risk situations, the Company will notify the government immediately and will file a SAR with FinCEN.

All SARs will be periodically reported to the Board of Directors and senior management, with a clear reminder of the need to maintain the confidentiality of the SAR.

All SARs will be filed no later than 30 calendar days after the date of the initial detection of the facts that constitute a basis for filing a SAR. If no suspect is identified on the date of initial detection, the Company may delay filing the SAR for an additional 30 calendar days, pending identification of a suspect, but in no case, will the reporting be delayed more than 60 calendar days after the date of initial detection.

The Company will retain copies of any SAR filed and the original or business record equivalent of any supporting documentation for five years from the date of filing the SAR. The Company will identify and maintain supporting documentation and make such information available to FinCEN, any other appropriate law enforcement agencies, or federal or state securities regulators, upon request.

The Company will not notify any person involved in the transaction that the transaction has been reported, except as permitted by the BSA regulations. The Company understands that anyone who is subpoenaed or required to disclose a SAR or the information contained in the SAR-SF, except where disclosure is requested by FinCEN or another appropriate law enforcement or regulatory agency, will decline to produce the SAR or to provide any information that would disclose that a SAR was prepared or filed. The Company will notify FinCEN of any such request and its response.

**b. Currency Transaction Reports (CTR): Form IRS FinCEN 8300**

The Company may receive payment in currency. The term "currency" means monetary instruments, such as cash in the form of U.S. and foreign currency, cashier's check, money order, bank draft or traveler's check.

**INTRODUCTION**

The Company must complete a Report of Cash Payment Over \$10,000 Received in a Trade or Business (FINCEN Form 8300) also known as CTR, anytime it receives \$10,000 or above in cash/currency in one transaction or in two or more related transactions on the same day.

**GENERAL INSTRUCTIONS**

Any CASH/currency transactions conducted between a payer and the recipient, 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 recipient knows, or has reason to know, that each transaction is one of a series of connected transactions.

The Company has no duty to file a Form 8300 on behalf of their customers when the customers are receiving currency in excess of \$10,000. The Company does have to supply the customer with the required information of the individual from whom the cash was received.

The obligation to file Form 8300 is solely on the person who receives the cash.

If the Company receives a cash payment of over \$10,000, it is required to file Form 8300 by the 15<sup>th</sup> day after the date the cash was received. If multiple payments are received for a single transaction or for related transactions, all payments must be reported any time the total amount exceeds \$10,000 within any 12-month period.

The form will be filed with the Internal Revenue Service (IRS), Detroit Computing Center, P.O. Box 32621, Detroit, MI 48232.

A written or electronic statement must be given to each person named on a required Form 8300 on or before January 31 of the year following the calendar year in which the cash is received. The statement must show the name, telephone number, and address of the information contact for the business, the aggregate amount of reportable cash received, and that the information was furnished to the IRS.

Copies of Form 8300 are required to be kept on file for 5 years from the date it was submitted.

**c. Money Transfers**

The Company's general policy is to avoid making or receiving third party money transfers.

When the Company transfers funds of \$3,000 or more, it will record on the transmittal order at least the following information:

- name,
- complete address,
- amount
- identity of the recipient's financial institution and
- the account number of the recipient.

The Company will also verify the identity of recipients who are not established customers and will check the recipient against Government lists of known and possible money launderers and terrorist financiers.

With the transmittal order, the Company will retain the letter of authority from the transmitter instructing to transfer funds.

## **12. AML Record Keeping**

### **a. SAR – Maintenance and Confidentiality.**

All SAR's and any supporting documentation are confidential. A SAR cannot be disclosed to the client or anyone outside of the Company. Additionally, employees are not permitted to advise or "tip off" any client who may be suspected of or under investigation. Generally, it should only be discussed among the Company's employees closely related to the incident.

Should a client learn or suspect that a SAR has been filed and contact an employee about the filing, or if an employee is served with a subpoena or other request for disclosure of a SAR, the employee, without admitting, confirming, or denying that a SAR was filed, should notify immediately the AML Compliance Officer. It is the Company's policy not to comment on these issues.

When requested to provide information, the Company should verify that the requestor of information is in fact a representative of FinCEN or an appropriate law enforcement or supervisory agency. These procedures may include, for example, asking the requestor to send the request in writing via e-mail so the Company can make sure that the e-mail address contains an official law enforcement agency, independent employment verification with the requestor's field office or face-to-face review of the requestor's credentials.

### **b. Company Liability for Reporting Suspicious Criminal Activities**

The "safe harbor" provision of Federal Law 31 U.S.C. 5318(g)(2) and (3) provides that Company Directors, Officers, Employees, and Agents who disclose possible violations of law or regulation, including the preparation of suspicious activity reports "shall NOT be liable to any person under any law or regulation of the United States or any constitution, law or regulation of any State for such disclosure or for any failure to notify the person involved in the transaction or any other person such disclosure". This provision applies whether the reports were filed pursuant to regulatory requirement or on a voluntary basis.

It is key thought that the Company has a good faith suspicion that a law or regulation has been violated, and that the Company has a good faith belief of the nexus between the illegal or suspicious activity and the account and/or client whose information is disclosed.

### **c. Records Required**

As part of the Company's AML program, it will create and maintain SARs, CTRs and relevant documentation on customer identity and verification and funds transfers and transmittals as well as any records related to customers listed on the OFAC list.

The Company will retain all customer identification information, SARs and their accompanying documentation for a period of five (5) years from the date the relationship with the client was established or from the date when the SAR was filed.

### **13. Training Programs**

The Bank Secrecy Act requires that all Company personnel be trained on AML/BSA requirements. Follow-up training sessions are required annually. Specific training is given if violations are detected which lack awareness or understanding of BSA requirements.

The Company will develop ongoing employee training under the leadership of the AML Compliance Officer and senior management. The Company requires all employees who have customer contact to undertake a training course upon employment and to receive refresher courses at least once a year. In addition, certain employees able to detect money laundering, such as those with compliance and corporate security responsibilities, are required to undertake similar general training.

The training can be conducted by the AML Compliance Officer or any qualified third-party consultant utilized by the company.

The Compliance Officer is required to schedule training for all existing employees no later than December 31st of the calendar year.

Management will also implement a training program for the AML Compliance Officer to assure familiarity with AML regulations. The training will include, at a minimum: how to identify red flags and signs of money laundering that arise during the course of the employees' duties; what to do once the risk is identified; employees' roles in the firm's compliance efforts and how to perform them; the firm's record retention policy; and the consequences (including civil and criminal penalties) for noncompliance with the anti-money laundering and anti-terrorist finance laws and regulations.

The training may include educational pamphlets, videos, intranet or internet courses, in person lectures, and explanatory memos. It the Company's policy to make all employees aware of money-laundering risks and the company's commitment to fight it.

The Company will maintain records enumerating the persons that have undergone training, the dates, and the subject matter of their training.

#### **14. Testing the AML Program**

The Bank Secrecy Act, OFAC and the U.S.A. Patriot Act require companies to adopt an AML program which needs to be audited for independent testing for compliance with the BSA requirements.

The Company will audit its AML program to confirm the systems and procedures established are being correctly implemented and followed, documentation is complete, records are being maintained, reports are being filed, staff is being trained and management is current on AML developments.

The testing of the AML program will be performed by an independent third-party external auditor. The third-party consultants are required to conduct an annual BSA compliance examination. If the Company decides to use an internal auditor, it will ensure that the auditor remains independent by separating the auditor's functions from other AML activities and by assigning the auditor no duties related to the administration of the AML program other than the duty to test the AML programs and systems.

The results of the examination are reported to the AML Compliance Officer and the Senior Management. BSA Audits will be conducted in accordance to a pre-approved schedule with the Company.

It is the responsibility of the AML Compliance Officer to correct all violations and deficiencies found and coordinate any additional training requirements of staff. The AML Compliance Officer is responsible for keeping Senior Management updated of any programs adopted to address BSA violations found.



### **15. Confidential Reporting of AML Non-Compliance**

Employees will report any violations of the AML compliance program to the AML Compliance Officer, unless the violations implicate the Compliance Officer in which case the employee shall report them to another senior manager. Such reports will be confidential, and the employee will suffer no retaliation for making them.


Employees may also report their concerns directly to a law enforcement agency, such as the Department of Homeland Security or the FBI. Reporting directly to a Government agency should be a last resort and should take place only if the employee is concerned that management is complicit.

**16. Senior Manager Approval**

I have approved this AML program as reasonably designed to achieve and monitor our firm's ongoing compliance with the requirements of the of the USA PATRIOT Act, the Bank Secrecy Act and other anti-money laundering and anti-terrorist finance laws and their implementing regulations.

Signed:  \_\_\_\_\_ Date: May 31st, 2021  
President: Franco Favilla

This AML Manual was designed by the Anti-Money Laundering external consultant Eduardo Solorzano, who is Certified Anti-Money Laundering Specialist (CAMS) since 2004 by the Association of Certified Anti-Money Laundering Specialists (ACAMS).

Signed:  \_\_\_\_\_ Date: May 31<sup>st</sup>, 2021

Certified Anti-Money Laundering Specialist, CAMS  
External Anti-Money Laundering Consultant

**Appendices**

**APPENDIX I: ANTI-MONEY LAUNDERING CONTACTS**

**Contact the Anti-Money Laundering Program Compliance Officer:**

The Anti-Money Laundering Program Compliance Officer is [Antoanela Chiritescu](#):

U.S. Office Phone: +1 (305) 850-4827

France Office Phone: +33 633927638

Office Fax:

Office E-Mail: [achiritescu@seasif.com](mailto:achiritescu@seasif.com)

Cell Phone:

Other anti-money laundering important contact information:

FinCEN (866) 556-3974

Department of Homeland Security Investigations (202) 282 8000

FBI (754) 703-2000

**APPENDIX II: GRAMM-LEACH-BLILEY ACT-SECTION 501-a**

TITLE V-PRIVACY

SUBTITLE A-Disclosure of Nonpublic Personal Information

(a) **PRIVACY OBLIGATION POLICY.** – It is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information.

(b). **FINANCIAL INSTITUTIONS SAFEGUARDS.** - In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical and physical safeguards-

- (1) To insure the security and confidentiality of customer records and information;
- (2) To protect against any anticipated threats or hazards to the security or integrity of such records; and
- (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

### **APPENDIX III: RED FLAGS**

Red flags that signal possible money laundering or terrorist financing include, but are not limited to:

- The customer exhibits unusual concern about the firm's compliance with government reporting requirements and the firm's AML policies (particularly concerning his or her identity, type of business and assets), or is reluctant or refuses to reveal any information concerning business activities, or furnishes unusual or suspicious identification or business documents.
- The customer wishes to engage in transactions that lack business sense or apparent investment strategy, or are inconsistent with the customer's stated business or investment strategy.
- The information provided by the customer that identifies a legitimate source for funds is false, misleading, or substantially incorrect.
- Upon request, the customer refuses to identify or fails to indicate any legitimate source for his or her funds and other assets.
- The customer (or a person publicly associated with the customer) has a questionable background or is the subject of news reports indicating possible criminal, civil, or regulatory violations.
- The customer exhibits a lack of concern regarding risks, commissions, or other transaction costs.
- The customer appears to be acting as an agent for an undisclosed principal, but declines or is reluctant, without legitimate commercial reasons, to provide information or is otherwise evasive regarding that person or entity.
- The customer has difficulty describing the nature of his or her business or lacks general knowledge of his or her industry.
- The customer attempts to make frequent or large deposits of currency, insists on dealing only in cash, or asks for exemptions from the firm's policies relating to the deposit of cash.
- The customer engages in transactions involving cash or cash equivalents or other monetary instruments that appear to be structured to avoid the \$10,000 government reporting requirements, especially if the cash or monetary instruments are in an amount just below reporting or recording thresholds.
- For no apparent reason, the customer has multiple accounts under a single name or multiple names, with many inter-account or third-party transfers.
- The customer is from, or has accounts in, a country identified as a non-cooperative country or territory by the FATF.
- The customer's account has unexplained or sudden extensive wire activity, especially in accounts that had little or no previous activity.

- The customer's account shows numerous currencies or cashier's check transactions aggregating to significant sums.
- The customer's account has many wire transfers to unrelated third parties inconsistent with the customer's legitimate business purpose.
- The customer's account has wire transfers that have no apparent business purpose to or from a country identified as a money laundering risk or a bank secrecy haven.
- The customer's account indicates large or frequent wire transfers, immediately withdrawn by check or debit card without any apparent business purpose.
- The customer makes a funds deposit followed by an immediate request that the money be wired out or transferred to a third party, or to another firm, without any apparent business purpose.
- The customer makes a funds deposit for purchasing a long-term investment followed shortly thereafter by a request to liquidate the position and transfer of the proceeds out of the account.
- The customer engages in excessive journal entries between unrelated accounts without any apparent business purpose.
- The customer requests that a transaction be processed to avoid the firm's normal documentation requirements.
- The customer maintains multiple accounts or maintains accounts in the names of family members or corporate entities, for no apparent purpose.
- The customer's account has inflows of funds or other assets well beyond the known income or resources of the customer.

**APPENDIX IV: Notice to Customers**

**AML CERTIFICATION**

To help the government fight money-laundering and the funding of terrorism, Federal law requires all dealers in precious metals to verify that their counterparts either have anti-money laundering programs or are exempt. Please complete and return the form below on your company's letterhead.

This is to certify that ( \_\_\_\_\_ )  
Company Name

( ) Has a written risk assessment and an anti-money laundering plan of compliance and supervisory procedures that complies with the USA PATRIOT Act, Bank Secrecy Act and other legislation and regulations to prevent money laundering and terrorist finance. Our anti-money laundering program provides for staff training and for periodic Anti- money laundering systems testing to confirm the efficacy of the anti-money laundering program and its systems.

**OR**

( ) Is exempt from coverage under the Act under the "retail," "industrial" or other exemption specified in the Interim Final Rule for Dealers in Precious Metals, Stones or Jewels or pursuant to an administrative exemption granted by the Financial Crimes Enforcement Network (FinCEN), or is a non-US entity that is compliant with its local AML requirements.

Signed \_\_\_\_\_

Name: \_\_\_\_\_

Officer/Title: \_\_\_\_\_

Date: \_\_\_\_\_

**APPENDIX V:**

***SUPPLY CHAIN POLICY FOR A RESPONSIBLE GLOBAL SUPPLY CHAIN OF MINERAL FROM CONFLICT AFFECTED AND HIGH-RISK AREAS***

The Company recognizes that risks of significant adverse impacts may be associated with extracting, trading, handling, and exporting minerals from conflict-affected and high-risk areas and recognize that it has the responsibility to respect human rights and not to contribute to conflict. The Company commits to adopt, widely disseminate, and incorporate in contracts and/or agreements with suppliers the following policy on responsible sourcing of minerals from conflict-sensitives sourcing practices and suppliers' risk awareness from the point of extraction until end user. The Company commits to refrain from any action which contributes to the financing of conflict and will comply with relevant United Nations sanctions resolutions or, where applicable, domestic laws implementing such resolutions.

**REGARDING SERIOUS ABUSES ASSOCIATED WITH THE EXTRACTION, TRANSPORT OR TRADE OF MINERALS**

1. While sourcing from, or operating in, conflict-affected and high-risk areas, we will neither tolerate nor by any means profit from, contribute to, assist with or facilitate the commission by any party of:

- a. Any forms of torture, cruel, inhuman and degrading treatment;
- b. Any forms of forced or compulsory labor, which means work or service which is exacted from any person under the menace of penalty and for which said person has not offered himself voluntarily;
- c. The worst forms of child labor;
- d. Other gross human rights violations and abuses such as widespread sexual violence;
- e. War crimes or other serious violations of international humanitarian law, crimes against humanity or genocide.

**REGARDING RISK MANAGEMENT OF SERIOUS ABUSES**

2. We will immediately suspend or discontinue engagement with upstream suppliers where we identify a reasonable risk that they are sourcing from, or linked to, any party committing serious abuses as defined in paragraph 1.

**REGARDING DIRECT OR INDIRECT SUPPORT TO NON-STATE ARMED GROUPS**

3. We will not tolerate any direct or indirect support to non-state armed groups through the extraction, transport, trade, handling or export of minerals. "Direct or indirect support" to non-state armed groups through the extraction, transport, trade, handling or export of minerals include, but is not limited to, procuring minerals from, making payments to or otherwise providing logistical assistance or equipment to, non-state armed groups or their affiliates who ("Affiliates" include middlemen, consolidators, intermediaries, and others in the supply chain that work directly with armed groups to facilitate extraction, trade, or handling of minerals):



- a. Illegally control mine sites or otherwise control transportation routes, points where minerals are traded and upstream actors in the supply chain (“Control” of mines, transportation routes, points where minerals are traded and upstream actors in the supply chain means: i) overseeing extraction, including grating access to mine sites and/or coordinating downstream sales to intermediaries, export companies or international traders; ii) making recourse to any forms of forced or compulsory labor to mine, transport, trade or sell minerals; or iii) acting as a director or officer of, or holding beneficial or other ownership interest in, upstream companies or mines.
- b. Illegally tax or extort money or minerals at points of access to mine site (“Extort” from mines, transportation routes, points where minerals are traded or upstream companies means the demanding, under the threat of violence or any other penalty, and for which the person has not voluntarily offered, sums of money or minerals, often in return for granting access to exploit the mine site, access transportation routes, or to transport, purchase, or sell minerals.

#### **REGARDING RISK MANAGEMENT OF DIRECT OR INDIRECT SUPPORT TO NON-STATE ARMED GROUPS**

4. We will immediately suspend or discontinue engagement with upstream suppliers where we identify a reasonable risk that they are sourcing from, or linked to, any party providing direct or indirect support to non-state armed groups as defined in paragraph 3.

#### **REGARDING PUBLIC OR PRIVATE SECURITY FORCES**

5. We agree to eliminate, in accordance with paragraph 10, direct or indirect support to public or private security forces who illegally control mine sites, transportation routes and upstream actors in the supply chain; illegally tax or extort money or minerals at point of access to mine sites, along transportation routes or at points where minerals are traded; or illegally tax or extort intermediaries, export companies or international traders.

6. We recognize that the role of public or private security forces at the mine sites and/or surrounding areas and/or along transportation routes should be solely to maintain the rule of law, including safeguarding human rights, providing security to mine workers, equipment and facilities, and protecting the mine site or transportation routes from interference with legitimate extraction and trade.

7. Where we or any company in our supply chain contract public or private security forces, we commit to or we will require that such security forces will be engaged in accordance with the Voluntary Principles on Security and Human Rights. In particular, we will support or take steps, too adopt screening policies to ensure that individuals or units of security forces that are known to have been responsible for gross human rights abuses will not be hired.

8. We will support efforts, or take steps, to engage with central or local authorities, international organizations and civil society organizations to contribute to workable solutions on how transparency, proportionality and accountability in payments made to public security forces for the provision of security could be improved.

9. We will support efforts, or take steps, to engage with local authorities, international organizations and civil society organizations to avoid or minimize the exposure of vulnerable groups, in particular, artisanal miners where minerals in the supply chain are extracted through artisanal or small-scale mining, to adverse impacts associated with the presence of security forces, public or private, on mine sites.

**REGARDING RISK MANAGEMENT OF PUBLIC OR PRIVATE FORCES**

10. In accordance with the specific position of the company in the supply chain, we will immediately devise, adopt and implement a risk management plan with upstream suppliers and other stakeholders to prevent or mitigate the risk of direct or indirect support to public or private security forces, as identified in paragraph 5, where we identify that such a reasonable risk exists. In such cases, we will suspend or discontinue engagement with upstream suppliers after failed attempts at mitigation within six months from the adoption of the risk management plan. Where we identify a reasonable risk of activities inconsistent with paragraphs 8 and 9, we will respond in the same vein.

**REGARDING BRIBERY AND FRAUDULENT MISREPRESENTATION OF THE ORIGIN OF MINERALS**

11. We will not offer, promise, give or demand any bribes, and will resist the solicitation of bribes to conceal or disguise the origin of minerals, to misrepresent taxes, fees and royalties paid to governments for the purposes of mineral extraction, trade, handling, transport and export.

**REGARDING MONEY LAUNDERING**

12. We will support efforts, or take steps, to contribute to the effective mitigation of money laundering where we identify a reasonable risk of money-laundering resulting from, or connected to, the extraction, trade, handling, transport or export of minerals derived from the illegal taxation or extortion of minerals at points of access to mine sites, along transportation routes or at points where minerals are traded by upstream suppliers.

**REGARDING THE PAYMENT OF TAXES, FEES, AND ROYALTIES DUE TO GOVERNMENTS**

13. We will ensure, to the best of our efforts, that all taxes, fees, and royalties related to mineral extraction, trade, and export from conflict-affected and high-risk areas are paid to governments and, in accordance with the company's position in the supply chain, we commit to disclose such payments in accordance with the principles set forth under the Extractive Industry Transparency Initiative (EITI).

**REGARDING RISK MANAGEMENT OF BRIBERY AND FRAUDULENT MISREPRESENTATION OF THE ORIGIN OF MINERALS, MONEY-LAUNDERING AND PAYMENT OF TAXES, FEES, AND ROYALTIES TO GOVERNMENTS**

14. In accordance with the specific position of the company in the supply chain, we commit to engage with suppliers, central or local government authorities, international organizations, civil society, and affected third parties, as appropriate, to improve and track performance with a view to preventing or mitigating risks of adverse impacts through measurable steps taken in reasonable timescales. We will suspend or discontinue engagement with upstream suppliers after failed attempts at mitigation.

**APPENDIX VI:**

***SITE VISITS TO KEY CUSTOMERS IN DOMESTIC AND INTERNATIONAL HIGH-RISK GEOGRAPHIES (HRG)***

The Company will perform the following activities regarding key customers in High Risk areas.

**Frequent Site Visits**

Frequent site visit should be programmed to countries in which the Company sources a significant amount of material. This site visits should be done as frequent as possible but no less than once a year and shall include creating a network with the country government, banking institutions, and other stakeholders directly related to the industry.

**Ordinary visits and control visits to customers/suppliers.**

As a result of the physical inspections conducted by the company to customers/ suppliers, the following information must be recorded in a certificate:

- Name or corporate name.
- City, time and date of the visit.
- Manager or legal Representative's name.
- Name of the person hosting the visit.
- Control Entity.
- Main Partners or shareholder.
- Business sensitivity.
- Overview of the company.
- Photographic record.
- Signature of the certificate by the parties that attended the visit.

The visits described in this procedure must be conducted at least every year for customers or suppliers deemed high risk. These visits must also be conducted when there are inconsistencies in transactions more in the documents provided by the customer or supplier.

The Company considers high risk the following categories of customers and suppliers:

- Those who because of the economic activity they conduct generate the risk itself.
- Those who because of their sole jurisdiction where they are located generate the risk itself.
- Those with whom the company establishes business relations sporadically.
- Politically exposed people.
- Natural Persons.
- Other customers and suppliers that the compliance officer, the president and the board of directors decide.

## **APPENDIX VII: ANTI-BRIBERY POLICY**

The Company is committed to conducting its business ethically and in compliance with all applicable laws and regulations, including the U.S. Foreign Corrupt Practices Act (FCPA) and other laws (including those of the countries in which the Company operates) that prohibit improper payments to obtain a business advantage. This document describes the Company Policy prohibiting bribery and other improper payments, business operations and employee responsibilities for ensuring implementation of the Policy. Questions about the Policy or its applicability to particular circumstances should be directed to the Company Compliance Committee or through the whistle blower program.

### **Policy Overview**

The Company strictly prohibits bribery or other improper payments in any of its business operations. This prohibition applies to all business activities, anywhere in the world, whether they involve government officials or are wholly commercial. A bribe or other improper payment to secure a business advantage is never acceptable and can expose individuals and the Company to possible criminal prosecution, reputational harm, or other serious consequences.

This Policy applies to everyone at the Company, including all officers, employees, and agents or other intermediaries acting on the Company's behalf. Each officer and employee of the Company has a personal responsibility and obligation to conduct the Company business activities ethically and in compliance with the law. Failure to do so may result in disciplinary action, up to and including dismissal. Improper payments prohibited by this policy include bribes, kickbacks, excessive gifts or entertainment, or any other payment made or offered to obtain an undue business advantage. These payments should not be confused with reasonable and limited expenditures for gifts, business entertainment and other legitimate activities directly related to the conduct of the Company business. The Company has developed a comprehensive program for implementing this Policy, through appropriate guidance, training, investigation, and oversight. The assigned Compliance Officer for the Company has overall responsibility for the program, supported by the ownership of the Company and the Company Compliance Committee is responsible for giving advice on the interpretation and application of this policy, supporting training and education, and responding to reported concerns.

### **Compliance with U.S. Foreign Corrupt Practices Act**

The prohibition on bribery and other improper payments applies to all business activities but is particularly important when dealing with government officials. The U.S. Foreign Corrupt Practices Act and similar laws in other countries strictly prohibit improper payments to gain a business advantage and impose severe penalties for violations. The following summary is intended to provide personnel engaged in international activities a basic familiarity with applicable rules so that inadvertent violations can be avoided, and potential issues recognized in time to be properly addressed.

### **Overview of the FCPA**

The FCPA is a criminal statute that prohibits improper payments to government officials to influence performance of their official duties. It makes it unlawful for any U.S. company and its employees or agents to offer, promise, pay or authorize the payment of "anything of value" to any "foreign official" – a term that is very broadly defined – to help the company obtain or keep business or secure some other

“improper business advantage.” This prohibition applies whether the offer or payment is made directly or through another person.

In addition to prohibiting improper payments to foreign officials, the FCPA requires U.S. companies and their controlled affiliates to keep accurate books and records of the transactions in which they engage and to maintain a system of internal controls that, among other things, can prevent “slush funds” and “off-the-books” accounts that might be used to facilitate or conceal questionable foreign payments. FCPA accounting requirements apply to all business activities, not just those involving foreign officials.

The penalties for violating the FCPA are severe. For a company, potential sanctions range from multi-million-dollar fines and “disgorgement” of any business profits from an improper payment to loss of export privileges or eligibility to compete for U.S. government contracts. These sanctions are in addition to potential reputational damage and investigation and defense costs, which may arise even without a formal government prosecution. The penalties for individuals can be even more severe, including substantial fines and imprisonment.

## **COMMON QUESTIONS ABOUT THE FCPA**

### **When does the FCPA bribery prohibition apply?**

The FCPA prohibition applies to improper payments made by a “U.S. person” anywhere in the world, whether or not there is any other connection to the United States. The term U.S. person includes both U.S. companies and individuals who are citizens or permanent residents of the United States. Foreign nationals also may be prosecuted for causing, directly or through a third person, any act in the U.S. in furtherance of a corrupt payment.

### **What does the FCPA prohibit?**

The FCPA makes it unlawful to bribe a foreign official to gain an “improper business advantage.” An improper business advantage may involve efforts to obtain or retain business, as in the awarding of a government contract, but also can involve regulatory actions such as licensing or approvals. Examples of prohibited regulatory bribery include paying a foreign official to ignore an applicable customs requirement or to accelerate a tax refund.

The FCPA bribery prohibition has been interpreted very broadly. A violation can occur even if an improper payment is only offered or promised and not actually made, it is made but fails to achieve the desired result, or the result benefits someone other than the giver (for example, directing business to a third party). Also, it does not matter that the foreign official may have suggested or demanded the bribe, or that a company feels that it is already entitled to the government action. While certain limited exceptions may apply (described below), these should never be relied upon without first seeking expert guidance.

### **Who is a “foreign official”?**

A “foreign official” under the FCPA can be essentially anyone who exercises governmental authority. This includes any officer or employee of a foreign government department or agency, whether in the executive, legislative or judicial branch of government, and whether at the national, state, or local level. Officials and employees of government-owned or controlled enterprises also are covered, as are private

citizens who act in an official governmental capacity. The FCPA prohibition also applies to political parties and candidates, and to officials of public international organizations such as the United Nations.

#### **What types of payments are prohibited?**

The FCPA prohibits offering, promising or giving “anything of value” to a foreign official to gain an improper business advantage. In addition to cash payments, “anything of value” may include:

- Gifts, entertainment or other business promotional activities;
- Covering or reimbursing an official’s expenses;
- Offers of employment or other benefits to a family member or friend of a foreign official;
- Political party and candidate contributions;
- Charitable contributions and sponsorships.

Other less obvious items provided to a foreign official can also violate the FCPA. Examples include in-kind contributions, investment opportunities, stock options or positions in joint ventures, and favorable or steered subcontracts. The prohibition applies whether an item would benefit the official directly or another person, such as a family member, friend or business associate.

#### **Are there any exceptions?**

The FCPA does not prohibit reasonable promotional or other business activities, including legitimate charitable contributions or sponsorships. Special care is required, however, when foreign officials may be involved to avoid any appearance that benefits are being offered to improperly influence the performance of official duties.

The FCPA also contains a limited exception for payments expressly authorized under the host country’s written law. This is a very narrow exception, however, requiring prior approval by Compliance Committee.

Finally, in certain limited circumstances, a payment to a foreign official may qualify under a narrow FCPA exception for “facilitating” payments made to secure “routine government action.” Examples of routine action recognized under the FCPA include:

- Obtaining permits, licenses or other official documents that qualify a person to do business in a foreign country;
- Processing governmental papers such as visas;
- Providing police protection or mail service;
- Scheduling inspections associated with contract performance or shipment of goods;
- Providing phone, power or water service;
- Loading or unloading cargo, or protecting perishable products or commodities from deterioration;
- Other similar actions that are ordinarily and commonly performed by an official.

Payments under this exception may only be made to expedite actions to which the company is already entitled and may not involve discretionary action by the foreign official. Facilitation payments may never be used to win or retain business or to influence discretionary decisions regarding compliance with building codes, environmental, health and safety rules or other regulatory requirements. Moreover, even if a payment falls within the FCPA exception it may still violate local law in the host country or

counterpart laws in other countries prohibiting foreign bribery that may not exempt facilitation payments.

Because facilitation payments can raise significant legal and business issues, reliance on this narrow exemption from FCPA liability is strongly discouraged and may not be undertaken without prior written approval of Compliance Committee. Further, all facilitation payments remain subject to FCPA accounting and recordkeeping requirements and must be properly described in company records.

### **Business Promotion**

Gifts, business entertainment and other legitimate promotional activities involving foreign officials may be permissible under the FCPA in certain limited circumstances. For example, the Act does not prohibit modest gifts at holidays, company logo gifts and routine business meals. To comply with the FCPA, such expenditures must be reasonable in cost, related to a legitimate business promotional activity or performance of an existing contract, and otherwise consistent with the Company business practices. Prior approval for such specific expenses shall be reviewed by the Compliance Committee.

### **Can the Company be held responsible for improper payments by third parties?**

Yes. The FCPA applies whether a bribe is made directly or through an agent, consultant or other intermediary. Under the law, the Company and individual officials or employees may be held liable for improper payments by an agent or other intermediary if there is actual knowledge or reason to know that a bribe will be paid. Willful ignorance – which includes not making reasonable inquiry when there are suspicious circumstances – is not a defense, and it also does not matter whether the intermediary is itself subject to the FCPA. All employees therefore must be alert to potential “red flags” in transactions with third parties.

### **Are there special accounting and recordkeeping requirements?**

Under the FCPA, the Company and its affiliates must keep accurate books and records that reflect transactions and asset dispositions in reasonable detail, supported by a proper system of internal accounting controls. These requirements are implemented through the Company standard accounting rules and procedures, which all personnel are required to follow without exception.

Special care must be exercised when transactions may involve payments to foreign officials. Off-the-books accounts should never be used. Facilitation or other payments to foreign officials should be promptly reported and properly recorded, with respect to purpose, amount and other relevant factors. Requests for false invoices or payment of expenses that are unusual, excessive or inadequately described must be rejected and promptly reported. Misleading, incomplete or false entries in the Company books and records are never acceptable.

### **Facilitation Payments**

Except under extreme or emergency circumstances, prior written approval is required for all facilitation payments. If prior approval is not possible because of concerns about safety or safe passage, the payment should be made and then clearly documented and reported to the Compliance Committee and Compliance Officer as soon as possible.

### **Do other countries have similar anti-bribery laws?**

Yes. Many countries now have similar laws to the U.S. FCPA that prohibit bribery of foreign officials by their citizens and companies, which can include local subsidiaries and affiliates of a foreign-based company. These laws are comparable to the FCPA but can differ in important aspects – such as the treatment of facilitation payments. In addition, virtually all countries have domestic laws that prohibit bribery of their public officials.

The Company requires all employees and agents to comply totally with applicable foreign laws and regulations. The laws that apply to specific international business activities include those of the country in which the activities occur, as well as others that (like the U.S. FCPA) govern the international operations of national companies and citizens. Employees involved in international operations should consult with counsel to ensure that they are aware of, and are complying with, applicable laws.

### **Working with Agents and Other Third Parties**

The Company from time to time may engage the services of an agent, consultant or other intermediary to support its business activities, or may participate with business partners in a joint venture or other business structure. These relationships are important to the Company and provide valuable contributions in many areas of business but can also pose compliance challenges and thus require appropriate measures to prevent bribery.

This Policy applies in all material aspects to business conducted with or through an agent, consultant, joint venture or other business partner. Employees who manage, supervise and/or oversee the activities of third parties working with the Company are responsible for ensuring that such persons or entities understand and fully comply with this Policy, through appropriate measures. Measures appropriate to a particular relationship or transaction may vary and should be identified pursuant to established guidelines, in consultation with the Compliance Committee.

Personnel working with agents and other third parties should pay particular attention to unusual or suspicious circumstances that may indicate possible legal or ethics concerns, commonly referred to as “red flags.” The presence of red flags in a relationship or transaction requires greater scrutiny and implementation of safeguards to prevent and detect improper conduct. Appointment of an agent or other third party ordinarily requires prior approval by an appropriate senior manager, description of the nature and scope of services provided in a written contract, and appropriate contractual safeguards against potential violations of law or the Company policy.

### **Third Party Checks**

The Company has established detailed standards and procedures for the selection, appointment and monitoring of agents, consultants and other third parties. These standards and procedures must be followed in all cases, with particular attention to “red flags” that may indicate possible legal or ethical violations. Due diligence ordinarily will include appropriate reference and background checks, written contract provisions that confirm a business partner’s responsibilities, and appropriate monitoring controls.

### **Employee Responsibilities**





This Policy imposes on all personnel specific responsibilities and obligations that will be enforced through standard disciplinary measures and properly reflected in personnel evaluations.

All officers, employees and agents are responsible for understanding and complying with the Policy, as it relates to their jobs. Every employee has an obligation to:

- Be familiar with applicable aspects of the Policy and communicate them to subordinates;
- Ask questions if the Policy or action required to take in a particular situation is unclear;
- Properly manage and monitor business activities conducted through third-parties;
- Be alert to indications or evidence of possible wrongdoing; and
- Promptly report violations or suspected violations through appropriate channels.

The Company's managers have a particular responsibility to ensure that subordinates, including agents, receive proper training, and to monitor for compliance with the Policy.

### **Common Red Flags**

Red flags that warrant further investigation when selecting or working with an agent, consultant or other third party vary from case to case. Common examples to watch for include:

- Transactions involving a country or sector known for corrupt payments;
- Background checks that raise questions about a third party's reputation, qualifications or trustworthiness;
- A third party suggested or recommended by a foreign official;
- Family or other relationships that could improperly influence the decision of a customer or government official;
- Compensation arrangements that are disproportionate, non-transparent or otherwise unusual;
- A third party who objects to FCPA representations and warranties or other elements of this policy.

### **Reporting Possible Violations**

Any employee who has reason to believe that a violation of this Policy has occurred, or may occur, must promptly report this information to his or her supervisor, the next level of supervision, or the Compliance Committee. Alternatively, information may be reported in confidence to the Company's hotline. Retaliation in any form against an employee who has, in good faith, reported a violation or possible violation of this Policy is strictly prohibited.

Employees who violate this Policy will be subject to disciplinary action, up to and including dismissal. Violations can also result in prosecution by law enforcement authorities and serious criminal and civil penalties.

**APPENDIX VIII:**

**The Anti-Money Laundering Act of 2020**  
(Executive Summary)

**OVERVIEW**

The Anti-Money Laundering Act of 2020 was enacted as part of the National Defense Authorization Act for Fiscal Year 2020 (the NDAA) and includes the most substantial changes to U.S. anti-money laundering law (AML) since the USA PATRIOT Act of 2001.

While the new law clarifies and streamlines certain Bank Secrecy Act (BSA) and AML obligations, it also imposes new regulatory requirements such as requiring financial institutions to integrate a set of National AML / Countering the Financing of Terrorism (CFT) Priorities into their compliance programs.

The AML Act ushers in the most significant changes to the Bank Secrecy Act of 1970, as amended (BSA) and other anti-money laundering/countering terrorism financing (AML/CFT) laws since the USA PATRIOT Act of 2001. The purpose of the AML Act is to:

- establish a uniform beneficial ownership information reporting regime that includes reporting requirements for certain U.S. corporations and limited liability companies designed to combat money laundering through shell companies;
- increase AML whistleblower awards and expand whistleblower protections;
- codify the risk-based approach to AML/CFT compliance;
- modernize the statutory definition of “financial institution” to include, consistent with existing Financial Crimes Enforcement Network (FinCEN) regulations, entities that provide services involving “**value that substitutes for currency**” –a category that includes stored value and virtual currency instruments;
- streamline and modernize BSA and AML requirements, regulations and systems;
- greatly expand enforcement and investigation-related authority including an expansion of the duties, powers, and functions of the U.S. Department of the Treasury’s Financial Crimes Enforcement Network (FinCEN) and the authority of U.S. courts to **subpoena foreign banks** that maintain correspondent accounts with U.S. banks; and
- align supervision and examination priorities by emphasizing coordination, cooperation, and information-sharing among financial institutions, U.S. financial regulators and foreign financial regulators.

The AML Act, and the changes to the existing BSA regime it represents, are the result of years of efforts by U.S. legislators, regulators, and the financial industry to reform the BSA legal framework and address longstanding concerns raised by the public and private sectors. The long-term effect of these comprehensive changes set by the AML Act will move the United States closer to a global regime of fighting financial crimes, as opposed to the current U.S.-centric legal framework.

### **Who is covered by the Act?**

The Anti-Money Laundering Act of 2020 impacts various types of entities and many of its provisions are applicable to “financial institutions” as broadly defined in the Bank Secrecy Act (31 U.S.C § 5312), including those engaged in the following businesses:

- Banks, thrifts, credit unions and any other insured depository institutions
- Branches and agencies of foreign banks
- Broker-dealers of securities
- Money services businesses, including money transmitters, issuers of checks, money orders or “similar instruments,” and foreign exchange dealers
- Nonbank lending companies
- Insurance companies
- Operators of credit card systems
- Mutual funds
- Futures commission merchants
- Travel agencies
- Casinos with revenues over \$1,000,000
- Pawnbrokers
- **Dealers in precious metals, stones or jewels**
- Other businesses or agencies designated by the Secretary of the Treasury to be an activity similar to a financial institution or whose cash transactions have a high degree of usefulness in criminal, tax, or regulatory matters.

### Entities Added to the Definition of “Financial Institutions”

The Anti-Money Laundering Act of 2020 amends the **Bank Secrecy Act’s** definition of “**Financial Institutions:**”

- Clarifies that a financial institution includes any person or business who “engages in as a business the transmission of currency, funds, or **value that substitutes for currency.**”
- Adds any person “engaged in the **trade of antiquities**, including an advisor, consultant, or any other person” who deals in the “**sale of antiquities.**”

### **BENEFICIAL OWNERSHIP REGISTRY**

The Anti-Money Laundering Act of 2020 includes the Corporate Transparency Act (CTA), which is intended to discourage the use of shell corporations to disguise and move illicit funds.

- The Corporate Transparency Act requires certain U.S. entities and entities doing business in the U.S. to report beneficial ownership information to FinCEN.
- Reporting Companies must provide information for each Beneficial Owner, including:
  - ✓ Full legal name
  - ✓ Date of birth

- ✓ Current residential or business address
- ✓ The Unique Identifying Number of an acceptable identification document (e.g., passport, driver's license)
- FinCEN will maintain a national registry of beneficial ownership information, which will not be public.
  - ✓ Federal, state, and tribal law enforcement agencies may obtain beneficial ownership information pursuant to a court order.
  - ✓ Financial institutions will be able to access the information with their customer's permission.

#### **Corporate Transparency Act v. Customer Due Diligence (CDD) Rule**

- The Corporate Transparency Act includes many requirements like those in FinCEN's CDD Rule; however, the requirements are imposed on reporting companies, not covered financial institutions.
- FinCEN is directed to rescind provisions of the existing CDD Rule that overlap with the Corporate Transparency Act's beneficial ownership requirements.
- FinCEN is specifically prohibited from rescinding the requirement to maintain procedures to identify legal entity customers' beneficial owners.

#### **Applicability of New Beneficial Ownership Requirements**

- The new beneficial ownership requirements are intended to capture ownership information about shell companies.
- The requirements are limited to Beneficial Owners of Reporting Companies with a few exceptions.
- A Reporting Company includes:
  - ✓ an entity created under the laws of the United States or Indian Tribe; or
  - ✓ a foreign entity registered to do business in the United States.
- A Beneficial Owner is any entity or individual who (directly or indirectly):
  - ✓ exercises substantial control over the entity; or
  - ✓ owns or controls 25% or more of the entity's ownership interest.
- The Beneficial Owner definition excludes several categories of entities and individuals, including:
  - ✓ Creditors of the entity unless the creditor otherwise holds 25% or more ownership interest or substantial control;
  - ✓ Certain individuals acting as custodians or agents for an individual or acting solely as an employee of the entity.
- The Corporate Transparency Act does not define "substantial control" and delegates authority to FinCEN to define the term.

Excluded from the Reporting Company Definition

- Publicly traded companies
- Certain non-profits and government entities
- Certain Financial Institutions: banks, credit unions, bank holding companies, savings & loan holding companies, money transmitting businesses, broker-dealers, exchanges or clearing agencies, insurance companies, commodities and futures dealers, public accounting firms, designated financial market utilities, and pooled investment vehicles
- Other entities that meet the following conditions:
  - ✓ Employ more than 20 full-time employees;
  - ✓ Filed a federal income tax return with more than \$5 million in sales or gross receipts; and
  - ✓ Maintain an operating presence in a physical office within the United States.

Implementation of New Beneficial Ownership Requirements

- The Corporate Transparency Act provides an extended timeframe for compliance with the new beneficial ownership reporting requirements.
- Existing entities are not required to report beneficial ownership requirements until 2 years after the effective date of the regulations promulgated under this law, which will likely take at least 18 months.
- Reporting Companies are subject to ongoing obligations to report updated changes in beneficial ownership information no later than 1 year after the date of the change.

Effective Date

- Existing Entities
  - ✓ Reporting Companies formed or registered before the effective date of the promulgated regulations must report beneficial ownership information within 2 years of the effective date of the regulations.
- Newly Formed Entities
  - ✓ Reporting Companies formed after the effective date of the promulgated regulations must report beneficial ownership information at the time of formation.

## **UPDATED AML WHISTLEBLOWER INCENTIVES**

### **Expanded AML Whistleblower Incentives**

- The Anti-Money Laundering Act expands the whistleblower awards that result in monetary sanctions of more than \$1 million.
- Eligible whistleblowers may receive up to 30% of the collected monetary sanction imposed in the action.

### **New AML Whistleblower Protections**

- The Anti-Money Laundering Act also includes new provisions to protect eligible AML whistleblowers from employer retaliation, including discharge, demotion, blacklisting, and harassment.
- Whistleblowers subject to retaliation may file a complaint with the U.S. Secretary of Labor.
- Prevailing whistleblowers are eligible for relief, including:
  - ✓ Reinstatement with the same seniority status;
  - ✓ Compensatory damages (including litigation expenses);
  - ✓ Two times the amount of back pay otherwise owed to the individual (with interest); and
  - ✓ Any other appropriate remedy with respect to the conduct that is subject to the complaint or action.

## **ENHANCED ANTI-MONEY LAUNDERING PENALTIES**

### **Additional Civil Monetary Damages for Repeat AML Violations**

- The Secretary of the Treasury may impose additional civil monetary penalties for certain repeat violators of AML laws, including three times the profit gained or loss avoided as a result of the violation or two times the maximum penalty for the violation.

### **Claw Back of Certain Bonuses for AML Convictions**

- Certain partners, directors, officers, or employees of financial institutions convicted of violating the BSA are required to repay any bonus paid to that individual during the calendar year during which or after the violation occurred.

### **Report to Congress on AML Deferred Prosecution Agreements and Non-Prosecution Agreements**

- The Department of Justice is required to provide an annual report to Congress for the next five years, which includes a list of deferred prosecution agreements and non-prosecution agreements during the covered year with respect to a violation or suspected violation of the BSA as well as a justification for such actions.

### **Prohibition of Certain AML Violators from Serving on Boards of U.S. Financial Institutions**

- Any individual found to have committed an “egregious violation” of the BSA is barred from serving on the board of directors of a U.S. financial institution for 10 years from the date of conviction or judgment.

### **OTHER CHANGES TO BSA/AML REQUIREMENTS**

The Act includes a number of provisions that will alter the landscape for financial institutions implementing BSA/AML programs. Key among these changes are requirements that FinCEN provide financial institutions with information about financial crime concerns and patterns. Within six months, the U.S. Department of Treasury (“Treasury”) must establish national AML priorities, to be updated at least once every four years. Federal regulators will subsequently review whether and to what extent financial institutions have incorporated the national AML priorities into their risk-based programs to comply with BSA requirements.

The Act also requires FinCEN, “to the extent practicable,” to periodically disclose to “each financial institution” a summary of information on SARs that “proved useful” to law enforcement. The Act does not require financial institutions to respond to FinCEN’s disclosures, but financial institutions that receive negative feedback or no positive feedback may wish to consider whether they are meeting regulatory expectations.

FinCEN also must publish information relating to emerging money laundering and terrorist financing threat patterns and trends. FinCEN must include typologies, “including data that can be adapted in algorithms if appropriate,” suggesting that financial institutions will be evaluated on whether and to what extent they have incorporated FinCEN’s published threat patterns and trends into the financial institutions’ BSA/AML programs and SAR reporting processes.

The Act addresses de-risking, which is the practice of cutting off financial services to underserved individuals, entities, and geographic areas when BSA/AML risks are difficult or expensive to manage. The Act states that BSA/AML policies “must not unduly hinder or delay legitimate access to the international financial system,” and that federal enforcement efforts should not primarily focus on BSA/AML policies that result in “incidental, inadvertent benefits” to designated groups in the course of delivering “life-saving aid to civilian populations.” The Office of the Comptroller of the Currency and FinCEN are required to study and report on de-risking, and to propose changes, as appropriate, to reduce any unnecessarily burdensome regulatory requirements.

A financial institution implementing a BSA/AML program will need to be able to demonstrate to its regulators that the financial institution has incorporated into its BSA/AML processes the information FinCEN provides about national AML priorities and other risk areas.

A statement that U.S. enforcement efforts are not focused on de-risking may cause financial institutions to maintain some lines of higher-risk business. However, the Act does not require financial institutions to maintain higher-risk business; if the cost of compliance outweighs the profit from the business, financial institutions may continue de-risking certain business lines.