



ANTI-MONEY LAUNDERING POLICIES AND PROCEDURES

DECEMBER 2023

VERITY ASSET MANAGEMENT, Inc.

AML Program

Introduction

In the wake of the attacks of September 11, 2001, the USA PATRIOT Act was passed into law with the intention to thwart international money laundering and terrorist financing. The Act significantly strengthens previous anti-money laundering laws, including the original Bank Secrecy Act, which imposes record-keeping and reporting requirements on certain financial institutions, such as the need to keep records and file reports on currency transactions and foreign bank accounts.

In today's global economy, criminal organizations generate huge sums of money by drug trafficking, arms smuggling and financial crime. "Dirty money", however, is of little use to organized crime because it raises the suspicions of law enforcement and leaves a trail of incriminating evidence. Criminals who wish to benefit from the proceeds of large-scale crime must disguise their illegal profits without compromising themselves. This process is known as money laundering.

Definition of Money Laundering

The Financial Action Task Force (FATF), the Paris-based multinational group formed in 1989 by the Group of Seven industrialized nations to foster international action against money laundering, has agreed to this "working definition" of money laundering:

1. The conversion or transfer of property, knowing it is derived from a criminal offense, for the purpose of concealing or disguising its illicit origin or of assisting any person who is involved in the commission of the crime to evade the legal consequences of his actions,
2. The concealment or disguising of the true nature, source, location, disposition, movement, rights with respect to, or ownership of property knowing that it is derived from a criminal offense,
3. The acquisition, possession or use of property, knowing at the time of its receipt that it was derived from a criminal offense or from participation in a crime.

In general, the U.S. money laundering laws apply to:

1. Any financial transaction, or anyone who transports, transfers, transmits a monetary instrument or funds from a place in the United States to or through a place outside the United States, or from a place outside the United States to or through a place in the United States, or attempts to do so,
2. Any activity involving the proceeds of "specified unlawful activity"
3. Any person or entity who has knowledge of funds that have come from some form of unlawful activity,
4. Any person or entity with the intent to promote an unlawful activity, or evade U.S. taxes, or conceal the ownership of the money or assets, or to cause a report required to be made under federal or state law.

Verity Asset Management AML Policies and Procedures

Money Laundering Process

Money laundering is the process that disguises illegal profits without compromising the criminals who wish to benefit from the proceeds. There are two reasons why criminals, whether drug traffickers, corporate embezzlers, or corrupt public officials, must launder money, (1) the money trail is evidence of their crime and (2) the money itself is vulnerable to seizure and must be protected. Regardless of who uses the apparatus of money laundering, the operational principles are essentially the same. Money laundering is a dynamic three-stage process. These three stages are usually referred to as Placement, Layering, and Integration.

- Placement, moving the funds from direct association with the crime,
- Layering, disguising the trail to foil pursuit; and,
- Integration, making the money available to the criminal once again with its occupational and geographic origins hidden from view.

The placement stage represents the initial entry of the funds into the financial system. For the drug trafficker this is not necessarily an easy task. The immense cash profits of the illegal drug trade can pose an enormous problem. Cash is awkward to deal with regularly and in bulk: \$200,000 in \$10 bills weighs 40 lbs. Banknotes are also easily lost, stolen, or destroyed.

The second stage is layering. This is the most complex stage of the process, and the most international in nature. This usually consists of a series of transactions designed to conceal the origin of the funds. The money launderer might begin by sending funds electronically from one country to another, then break them up into investments in advanced financial options or in overseas markets, moving them constantly to evade detection, each time hoping to exploit loopholes or discrepancies in legislation and delays in judicial or police cooperation.

The final stage of money laundering is termed the integration stage because it is at this point that the funds return fully assimilated into the legal economy. Having been placed initially as cash and layered through several financial operations, the criminal proceeds are fully integrated into the financial system and can be used for any purpose.

General Policy

It is strictly prohibited for any person associated with the Firm to engage in the laundering of money or any activity associated with the funding of terrorist or other illegal activities. The Firm and its management are firmly committed to reporting and prosecuting all personnel who participate, or have any knowledge whatsoever, of any money laundering or terrorist funding activities.

It is the responsibility of every person associated with this Firm to IMMEDIATELY report any suspicious activity in a customer account, or suspicious activity of any registered, non-registered, or affiliated person of the Firm, directly to the Anti-Money Laundering Compliance Officer (AMLCO), unless violations implicate the AMLCO, in which case the employee will report to one of the other officers of the Corporation. Such reports are confidential, and it is strictly prohibited for any person associated with the Firm to prevent, obstruct, or retaliate against any person who reports suspicious activity. The AMLCO will report all activity to the proper authorities as required by the USA PATRIOT Act and fully comply with any other legislation associated with money laundering and terrorist activities.

Verity Asset Management AML Policies and Procedures

Anti-Money Laundering Compliance Officer (AMLCO)

The SEC has requested that each registered firm designate a person to communicate with the SEC if any person or entity associated with the firm is suspected of money laundering. The SEC also stated that the "point person" should be a senior level individual who understands the sensitive and confidential nature of the information provided by the government. The Firm has accordingly designated Gordon T. Wegwart as its Anti-Money Laundering Compliance Officer (AMLCO) and William R. Hopwood as back-up AMLCO.

It will be the responsibility of the AMLCO to continuously monitor the activity of the Firm, its clients, and its associated personnel to ensure that they are not participating in any inappropriate activity. The AMLCO also maintains the responsibility to file all required money laundering and currency reports and all Suspicious Activity Reports (SARS) with the regulatory agencies and ensures compliance with the policies and procedures outlined below. The AMLCO ensures that the firm cooperates with all regulatory money laundering investigations and provides the documentation and information requested by state, federal, and self-regulatory organizations. The AMLCO is responsible for monitoring pertinent rule changes under the USA Patriot Act and modifying these procedures as needed to maintain compliance. The AMLCO is also required to ensure that the Firm provides its associated personnel with adequate training relating to money laundering and updates the Firm's Written Supervisory Procedures (WSPs) relating to money laundering, cash and currency transactions and the USA PATRIOT Act as necessary. Additionally, the AMLCO ensures that proper AML records are kept.

AML Information Sharing

The Firm is committed to responding to any Financial Crimes Enforcement Network (FinCEN) requests about accounts or transactions including responses to email reminders to check the FinCEN website directed every two weeks. Under the supervision of the AMLCO, all names are researched within 10 days of receipt or reminder to determine whether they match any clients in the Firm's client database. Confirmation is retained in the form of the AMLCO's initials on a copy of the request. The Firm reports to FinCEN the identity of any matching individuals or organizations, the account number, all identifying information provided by the account holder, when the account was established, and the date and type of transaction. Reporting is both by email to SYS314a@fincen.gov AND via the web-enabled system at <https://www.fincen.gov/314a/>, as well as by any other means that FinCEN specifies.

The Firm shares information about those suspected of terrorism and money laundering with other financial institutions for the purposes of identifying and reporting activities that may involve terrorist acts or money laundering activities. Using the certification form found at <https://www.fincen.gov/314b/>, the Firm files with FinCEN an initial certification, before any sharing occurs, and annual certifications afterwards. The Firm also confirms that the institution has filed the requisite notice with FinCEN by obtaining from them a copy of that certification. The Firm employs strict procedures both to ensure that only relevant information is shared and to protect the security and confidentiality of this information, including segregating it from the Firm's other books and records.

Verity Asset Management AML Policies and Procedures

Employee Training

The PATRIOT Act requires financial institutions to implement ongoing employee training programs relating to money laundering. The AMLCO establishes a training program for employees regarding "red flags" that could indicate money laundering transactions. The Firm has contracted with a third-party vendor to facilitate training courses that are administered to all employees at least annually. Additionally, educational pamphlets, videos, intranet systems, in-person lectures, and explanatory memos are all appropriate training vehicles which may be used for anti-money laundering training.

The training is tailored to the apply to the type and size, customer base, and resources of Verity Investments, Inc. The Firm instructs its employees about the following topics, at a minimum:

- How to identify "red flags" and possible signs of money laundering that could arise during the course of their duties;
- What to do once the risk is identified;
- What their roles are in the Firm's compliance efforts;
- How to perform their roles;
- The Firm's record retention policy; and
- Disciplinary consequences, including civil and criminal penalties, for non-compliance with the Money Laundering Abatement Act.

The AMLCO is responsible for ensuring that the Firm conducts anti-money laundering training on an annual basis, typically as part of the Firm Element Continuing Education plan. Additionally, the AMLCO verifies that the Firm maintains documentation of completion of the training by having all participants sign an acknowledgment and maintain notes of the topics covered and training materials used during the training. These acknowledgments, notes, and training materials are maintained in accordance with SEC Rule 17a-3 and 17a-4.

The AMLCO periodically scrutinizes the Firm's operations to determine if there are certain employees who may need additional or specialized training due to their duties and responsibilities. For example, employees in Compliance may need more comprehensive training.

The AMLCO is responsible to conduct periodic evaluation of the anti-money laundering training program to ensure that employees are informed about any new developments with money laundering rules and regulations. Training materials are updated, as necessary, to reflect new developments in the law.

Independent Audit and Testing

The PATRIOT Act requires financial institutions to establish an independent audit system to ensure that the Firm's internal anti-money laundering program and systems are adequate and are being followed properly.

While the AMLCO provides the auditor/committee with information regarding the Firm's compliance, the testing itself may not be conducted by the AMLCO(s), individuals responsible for implementing and monitoring the day-to-day operations and internal controls of the AML program, persons who perform the AML functions being tested, or anyone who reports to these persons.

Verity Asset Management AML Policies and Procedures

[At this time, investment advisory firms are not subject to the regulation. While the procedures of Verity Asset Management are parallel to those of our affiliated broker dealer, Verity Investments, Inc., which does undergo annual testing, the procedures of Verity Asset Management are not specifically tested by an independent third-party.]

Opening Accounts

Identification of Customers

Registered firms must implement procedures released jointly by the Securities and Exchange Commission and the Department of the Treasury to verify the identity of customers. These procedures require financial institutions at a minimum to (i) verify, to the extent reasonable and practicable, the identity of anyone seeking to open an account, including existing clients who open new accounts after the effective date of the final regulations; (ii) maintain records of the information used to verify the identity of the person; and (iii) consult lists of known or suspected terrorists to see if such persons appear on the lists.

To comply with these requirements, the new account review process ensures that the following information is obtained, and procedures followed for all new accounts:

- The customer's full name (An anonymous account is not permitted)
- The customer's full residential or business street address, including apartment number (Individuals without a street address may use an Army Post Office or Fleet Post Office box number, or the residential or business street address of a next of kin or another contact individual)
- The customer's date of birth
- For U.S. persons or entities (which means a U.S. citizen or an entity such as a corporation, partnership or trust established under the laws of a state or the United States), the customer's taxpayer identification number
- For non-U.S. persons or entities, a taxpayer identification number, a passport number and country of issuance, an alien identification card number, or the number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or other biometric safeguard
- The customer's occupation, employer, and employment address

Depending upon the nature of the account, we will take the following additional steps to the extent reasonable and practicable:

- Inquires about the source of the customer's assets and income so it can determined if the inflow and outflow of money is consistent with the customer's financial status.
- Gains an understanding of what the customer's likely trading patterns will be, so that any deviations from the pattern may be detected later.

Customer Unwillingness to Provide Information

Employees must notify the AMLCO if a prospective customer seems unwilling to provide complete information or appears to have intentionally provided misleading information. The unwillingness of a

Verity Asset Management AML Policies and Procedures

customer to provide complete information is a “red flag” that the customer may be trying to hide something.

Verification of Identity

These procedures are designed to enable the Firm to form a reasonable belief that it knows the true identity of each customer. They are based on an assessment of the relevant risks, including those presented by the various types of accounts maintained, the methods of opening accounts, and the types of identifying information available, as well as the Firm’s size, location, and customer base. In verifying customer identity, the Firm evaluates logical inconsistencies in the information obtained.

In evaluating the risk of having an inaccurate identity provided to the Firm by a customer, the following observations have been noted:

- Verity Asset Management is an investment advisory firm that restricts trading, account opening, and account distribution authority to a very limited number of internal personnel.
- The Firm’s target market is predominantly in the retirement plans arena (including salary reduction contributions and rollovers/transfers of retirement plan accounts).
- Practically all business comes through referrals from existing clients, referrals from other advisors, or from calling on employees of institutions with which the Firm has established a relationship. There is virtually no walk-in or unsolicited call-in business of any kind.
- The Firm accepts accounts from various parts of the United States but does not maintain any foreign accounts.
- The Firm does not accept currency under any circumstance.

Because of these factors, the Firm does not consider its clientele to be high risk. However, the Firm uses documents to verify customer identity when appropriate documents are available. Appropriate documents include:

- For U.S. persons, including beneficial owners of legal entity accounts, an unexpired driver’s license, passport, or other government identification showing nationality or residence and bearing a photograph or other biometric safeguard.
- For non-U.S. persons, an unexpired alien registration card, passport or other government-issued identification showing nationality or residence and bearing a photograph or other biometric safeguard. Additionally due diligence may be required for various reasons including the customer’s country of origin. The AMLCO maintains the responsibility to determine what, if any, additional information should be obtained for non-resident alien accounts.
- For domestic businesses, certified articles of incorporation, a government-issued business license, a partnership agreement, any corporate resolutions, or similar documents, including documentation verifying the authority of the businesses representative to act on its behalf (along with documentation of the personal identity of such representative). Documentation for businesses or other legal entities not publicly traded in the United States should provide sufficient information about the structure or ownership of the entity to allow the Firm to determine whether the account poses a heightened risk.
- For domestic trusts, a copy of the trust document or other documentation that identifies the trustee, the activity the trust authorizes, and the authority of the trust’s representative to act

Verity Asset Management AML Policies and Procedures

on its behalf (along with documentation of the personal identity of such representative). Documentation should provide a reasonable understanding of the trust structure and provider of funds and any persons or entities that have control over the funds or have the power to remove the trustees.

- For foreign operating commercial entities, documents regarding the nature of the company's business, its location, and any other due diligence information that the AMLCO deems necessary. Documentation should provide sufficient information about the structure or ownership of the entity to allow the Firm to determine whether the account poses a heightened risk.
- For personal investment corporations or personal holding companies, documents to identify the principal beneficial owner(s) of offshore corporate accounts where such accounts are personal investment corporations or personal holding companies. The AMLCO maintains the responsibility to determine what, if any, additional information should be obtained for these types of accounts.
- For offshore trusts, documents to identify the principal and beneficial ownership, which will then be cross-referenced with SDN and OFAC lists (see "Government Lists" below). The Firm reserves the right to conduct additional due diligence for accounts under the jurisdiction of countries who lack regulatory oversight over trust formation. The AMLCO is informed upon any application by an offshore trust and maintains the responsibility to determine what, if any, additional information should be obtained for these types of accounts.
- Intermediary accounts (such as hedge funds, investment company funds, and institutional accounts) are not currently held and the Firm does not anticipate holding such accounts in the future. Should the Firm decide to hold such accounts, procedures will be established on a case-by-case basis, considering, among other things, whether the intermediary has its own established procedures for anti-money laundering, its public reputation, and whether it is from a jurisdiction which warrants greater scrutiny.

Verification of customer identity through the use of non-documentary evidence is required in the following situations: (1) when the customer is unable to present the required documents; (2) when the documents the customer presents for identification verification are unfamiliar to the Firm; (3) when the customer and Firm do not have face-to-face contact; or (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. Under these circumstances, the Firm may use the following non-documentary methods of verifying identity:

- Contact the customer after the account has been opened (although this cannot be the sole means of verification).
- Obtain financial statements from the customer.
- Compare information obtained from the customer against databases, such as Equifax, Experian, Lexis/Nexis, or other in-house or custom databases.
- Compare information obtained from customer with information available from a trusted third-party source (such as a credit report).
- Check references with other financial institutions.

Verity Asset Management AML Policies and Procedures

- Any other non-documentary means deemed appropriate by the AMLCO.

For entities of any type other than legal entities, should the Firm be unable to verify the identity using the verification methods described above, information about the individuals with authority or control over the account, included standard documentation used to verify their individual identities as well as documentation verifying their legal authority over the account is required.

Accounts of any type identified as posing a heightened risk are subject to enhanced due diligence including, at the discretion of the AMLCO, steps to identify and verify beneficial owners, to reasonably understand the sources and uses of funds in the account, and to reasonably understand the relationship between the customer and the beneficial owner. In addition, the information collected should be used for monitoring purposes and to determine whether there are discrepancies between information obtained regarding the account's intended purpose and expected account activity, and the actual sources of funds and uses of the account.

The Firm verifies the information at the time new accounts are opened, if possible, but in most situations no later than five business days after opening. However, the Firm recognizes that there may be situations where even a five-day delay will be too long. Depending on the nature of the account and requested transactions, the Firm may refuse to complete a transaction before the information is verified. If the Firm is unable to complete verification for an account that has already been opened, the Firm may, if warranted, close the account. For each customer, identity verification is performed at the time of opening of the initial account; no additional verification is required for opening of subsequent accounts by the same customer.

Foreign Banks and Correspondent Accounts

Broker dealers are prohibited from establishing, maintaining, administering, or managing a "correspondent account" in the United States for an unregulated foreign "shell bank".

A "correspondent" bank account is defined as: *An account established to receive deposits from, make payments on behalf of, or handle other financial transactions for a foreign bank.*

A "shell bank" is defined as: *A foreign bank with no physical presence in any country.*

Verity Asset Management, Inc. does not maintain correspondent accounts and does not accept any paperwork intended to establish such an account. By verifying the identity of beneficial owners of accounts and tracing the source of funds used to open an account (as described elsewhere in this section), the Firm can determine whether an attempt is being made to open a correspondent account for a foreign bank. Any such attempt must be brought to the attention of the AMLCO.

The Firm requires any foreign bank account holders to complete model certifications issued by the Treasury. The Firm sends the certification forms to foreign bank account holders for completion, which requires them to certify that they are not shell banks and to provide ownership and agent information. The Firm recertifies when it is determined the information is no longer accurate and at least once every three years.

If the Firm does establish an account with a foreign bank or any other financial account in a foreign country, a Foreign Bank and Financial Accounts Report (FBAR) is filed with FinCEN within 5 business days for any account of more than \$10,000 held, or for which a signature or other authority is maintained.

In addition, should the Firm receive a written request from a federal law enforcement officer for information concerning correspondent accounts, the Firm provides that information to the

Verity Asset Management AML Policies and Procedures

requesting officer not later than 7 days after receipt of the request. Within 10 days, any account for a bank (that the Firm has been notified from the Treasury or the Department of Justice) that has failed to comply with a summons or has contested a summons is closed. The Firm scrutinizes any account activity during that 10-day period to ensure that suspicious activity is appropriately reported and ensures that no new positions are established in these accounts.

Foreign Commercial Operating Entities

The Firm conducts special due diligence for all foreign commercial operating entities. Applications by a foreign entity are brought to the attention of the AMLCO by personnel involved in opening accounts. The AMLCO oversees customer identification procedures for such an account and makes a determination regarding any special procedures that may be warranted based upon the circumstances identified and an assessment of risk.

Private Banking Accounts

The Money Laundering Abatement Act requires registered firms, at a minimum, to take reasonable steps to determine the identity of the nominal and beneficial account holders of, and the source of funds deposited into, a private banking account maintained by or on behalf of a non-U.S. citizen. Care is taken to ascertain whether nominal or beneficial owners are senior foreign political figures. A private bank account is an account (or combination of accounts) that requires an aggregate deposit of funds or other assets of more than \$1,000,000 established on behalf of one or more individuals who have a direct or beneficial ownership interest in the account, and is assigned to, or administered by, in whole or in part, an officer, employee, or agent of a financial institution acting as a liaison between the institution and the direct or beneficial owner of the account.

Verity Asset Management, Inc. does not maintain private bank accounts and does not, without establishing procedures for such and conducting appropriate and satisfactory due diligence under the PATRIOT Act and FINRA regulations, accept paperwork intended to establish such an account. By verifying the identity of beneficial owners of accounts and tracing the source of funds used to open an account (as described elsewhere in this section), the Firm may determine whether an attempt is being made to open a private bank account.

Senior Foreign Government Official Accounts

In addition to the above, the Firm conducts enhanced scrutiny of accounts requested or maintained by, or on behalf of, a senior foreign political figure, or any immediate family member or close associate of a senior foreign political figure. Included in this scrutiny is a review of the personal investments, accounts, and other holdings of such individuals.

Shell Companies

A shell company is a business entity that has no significant assets or operations. Such entities provide an opportunity to move money by means of wire transfers or other methods without company owners having to disclose their true identities or the nature or purpose of transactions.

Verity Asset Management, Inc. does not maintain accounts for shell companies and does not, without establishing procedures for such, accept paperwork intended to establish such an account. In considering the establishment of an account for a business entity, the Firm seeks to determine, through a sufficient combination of factors such as identification of ownership, nature of operations, assets, and/or revenue, that the business is not operating as a shell company.

Verity Asset Management AML Policies and Procedures

Recordkeeping

The Firm documents verification, including the type of document used, any identification number contained in the document, the place of issuance, and, if any, the date of issuance and the expiration date. If using non-documentary verification, the Firm provides a description of the methods used and results of verification. In either case, the Firm makes a record of the resolution of any discrepancy in the identifying information. The Firm maintains these records for five years after the account has been closed or the customer's trading authority over the account has ended.

Notification Requirements Prior to Opening Atypical Accounts

Personnel with duties involving account opening are required to notify the AMLCO upon application for any type of account other than typical accounts for U.S. persons, domestic businesses, and domestic trusts. Notification prior to account opening is made for non-U.S. persons, foreign commercial entities, personal investment corporations or holding companies, offshore trusts, or intermediary accounts. The Firm does not permit anonymous accounts, correspondent accounts, private bank accounts, or shell companies, and any attempt to open any account of these types must be brought to the attention of the AMLCO.

Checking Government Lists of Terrorists and Other Criminals

Before opening an account, and no less than annually thereafter, the Firm checks to ensure that the customer – or, for legal entities, any beneficial owner - does not appear on any list of known or suspected terrorists or terrorist organizations issued by any Federal government agency and designated as such by Treasury in consultation with the Federal functional regulators and follows all Federal directives issued in connection with such lists. [Currently, and until further notice, the Firm checks for persons and organizations listed on Treasury's Office of Foreign Assets Control (OFAC) website (<https://sanctionssearch.ofac.treas.gov/>), also available through an automated search tool on <https://ofac.finra.org/> under "Terrorists" or "Specially Designated Nationals and Blocked Persons" (SDN List), as well as the listed embargoed countries and regions (collectively, the OFAC List).] In this manner, the Firm references a currently updated list of suspect persons and organizations. The Firm has also engaged a third-party vendor to check the client base against the OFAC list on an annual basis.

If the Firm determines a customer, beneficial owner, or someone with or for whom the customer is transacting, is on the SDN List or is from or engaging in transactions with a person or entity located in an embargoed country or region, the Firm rejects the transaction and/or blocks the customer's assets and files a blocked assets and/or rejected transaction form with OFAC. The Firm also calls the OFAC Hotline at 800-540-6322.

Notice to Customers

The Firm provides notice to customers that it is requesting information from them to verify their identities, as required by Federal law. This notice is provided in writing on the Firm's new account application.

Monitoring For Suspicious Activity

The AMLCO is responsible to continuously monitor the Firm's activities for indications of money laundering. As part of this process, designated principals review the Firm's trade blotters, new account applications, and account change forms for signs of suspicious activity. Account applications and change forms are reviewed daily; the new account review principal's initials on file copies of the

Verity Asset Management AML Policies and Procedures

forms document this review. Account distributions are monitored on an ongoing basis by a designated principal with particular attention directed to the size and pattern of withdrawal transactions; the principal's initial and date on the distribution forms reflects this review.

The designated principals, as well as all other associated personnel, are aware of "red flags" that may indicate suspicious activity. If "red flags" are detected, the associated person identifying the suspicious activity immediately notifies the AMLCO for investigation to determine whether to freeze the account and/or file a Suspicious Activity Report. Additionally, if the account holder is listed on the OFAC list; an account is held by an entity that is owned or controlled by a person or entity listed on the OFAC list; a customer tries to use bribery, coercion, or similar means to open an account or carry out a suspicious activity; the Firm has reason to believe the customer is trying to move illicit cash out of the government's reach; or the Firm has reason to believe the customer is about to use the funds to further an act of terrorism, the Firm must call the OFAC Hotline at 800-540-6322.

Monitoring For "Red Flags"

Examples of "red flags" can include but are not limited to the following:

1. The customer exhibits unusual concern regarding the firm's compliance with government reporting requirements and the firm's anti-money laundering policies, particularly with respect to 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 suspect identification or business documents.
2. The customer wishes to engage in transactions that lack business sense or apparent investment strategy or are inconsistent with the customer's stated business strategy.
3. The information provided by the customer that identifies a legitimate source for funds is false, misleading, or substantially incorrect.
4. Upon request, the customer refuses to identify or fails to indicate any legitimate source for his or her funds and other assets.
5. 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.
6. The customer exhibits a lack of concern regarding risks, commissions, or other transaction costs.
7. 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.
8. The customer has difficulty describing the nature of his or her business or lacks general knowledge of his or her industry.
9. For no apparent reason, the customer has multiple accounts under a single name or multiple names, with a large number of inter-account or third-party transfers.
10. The customer is from, or has accounts in, a country identified as a non-cooperative country or territory by the Financial Action Task Force (FATF).

Verity Asset Management AML Policies and Procedures

11. The customer's account has unexplained or sudden extensive wire activity, especially in accounts that had little or no previous activity.
12. The customer's account has a large number of wire transfers to unrelated third parties inconsistent with the customer's legitimate business purpose.
13. 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.
14. The customer's account indicates large or frequent wire transfers, immediately withdrawn by check or debit card without any apparent business purpose.
15. The customer deposits funds 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.
16. The customer makes a funds deposit for the purpose of purchasing a long-term investment followed shortly thereafter by a request to liquidate the position and transfer of the proceeds out of the account.
17. The customer engages in excessive journal entries between unrelated accounts without any apparent business purpose.
18. The customer requests that a transaction be processed in such a manner to avoid the Firm's normal documentation requirements.
19. The customer, for no apparent reason or in conjunction with other "red flags," engages in transactions involving certain types of securities, such as penny stocks, Regulation "S" (Reg S) stocks, and bearer bonds, which although legitimate, have been used in connection with fraudulent schemes and money laundering activity. (Such transactions may warrant further due diligence to ensure the legitimacy of the customer's activity.)
20. The customer's account shows an unexplained high level of account activity with very low levels of securities transactions.
21. The customer maintains multiple accounts or maintains accounts in the names of family members or corporate entities, for no apparent business purpose.
22. The customer's account has inflows of funds or other assets well beyond the known income or resources of the customer.

Additional Red Flags relating to potential Email Compromise Fraud - Schemes in which criminals potentially compromise the email accounts of clients present a new and growing type of AML concern. This type of fraud presents additional challenges for the Firm because the suspicious activity does not involve the customer. In these cases, the customer would be a victim along with the Firm whereby fraudulent wire transfer instructions are provided to the Firm by criminals that are impersonating our customers to misappropriate funds.

- A customer's seemingly legitimate emailed transaction instructions contain different language, timing, and amounts than previously verified and authentic transaction instructions.
- Transaction instructions originate from an email account closely resembling a known customer's email account; however, the email address has been slightly altered by adding, changing, or deleting one or more characters. For example:

Verity Asset Management AML Policies and Procedures

Legitimate email address: *john-doe@abc.com*

Fraudulent email addresses: *john_doe@abc.com, john-doe@bcd.com*

- Emailed transaction instructions direct payment to a known beneficiary; however, the beneficiary's account information is different from what was previously used.
- Emailed transaction instructions direct wire transfers to a foreign bank account that has been documented in customer complaints as the destination of fraudulent transactions.
- Emailed transaction instructions direct payment to a beneficiary with which the customer has no payment history or documented business relationship, and the payment is in an amount similar to or in excess of payments sent to beneficiaries whom the customer has historically paid.
- Emailed transaction instructions include markings, assertions, or language designating the transaction request as "Urgent," "Secret," or "Confidential."
- Emailed transaction instructions are delivered in a way that would give the financial institution limited time or opportunity to confirm the authenticity of the requested transaction.
- Emailed transaction instructions originate from a customer's employee who is a newly authorized person on the account or is an authorized person who has not previously sent wire transfer instructions.
- A customer's employee or representative emails a financial institution transaction instruction on behalf of the customer that are based exclusively on email communications originating from executives, attorneys, or their designees. However, the customer's employee or representative indicates he/she has been unable to verify the transactions with such executives, attorneys, or designees.
- A customer emails transaction requests for additional payments immediately following a successful payment to an account not previously used by the customer to pay its suppliers/vendors. Such behavior may be consistent with a criminal attempting to issue additional unauthorized payments upon learning that a fraudulent payment was successful.
- A wire transfer is received for credit into an account; however, the wire transfer names a beneficiary that is not the account holder of record. This may reflect instances where a victim unwittingly sends wire transfers to a new account number, provided by a criminal impersonating a known supplier/vendor, while thinking the new account belongs to the known supplier/vendor. This red flag may be seen by financial institutions receiving wire transfers sent by another financial institution as the result of email-compromise fraud.

Reporting Requirements

All registered firms are subject to existing Bank Secrecy Act ("BSA") reporting and record keeping requirements. The designated principal maintains the responsibility to file all the required reports summarized below:

Funds Transfers and Transmittals

When the Firm transfers or wires funds of \$3,000 or more, the Firm collects, retains, and records on the transmittal/wire order certain information regarding the transfer, including the name and address of the transmitter and recipient, the amount of the transmittal/wire order, the execution

Verity Asset Management AML Policies and Procedures

date, any payment instructions, the identity of the recipient's financial institution, and the account number of the recipient. Additionally, if the customer is a non-resident alien, the Firm also records a current passport number or other valid government identification number.

Suspicious Activity Reports ("SARs")

The Firm files an SAR for any transactions conducted or attempted through the Firm involving \$5,000 or more where it is suspected the transaction: (1) involves funds derived from illegal activity or an attempt to hide or disguise funds or assets derived from illegal activity; (2) is designed to evade the requirements of the Bank Secrecy Act ("BSA"); (3) has no apparent lawful or business purpose or is not the sort in which the customer would normally be expected to engage, and no reasonable explanation for the transaction can be ascertained; or (4) involves the use of the Firm to facilitate criminal activity.

The Firm does not base its decision on whether to file an SAR solely on whether the transaction falls above a set threshold. The Firm files an SAR and notifies law enforcement of all transactions that raise an identifiable suspicion of criminal, terrorist, or corrupt activities. In high-risk situations, the Firm notifies the government immediately and files an SAR with FinCEN. The SAR is filed no later than 30 calendar days after the date of the initial detection of the facts that constitute the basis for the filing. If no suspect is identified on the date of the initial detection, the Firm may delay filing for an additional 30 days pending identification of a suspect, but in no case will the reporting be delayed more than 60 days after the date of initial detection. After July 12, 2012, SARs must be submitted electronically, or civil monetary penalties may be imposed, including \$500 per violation.

Confidentiality of SARS is critical. This applies not only to the SAR itself, but also to information that would reveal the existence (or non-existence) of the SAR. Penalties for failure to maintain confidentiality are severe, with civil penalties of up to \$100,000 and criminal penalties of up to \$250,000 and/or imprisonment not to exceed 5 years. Should the Firm decide to file an SAR, it is prohibited, by strict Firm policy, to notify any person involved in a reported transaction that the transaction has been reported on an SAR. In addition, it is prohibited for any associated person to disclose any information relating to an SAR or the fact that an SAR was filed, to any party other than to law enforcement agencies or securities regulators, including FINRA and the SEC. (In this regard, the Firm makes available to FINRA any SARs and supporting documentation as well as any information that would reveal the existence of an SAR or any decision not to file an SAR.) Access to all information regarding SARs is restricted exclusively to the AMLCO, the Board of Directors, and members of senior management.

All subpoena requests for information relating to an SAR is forwarded to the AMLCO. If the Firm becomes aware of an unauthorized disclosure of an SAR, or if the Firm receives a subpoena or other request for an SAR from a party other than an authorized government authority or FINRA, as defined in the applicable SAR regulations, the AMLCO immediately contacts both FinCEN's Office of Chief Counsel at 703-905-3590 and the Firm's legal counsel. Subpoena requests are denied pending the outcome of these consultations.

The Firm segregates SAR filings and copies of supporting documentation from other Firm books and records to avoid disclosing SAR filings. Copies of all SAR filings are maintained for at least 5 years.

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

Verity Asset Management AML Policies and Procedures

Currency Transaction Reports (CTR)

The Firm prohibits the receipt of currency. If the Firm discovers that currency has been received, the Firm files with FinCEN within 5 business days CTRs for transactions involving currency that exceed \$10,000. Multiple transactions are treated as a single transaction if they total more than \$10,000 during any one business day. Copies of all filings are initialed by the Compliance Officer and retained in the compliance files as documentation.

Currency and Monetary Instrument Transportation Reports (CMIR)

The Firm prohibits the receipt of currency and monetary instruments (including traveler's checks, checks of any type that are endorsed without restriction, incomplete negotiable instruments that are signed but with the payee's name omitted, and securities or stock in bearer form). The Firm files a CMIR with the Commissioner of Customs within 5 business days whenever the Firm transports, mails, ships or receives monetary instruments of more than \$10,000 at one time (in one calendar day, or if for the purpose of evading the reporting requirements, in one or more days) in or out of the U.S. Copies of all filings are initialed by the Compliance Officer and retained in the compliance files as documentation.

State Reporting Requirements

In addition to the federal requirements for currency and money laundering reporting, the Firm may be required to report information to individual states as well depending on the circumstances. The designated principal maintains responsibility to comply with all state currency and money laundering requirements as well as all federal requirements.

Employee Accounts

The Firm's compliance obligations relating to surveillance for money laundering not only applies to customer activity but to the activity of the Firm and its associated personnel. The AMLCO maintains the responsibility to review the activity of the Firm and its cash accounts as well as the activity of employee accounts maintained with the Firm and at other broker dealers. Accounts maintained by the AMLCO are reviewed by either William Hopwood or Amy Simonson.

Monitoring for New AML Rules and Regulations

The AMLCO or designee monitors The USA PATRIOT Act, Treasury, and BSA rules and regulations (as well as guidance issued by FINRA) on an ongoing basis to ensure that any new requirements related to "type" of account (e.g., Foreign Bank, Private Banking Account, Foreign Senior Official), specific transactions within an account (e.g., wire orders, large transactions), reporting or new account monitoring are incorporated into the Firm's AML program.

To ensure that the AML Program is updated in a timely manner, the AMLCO or designee reviews the following websites each quarter, at minimum, to determine if new AML procedures must be put into effect:

<https://www.bankersonline.com/>

<https://home.treasury.gov/>

<https://www.fincen.gov/>

Documentation of the review including any resulting amendments to the procedures is maintained by the AMLCO.

Verity Asset Management AML Policies and Procedures

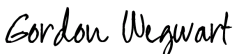
Recordkeeping

The Firm maintains all records and documentation relating to the AML Compliance program for a minimum of six years.

Written Supervisory Procedures

It is the responsibility of the designated principal to review and amend the Firm's Written Supervisory Procedures to reflect changes and amendments relating to the USA PATRIOT Act, Bank Secrecy Act, and Anti-Money Laundering rules and regulations.

Reviewed and approved:

DocuSigned by:

AF3ED10F152C471...
Gordon T. Wegwart

12/21/2023

Date