

The Ravenswood Group

Anti-Money Laundering (AML)/Anti-Terrorist Program

January 1, 2023

1. Firm Policy

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

Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the proceeds appear to have derived from legitimate origins or constitute legitimate assets. Generally, money laundering occurs in three stages. Cash first enters the financial system at the "placement" stage, where the cash generated from criminal activities is converted into monetary instruments, such as money orders or traveler's checks, or deposited into accounts at financial institutions. At the "layering" stage, the funds are transferred or moved into other accounts or other financial institutions to further separate the money from its criminal origin. At the "integration" stage, the funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses.

Our AML policies, procedures and internal controls are designed to ensure compliance with all applicable BSA regulations and FINRA rules and will be reviewed and updated on a regular basis to ensure appropriate policies, procedures and internal controls are in place to account for both changes in regulations and changes in our business.

2. AML Compliance Person Designation and Duties

The firm has designated Gustin as its Anti-Money Laundering Program Compliance Person (AML Compliance Person), with full responsibility for the firm's AML program. Gustin has a limited knowledge of the BSA and its implementing regulations and is qualified by experience, knowledge and training. The duties of the AML Compliance Person will include monitoring the firm's compliance with AML obligations, overseeing communication and training for employees.

3. Giving AML Information to Federal Law Enforcement Agencies and Other Financial Institutions

We will respond to a Financial Crimes Enforcement Network (FinCEN) request concerning accounts and transactions (a 314(a) Request) by immediately searching our records to determine whether we maintain or have maintained any account for, or have engaged in any transaction with, each individual, entity or organization named in the 314(a) Request as outlined in the Frequently Asked Questions (FAQ) located on FinCEN's secure website.

If Gustin searches our records and does not find a matching account or transaction, then Gustin will not reply to the 314(a) Request. We will maintain documentation that we have performed the required search.

We will not disclose the fact that FinCEN has requested or obtained information from us, except to the extent necessary to comply with the information request. Gustin will review, maintain and implement procedures to protect the security and confidentiality of requests from FinCEN similar to those procedures established to satisfy the requirements of Section 501 of the Gramm-Leach-Bliley Act with regard to the protection of customers' nonpublic information.

We will direct any questions we have about the 314(a) Request to the requesting federal law enforcement agency as designated in the request.

Unless otherwise stated in the 314(a) Request, we will not be required to treat the information request as continuing in nature, and we will not be required to treat the periodic 314(a) Requests as a government provided list of suspected terrorists for purposes of the customer identification and verification requirements.

We understand that the receipt of a National Security Letter (NSL) is highly confidential. We understand that none of our officers, employees or agents may directly or indirectly disclose to any person that the FBI or other federal government authority has sought or obtained access to any of our records. To maintain the confidentiality of any NSL we receive, we will process and maintain the NSL. If we file a SAR after receiving an NSL, the SAR will not contain any reference to the receipt or existence of the NSL. The SAR will only contain detailed information about the facts and circumstances of the detected suspicious activity.

We understand that the receipt of a grand jury subpoena concerning a customer does not in itself require that we file a Suspicious Activity Report (SAR). When we receive a grand jury subpoena, we will conduct a risk assessment of the customer subject to the subpoena as well as review the customer's account activity. If we uncover suspicious activity during our risk assessment and review, we will elevate that customer's risk assessment and file a SAR in accordance with the SAR filing requirements. We understand that none of our officers, employees or agents may directly or indirectly disclose to the person who is the subject of the subpoena its existence, its contents or the information we used to respond to it. To maintain the confidentiality of any grand jury subpoena we receive, we will process and maintain the subpoena. If we file a SAR after receiving a grand jury subpoena, the SAR will not contain any reference to the receipt or

existence of the subpoena. The SAR will only contain detailed information about the facts and circumstances of the detected suspicious activity.

We will share information with other financial institutions regarding individuals, entities, organizations and countries for purposes of identifying and, where appropriate, reporting activities that we suspect may involve possible terrorist activity or money laundering. Gustin will ensure that the firm files with FinCEN an initial notice before any sharing occurs and annual notices thereafter.

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

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

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

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

The confidentiality agreement will state that the recipient foreign parent entity (or entities) may not disclose further any SAR, or the fact that such report has been filed. The agreement will allow for the foreign parent entity (or entities) to disclose without permission underlying information (that is, information about the customers and transaction(s) reported) that forms the basis for the SAR and that does not explicitly reveal that a SAR was filed and that is not otherwise subject to disclosure restrictions.

4. Checking the Office of Foreign Assets Control Listings

Before opening an account, and on an ongoing basis, Gustin will check to ensure that a customer does not appear on the SDN list or is not engaging in transactions that are prohibited by the economic sanctions and embargoes administered and enforced by OFAC. Because the SDN list and listings of economic sanctions and embargoes are updated frequently, we will consult them on a regular basis and subscribe to receive any available updates when they occur. With respect to the SDN list, we may also access that list through various software programs to ensure speed and accuracy. lists administered by OFAC. Gustin will also review existing accounts against the SDN list and listings of current sanctions and embargoes when they are updated and he will document the review.

If we determine that a customer is on the SDN list or is engaging in transactions that are prohibited by the economic sanctions and embargoes administered and enforced by OFAC, we will reject the transaction and/or block the customer's assets and file a blocked assets and/or rejected transaction form with OFAC within 10 days. We will also call the OFAC Hotline at (800) 540-6322 immediately.

Our review will include customer accounts, transactions involving customers (including activity that passes through the firm such as wires) and the review of customer transactions.

5. Customer Identification Program

We do not open or maintain customer accounts within the meaning of 31 CFR 1023.100, in that we do not establish formal relationships with “customers” for the purpose of effecting transactions in securities. If in the future the firm elects to open customer accounts or to establish formal relationships with customers for the purpose of effecting transactions in securities, we will first establish, document and ensure the implementation of appropriate CIP procedures.

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 that is opening a new account and whose name is on the account:

- (1) the name;
- (2) date of birth (for an individual);
- (3) an address, which will be a residential or business street address (for an individual), an Army Post Office (APO) or Fleet Post Office (FPO) box 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 location (for a person other than an individual); and
- (4) 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, or 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).

In the event that a customer has applied for, but has not received, a taxpayer identification number, we will confirm that the application was filed before the customer opens the account and to obtain the taxpayer identification number within a reasonable period of time after the account is opened.

When opening an account for a foreign business or enterprise that does not have an identification number, we will request alternative government-issued documentation certifying the existence of the business or enterprise.

b. Customers Who Refuse to Provide Information - NA

c. Verifying Information

Based on the risk, and to the extent reasonable and practicable, we will ensure that we have a reasonable belief that we know the true identity of our customers by using risk-based procedures to verify and document the accuracy of the information we get about our customers. Gustin will analyze the information we obtain to determine whether the information is sufficient to form a reasonable belief that we know the true identity of the customer (*e.g.*, whether the information is logical or contains inconsistencies).

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

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

- For an individual, an unexpired government-issued identification evidencing nationality or residence and bearing a photograph or similar safeguard, such as a driver's license or passport; and
- For a person other than an individual, documents showing the existence of the entity, such as certified articles of incorporation, a government-issued business license, a partnership agreement or a trust instrument.

We understand that we are not required to take steps to determine whether the document that the customer has provided to us for identity verification has been validly issued and that we may rely on a government-issued identification as verification of a customer's identity. If, however, we note that the document shows some obvious form of fraud, we must consider that factor in determining whether we can form a reasonable belief that we know the customer's true identity.

We will use the following non-documentary methods of verifying identity:

- 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 sources.
-
- Checking references with other financial institutions; or
- Obtaining a financial statement.

We will use non-documentary methods of verification when:

- (1) the customer is unable to present an unexpired government-issued identification document with a photograph or other similar safeguard;
- (2) the firm is unfamiliar with the documents the customer presents for identification verification;
- (3) the customer and firm do not have face-to-face contact; and
- (4) 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.

We will verify the information within a reasonable time before or after the account is opened. Depending on the nature of the account and requested transactions, we may refuse to complete a transaction before we have verified the information, or in some instances when we need more time, we may, pending verification, restrict the types of transactions or dollar amount of transactions. If we find suspicious information that indicates possible money laundering, terrorist financing activity, or other suspicious activity, we will, after internal consultation with the firm's AML Compliance Person, file a SAR in accordance with applicable laws and regulations.

We recognize that the risk that we may not know the customer’s true identity may be heightened for certain types of accounts, such as an account opened in the name of a corporation, partnership or trust that is created or conducts substantial business in a jurisdiction that has been designated by the U.S. as a primary money laundering jurisdiction, a terrorist concern, or has been designated as a non-cooperative country or territory. We will identify customers that pose a heightened risk of not being properly identified. We will also take the following additional measures that may be used to obtain information about the identity of the individuals associated with the customer when standard documentary methods prove to be insufficient:

d. Lack of Verification

When we cannot form a reasonable belief that we know the true identity of a customer, we will do the following: (1) not open an account; (2) impose terms under which a customer may conduct transactions while we attempt to verify the customer’s identity; (3) close an account after attempts to verify a customer’s identity fail; and (4) determine whether it is necessary to file a SAR in accordance with applicable laws and regulations.

e. Recordkeeping

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

f. Comparison with Government-Provided Lists of Terrorists

At such time as we receive notice that a federal government agency has issued a list of known or suspected terrorists and identified the list as a list for CIP purposes, we will, within a reasonable period of time after an account is opened (or earlier, if required by another federal law or regulation or federal directive issued in connection with an applicable list), determine whether a customer appears on any such 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. We will follow all federal directives issued in connection with such lists.

We will continue to comply separately with OFAC rules prohibiting transactions with certain foreign countries or their nationals.

g. Notice to Customers

We will provide notice to customers that the firm is requesting information from them to verify their identities, as required by federal law. We will use the following method to provide notice to customers:

Important Information About Procedures for Opening a New Account

To help the government fight the funding of terrorism and money laundering activities, federal law requires all financial institutions to obtain, verify, and record information that identifies each person who opens an account.

h. Reliance on Another Financial Institution for Identity Verification

We may, under the following circumstances, rely on the performance by another financial institution (including an affiliate) of some or all of the elements of our CIP with respect to any customer that is opening an account or has established an account or similar

business relationship with the other financial institution to provide or engage in services, dealings or other financial transactions:

- when such reliance is reasonable under the circumstances;
- when the other financial institution is subject to a rule implementing the anti-money laundering compliance program requirements of 31 U.S.C. § 5318(h), and is regulated by a federal functional regulator; and
- when the other financial institution has entered into a contract with our firm requiring it to certify annually to us that it has implemented its anti-money laundering program and that it will perform (or its agent will perform) specified requirements of the customer identification program.

6. Customer Due Diligence Rule

We do not open or maintain accounts for legal entity customers within the meaning of 31 CFR 1010.230. If in the future the firm elects to open accounts for legal entity customers, we will first establish, document and ensure the implementation of appropriate CDD procedures.

7. Correspondent Accounts for Foreign Shell Banks

We will identify foreign bank accounts and any such account that is a correspondent account (any account that is established for a foreign bank to receive deposits from, or to make payments or other disbursements on behalf of, the foreign bank, or to handle other financial transactions related to such foreign bank) for foreign shell banks. Upon finding or suspecting such accounts, firm employees will notify the AML Compliance Person, who will terminate any verified correspondent account in the United States for a foreign shell bank. We will also terminate any correspondent account that we have determined is not maintained by a foreign shell bank but is being used to provide services to such a shell bank. We will exercise caution regarding liquidating positions in such accounts and take reasonable steps to ensure that no new positions are established in these accounts during the termination period. We will terminate any correspondent account for which we have not obtained the information described in Appendix A of the regulations regarding shell banks within the time periods specified in those regulations.

8. Due Diligence and Enhanced Due Diligence Requirements for Correspondent Accounts of Foreign Financial Institutions - NA

We have reviewed our accounts and we do not have, nor do we intend to open or maintain, correspondent accounts for foreign financial institutions.

9. Due Diligence and Enhanced Due Diligence Requirements for Private Banking Accounts/Senior Foreign Political Figures

We do not open or maintain private banking accounts.

10. Compliance with FinCEN's Issuance of Special Measures Against Foreign Jurisdictions, Financial Institutions or International

We do not maintain any accounts (including correspondent accounts) with any foreign jurisdiction or financial institution. However, if FinCEN issues a final rule imposing a special measure against one or more foreign jurisdictions or financial institutions, classes of international transactions or types of accounts deeming them to be of primary money laundering concern, we understand that we must read FinCEN's final rule and follow any prescriptions or prohibitions contained in that rule.

11. Monitoring Accounts for Suspicious Activity

We will monitor account activity for unusual size, volume, pattern or type of transactions, taking into account risk factors and red flags that are appropriate to our business and review relevant information from internal or third-party sources before a SAR is filed.

a. Emergency Notification to Law Enforcement by Telephone

In situations involving violations that require immediate attention, such as terrorist financing or ongoing money laundering schemes, we will immediately call an appropriate law enforcement authority. If a customer or company appears on OFAC's SDN list, we will call the OFAC Hotline at (800) 540-6322. Other contact numbers we will use are: FinCEN's Financial Institutions Hotline ((866) 556-3974) (especially to report transactions relating to terrorist activity), local U.S. Attorney's office (*insert contact number*), local FBI office and local SEC office to voluntarily report such violations to the SEC in addition to contacting the appropriate law enforcement authority). If we notify the appropriate law enforcement authority of any such activity, we must still file a timely a SAR.

b. Red Flags

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

Potential Red Flags in Customer Due Diligence and Interactions with Customers

- The customer provides the firm with unusual or suspicious identification documents that cannot be readily verified or are inconsistent with other statements or documents that the customer has provided. Or, the customer provides information that is inconsistent with other available information about the customer. This indicator may apply to account openings and to interaction subsequent to account opening.
- The customer is reluctant or refuses to provide the firm with complete customer due diligence information as required by the firm's procedures, which may include information regarding the nature and purpose of the customer's business, prior

financial relationships, anticipated account activity, business location and, if applicable, the entity's officers and directors.

- The customer refuses to identify a legitimate source of funds or information is false, misleading or substantially incorrect.
- The customer is domiciled in, doing business in or regularly transacting with counterparties in a jurisdiction that is known as a bank secrecy haven, tax shelter, high-risk geographic location (*e.g.*, known as a narcotics producing jurisdiction, known to have ineffective AML/Combating the Financing of Terrorism systems) or conflict zone, including those with an established threat of terrorism.
- The customer has difficulty describing the nature of his or her business or lacks general knowledge of his or her industry.
- The customer has no discernable reason for using the firm's service or the firm's location (*e.g.*, the customer lacks roots to the local community or has gone out of his or her way to use the firm).
- The customer has been rejected or has had its relationship terminated as a customer by other financial services firms.
- The customer's legal or mailing address is associated with multiple other accounts or businesses that do not appear related.
- The customer appears to be acting as an agent for an undisclosed principal, but is reluctant to provide information.
- The customer is a trust, shell company or private investment company that is reluctant to provide information on controlling parties and underlying beneficiaries.
- The customer is publicly known or known to the firm to have criminal, civil or regulatory proceedings against him or her for crime, corruption or misuse of public funds, or is known to associate with such persons. Sources for this information could include news items, the Internet or commercial database searches.
- The customer's background is questionable or differs from expectations based on business activities.
- The customer maintains multiple accounts, or maintains accounts in the names of family members or corporate entities, with no apparent business or other purpose.
- An account is opened by a politically exposed person (PEP),⁹ particularly in conjunction with one or more additional risk factors, such as the account being opened by a shell company¹⁰ beneficially owned or controlled by the PEP, the PEP is from a country which has been identified by FATF as having strategic AML regime deficiencies, or the PEP is from a country known to have a high level of corruption.
- An account is opened by a non-profit organization that provides services in geographic locations known to be at higher risk for being an active terrorist threat.¹¹
- An account is opened in the name of a legal entity that is involved in the activities of an association, organization or foundation whose aims are related to the claims or demands of a known terrorist entity.¹²

- An account is opened for a purported stock loan company, which may hold the restricted securities of corporate insiders who have pledged the securities as collateral for, and then defaulted on, purported loans, after which the securities are sold on an unregistered basis.
- An account is opened in the name of a foreign financial institution, such as an offshore bank or broker-dealer, that sells shares of stock on an unregistered basis on behalf of customers.
- An account is opened for a foreign financial institution that is affiliated with a U.S. broker-dealer, bypassing its U.S. affiliate, for no apparent business purpose. An apparent business purpose could include access to products or services the U.S. affiliate does not provide.
- Seemingly unrelated clients open accounts on or at about the same time, deposit the same low-priced security and subsequently liquidate the security in a manner that suggests coordination.

Potential Red Flags in Money Movements

- The customer attempts or makes frequent or large deposits of currency, insists on dealing only in cash equivalents, or asks for exemptions from the firm's policies and procedures relating to the deposit of cash and cash equivalents.
- The customer "structures" deposits, withdrawals or purchases of monetary instruments below a certain amount to avoid reporting or recordkeeping requirements, and may state directly that they are trying to avoid triggering a reporting obligation or to evade taxing authorities.
- The customer seemingly breaks funds transfers into smaller transfers to avoid raising attention to a larger funds transfer. The smaller funds transfers do not appear to be based on payroll cycles, retirement needs, or other legitimate regular deposit and withdrawal strategies.
- The customer's account shows numerous currency, money order (particularly sequentially numbered money orders) or cashier's check transactions aggregating to significant sums without any apparent business or lawful purpose.
- The customer frequently changes bank account details or information for redemption proceeds, in particular when followed by redemption requests.
- 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.
- Wire transfers are made in small amounts in an apparent effort to avoid triggering identification or reporting requirements.

- Incoming payments are made by third-party checks or checks with multiple endorsements.
- Outgoing checks to third parties coincide with, or are close in time to, incoming checks from other third parties.
- Payments are made by third party check or money transfer from a source that has no apparent connection to the customer.
- Wire transfers are made to or from financial secrecy havens, tax havens, high-risk geographic locations or conflict zones, including those with an established presence of terrorism.
- Wire transfers originate from jurisdictions that have been highlighted in relation to black market peso exchange activities.
- The customer engages in transactions involving foreign currency exchanges that are followed within a short time by wire transfers to locations of specific concern (*e.g.*, countries designated by national authorities, such as FATF, as non-cooperative countries and territories).
- The parties to the transaction (*e.g.*, originator or beneficiary) are from countries that are known to support terrorist activities and organizations.
- Wire transfers or payments are made to or from unrelated third parties (foreign or domestic), or where the name or account number of the beneficiary or remitter has not been supplied.
- There is wire transfer activity that is unexplained, repetitive, unusually large, shows unusual patterns or has no apparent business purpose.
- The securities account is used for payments or outgoing wire transfers with little or no securities activities (*i.e.*, account appears to be used as a depository account or a conduit for transfers, which may be purported to be for business operating needs).
- Funds are transferred to financial or depository institutions other than those from which the funds were initially received, specifically when different countries are involved.
- The customer engages in excessive journal entries of funds between related or unrelated accounts without any apparent business purpose.
- The customer uses a personal/individual account for business purposes or vice versa.
- A foreign import business with U.S. accounts receives payments from outside the area of its customer base.

- There are frequent transactions involving round or whole dollar amounts purported to involve payments for goods or services.
- Upon request, a customer is unable or unwilling to produce appropriate documentation (*e.g.*, invoices) to support a transaction, or documentation appears doctored or fake (*e.g.*, documents contain significant discrepancies between the descriptions on the transport document or bill of lading, the invoice, or other documents such as the certificate of origin or packing list).
- The customer requests that certain payments be routed through nostro¹⁴ or correspondent accounts held by the financial intermediary instead of its own accounts, for no apparent business purpose.
- Funds are transferred into an account and are subsequently transferred out of the account in the same or nearly the same amounts, especially when the origin and destination locations are high-risk jurisdictions.
- A dormant account suddenly becomes active without a plausible explanation (*e.g.*, large deposits that are suddenly wired out).
- Nonprofit or charitable organizations engage in financial transactions for which there appears to be no logical economic purpose or in which there appears to be no link between the stated activity of the organization and the other parties in the transaction.
- There is unusually frequent domestic and international automated teller machine (ATM) activity.
- A person customarily uses the ATM to make several deposits into a brokerage account below a specified BSA/AML reporting threshold.
- Many small, incoming wire transfers or deposits are made using checks and money orders that are almost immediately withdrawn or wired out in a manner inconsistent with the customer's business or history; the checks or money orders may reference in a memo section "investment" or "for purchase of stock." This may be an indicator of a Ponzi scheme or potential funneling activity.
- Wire transfer activity, when viewed over a period of time, reveals suspicious or unusual patterns, which could include round dollar, repetitive transactions or circuitous money movements.

Other Potential Red Flags

- The customer is reluctant to provide information needed to file reports to proceed with the transaction.
- The customer exhibits unusual concern with the firm's compliance with government reporting requirements and the firm's AML policies.

- The customer tries to persuade an employee not to file required reports or not to maintain the required records.
- Notifications received from the broker-dealer's clearing firm that the clearing firm had identified potentially suspicious activity in customer accounts. Such notifications can take the form of alerts or other concern regarding negative news, money movements or activity involving certain securities.
- Law enforcement has issued subpoenas or freeze letters regarding a customer or account at the securities firm.
- The customer makes high-value transactions not commensurate with the customer's known income or financial resources.
- The customer wishes to engage in transactions that lack business sense or an apparent investment strategy, or are inconsistent with the customer's stated business strategy.
- The stated business, occupation or financial resources of the customer are not commensurate with the type or level of activity of the customer.
- The customer engages in transactions that show the customer is acting on behalf of third parties with no apparent business or lawful purpose.
- The customer engages in transactions that show a sudden change inconsistent with normal activities of the customer.
- Securities transactions are unwound before maturity, absent volatile market conditions or other logical or apparent reason.
- The customer does not exhibit a concern with the cost of the transaction or fees (*e.g.*, surrender fees, or higher than necessary commissions).
- A borrower defaults on a cash-secured loan or any loan that is secured by assets that are readily convertible into currency.
- There is an unusual use of trust funds in business transactions or other financial activity.

c. Responding to Red Flags and Suspicious Activity

When an employee of the firm detects any red flag, or other activity that may be suspicious, he or she will notify Gustin of the activity. Under the direction of the AML Compliance Person, the firm will determine whether or not and how to further investigate the matter. This may include gathering additional information internally or from third-party sources, contacting the government, freezing the account and/or filing a SAR.

12. Suspicious Transactions and BSA Reporting

a. Filing a SAR

We will file SARs with FinCEN for any transactions (including deposits and transfers) conducted or attempted by, at or through our firm involving \$5,000 or more of funds or assets (either individually or in the aggregate) where we know, suspect or have reason to suspect:

- (1) the transaction involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity as part of a plan to violate or evade 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 any 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 after examining the background, possible purpose of the transaction and other facts, we know of no reasonable explanation for the transaction; or
- (4) the transaction involves the use of the firm to facilitate criminal activity.

We will also file a SAR and notify the appropriate law enforcement authority in situations involving violations that require immediate attention, such as terrorist financing or ongoing money laundering schemes. In addition, although we are not required to, we may contact that SEC in cases where a SAR we have filed may require immediate attention by the SEC. We also understand that, even if we notify a regulator of a violation, unless it is specifically covered by one of the exceptions in the SAR rule, we must file a SAR reporting the violation.

We may file a voluntary SAR for any suspicious transaction that we believe is relevant to the possible violation of any law or regulation but that is not required to be reported by us under the SAR rule. It is our policy that all SARs will be reported regularly to the Board of Directors and appropriate senior management, with a clear reminder of the need to maintain the confidentiality of the SAR.

We 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-SF. We will identify and maintain supporting documentation and make such information available to FinCEN, any other appropriate law enforcement agencies, federal or state securities regulators or SROs upon request.

We will not notify any person involved in the transaction that the transaction has been reported, except as permitted by the BSA regulations. We understand that anyone who is subpoenaed or required to disclose a SAR or the information contained in the SAR will, except where disclosure is requested by FinCEN, the SEC, or another appropriate law enforcement or regulatory agency, or an SRO registered with the SEC, decline to produce the SAR or to provide any information that would disclose that a SAR was prepared or filed. We will notify FinCEN of any such request and our response.

b. Currency Transaction Reports

Our firm prohibits transactions involving currency and has the following procedures to prevent such transactions. If we discover such transactions have occurred, we will file with FinCEN CTRs for currency transactions that exceed \$10,000. Also, we will treat multiple transactions involving currency as a single transaction for purposes of determining whether to file a CTR if they total more than \$10,000 and are made by or on behalf of the same person during any one business day.

c. Currency and Monetary Instrument Transportation Reports

Our firm prohibits both the receipt of currency or other monetary instruments that have been transported, mailed or shipped to us from outside of the United States, and the physical transportation, mailing or shipment of currency or other monetary instruments by any means other than through the postal service or by common carrier.

d. Foreign Bank and Financial Accounts Reports

We will file a Foreign Bank and Financial Accounts Report (FBAR) for any financial accounts of more than \$10,000 that we hold, or for which we have signature or other authority over, in a foreign country

e. Monetary Instrument Purchases

We do not issue bank checks or drafts, cashier's checks, money orders or traveler's checks in the amount of \$3,000 or more.

f. Funds Transmittals of \$3,000 or More Under the Travel Rule - NA

13. AML Recordkeeping

a. Responsibility for Required AML Records and SAR Filing

Our AML Compliance Person and his or her designee will be responsible for ensuring that AML records are maintained properly and that SARs are filed as required.

b. SAR Maintenance and Confidentiality

We will hold SARs and any supporting documentation confidential. We will not inform anyone outside of FinCEN, the SEC, an SRO registered with the SEC or other appropriate law enforcement or regulatory agency about a SAR. We will refuse any subpoena requests for SARs or for information that would disclose that a SAR has been prepared or filed and immediately notify FinCEN of any such subpoena requests that we receive.

c. Additional Records

We shall retain either the original or a microfilm or other copy or reproduction of each of the following:

- A record of each extension of credit in an amount in excess of \$10,000, except an extension of credit secured by an interest in real property. The record shall contain the name and address of the person to whom the extension of credit is made, the amount thereof, the nature or purpose thereof and the date thereof;
- A record of each advice, request or instruction received or given regarding any transaction resulting (or intended to result and later canceled if such a record is normally made) in the transfer of currency or other monetary instruments, funds, checks, investment securities or credit, of more than \$10,000 to or from any person, account or place outside the U.S.;
- A record of each advice, request or instruction given to another financial institution (which includes broker-dealers) or other person located within or without the U.S., regarding a transaction intended to result in the transfer of funds, or of currency, other monetary instruments, checks, investment securities or credit, of more than \$10,000 to a person, account or place outside the U.S.;
- A record of each remittance or transfer of funds, or of currency, checks, other monetary instruments, investment securities or credit, of more than \$10,000 to a person, account or place, outside the U.S.; and
- A record of each receipt of currency, other monetary instruments, checks or investment securities and of each transfer of funds or credit, of more than \$10,000 received on any one occasion directly and not through a domestic financial institution, from any person, account or place outside the U.S.

14. Clearing/Introducing Firm Relationships - NA

15. Training Programs

We will develop ongoing employee training under the leadership of the AML Compliance Person and senior management. Our training will occur on at least an annual basis. It will be based on our firm's size, its customer base, and its resources and be updated as necessary to reflect any new developments in the law.

Our training will include, at a minimum: (1) how to identify red flags and signs of money laundering that arise during the course of the employees' duties; (2) what to do once the risk is identified (including how, when and to whom to escalate unusual customer activity or other red flags for analysis and, where appropriate, the filing of SARs); (3) what employees' roles are in the firm's compliance efforts and how to perform them; (4) the firm's record retention policy; and (5) the disciplinary consequences (including civil and criminal penalties) for non-compliance with the BSA.

We will develop training in our firm, or contract for it. We will review our operations to see if certain employees, such as those in compliance, margin and corporate security, require specialized additional training. Our written procedures will be updated to reflect any such changes.

16. Program to Independently Test AML Program

a. Staffing

The testing of our AML program will be performed every two years by Gustin.

b. Evaluation and Reporting

After we have completed the independent testing, staff will report its findings to senior management. We will promptly address each of the resulting recommendations and keep a record of how each noted deficiency was resolved.

17. Monitoring Employee Conduct and Accounts

We will subject employee accounts to the same AML procedures as customer accounts.

18. Confidential Reporting of AML Non-Compliance


Employees will promptly report any potential violations of the firm's AML compliance program to the AML Compliance Person, unless the violations implicate the AML Compliance Person, in which case the employee shall report to the CEO. Such reports will be confidential, and the employee will suffer no retaliation for making them.

19. Additional Risk Areas

The firm has reviewed all areas of its business to identify potential money laundering risks that may not be covered in the procedures described above.

20. Senior Manager Approval

Senior management has approved this AML compliance program in writing as reasonably designed to achieve and monitor our firm's ongoing compliance with the requirements of the BSA and the implementing regulations under it. This approval is indicated by signatures below.


Signed: Gregory F. Gustin
Title: CEO/President
Date: January 1, 2023