Policy Name	Anti-Money Laundering (AML) Policy
Responsible Party	David Trost
Contact	support@compto.com
Status	Under Review
Effective Date	TBD
Revision Date	February 2025

Compto Public Benefit Corporation Anti-Money Laundering (AML) Program: Compliance and Supervisory Procedures

1. Company Position

It is the policy of Compto Public Benefit Corporation (the "Company") 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 established anti-money laundering regulations, particularly 31 CFR 1022.210 (collectively the "AML Laws").

Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the unlawful proceeds appear to have derived from legitimate origins or constitute legitimate assets. Generally, money laundering occurs in three stages. Cash first enters the financial system at the "placement" stage, where the cash generated from criminal activities is converted into monetary instruments, such as money orders or traveler's checks, or deposited into accounts at financial institutions. At the "layering" stage, the funds are transferred or moved into other accounts or other financial institutions to further separate the money from its criminal origin. At the "integration" stage, the funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses. Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal the origin or intended use of the funds, which will later be used for criminal purposes.

The Company's Anti-Money Laundering ("AML") policies, procedures and internal controls (collectively, the "AML Policy") are designed to address the risks specific to the Company's customers, structure, size, products and services, sales force, distribution channels, transaction processing practices, and other relevant factors. The AML Policy will be reviewed and updated by the designated AML Compliance Officer on a regular basis, at a minimum annually, to ensure appropriate procedures and internal controls are in place to account for both changes in regulations and changes in the Company's business. To accomplish this, the Company will conduct an annual AML risk assessment, or more often if the need arises. The results of the risk assessment will drive improvements in the Company's AML risk management by identifying money laundering risks, assessing how these risks are controlled and mitigated, determining the remaining residual risk and identifying possible enhancements to existing controls, including policies, procedures, and processes.

No part of the Company's AML Policy or Program should be interpreted as contravening or superseding other Legal and/or Regulatory requirements imposed upon the Company. Any conflicts should be escalated to the AML Compliance Officer for review. All exceptions to the Company's AML Policy must be escalated to, reviewed, and approved by the AML Compliance Officer. Key components of the AML Policy include:

1. AML Compliance Officer Designation and Duties
2. AML Training and Education (New Employees, Existing Employees & Agents)
3. Know Your Customer ("KYC")
4. Monitoring Accounts and Reporting Suspicious Activity

2. AML Compliance Officer Designation and Duties

The firm designates David Trost as its Anti-Money Laundering Program Compliance Officer, with full responsibility for the firm's AML program. David Trost is a trained and professionally credentialed Certified Anti-Money Laundering Specialist. The duties of the AML Compliance Officer will include monitoring the firm's compliance with AML obligations and overseeing communication and training for employees. The AML Compliance Officer will also ensure that proper AML records are kept. When warranted, the AML Compliance Officer will ensure Suspicious Activity Reports (SAR SFs) are filed.

The firm will provide NASD with contact information for the AML Compliance Officer, including name, title, mailing address, e-mail address, telephone number and facsimile number. The firm will promptly notify NASD of any change to this information.

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

a. FinCEN Requests Under PATRIOT Act Section 314

Under Treasury's final regulations (published in the Federal Register on September 26, 2002), we will respond to a Financial Crimes Enforcement Network (FinCEN) request about accounts or transactions by immediately searching our records, at our head office or at one of our branches operating in the United States, to determine whether we maintain or have maintained any account for, or have engaged in any transaction with, each individual, entity, or organization named in FinCEN's request. Upon receiving an information request, we will designate one person to be the point of contact regarding the request and to receive similar requests in the future. Unless otherwise stated in FinCEN's request, we are required to search current accounts, accounts maintained by a named suspect during the preceding 12 months, and transactions conducted by or on behalf of or with a named subject during the preceding six months. If we find a match, we will report it to FinCEN by completing FinCEN's subject information form. This form can be sent to FinCEN by electronic mail at sys314a@fincen.treas.gov, or by facsimile transmission to 703-905-3660. If the search parameters differ from those mentioned above (for example, if FinCEN requests longer periods of time or limits the search to a geographic location), we will limit our search accordingly. If we search our records and do not uncover

a matching account or transaction, then we will not reply to a 314(a) request. 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. We will maintain procedures to protect the security and confidentiality of requests from FinCEN, such as those established to satisfy the requirements of Section 501 of the Gramm-Leach-Bliley Act. 3 We will direct any questions we have about the request to the requesting Federal law enforcement agency as designated in the 314(a) request. Unless otherwise stated in the information request, we will not be required to treat the information request as continuing in nature, and we will not be required to treat the request as a list for purposes of the customer identification and verification requirements. We will not use information provided to FinCEN for any purpose other than (1) to report to FinCEN as required under Section 314 of the PATRIOT Act; (2) to determine whether to establish or maintain an account, or to engage in a transaction; or (3) to assist the firm in complying with any requirement of Section 314 of the PATRIOT Act.

b. Sharing Information with Other Financial Institutions

We will share information about those suspected of terrorist financing and money laundering with other financial institutions for the purposes of identifying and reporting activities that may involve terrorist acts or money laundering activities and to determine whether to establish or maintain an account or engage in a transaction. We will file with FinCEN an initial notice before any sharing occurs and annual notices afterwards. We will use the notice form found at https://www.fincen.gov. Before we share information with another financial institution, we will take reasonable steps to verify that the other financial institution has submitted the requisite notice to FinCEN, either by obtaining confirmation from the financial institution or by consulting a list of such financial institutions that FinCEN will make available. We understand that this requirement applies even with respect to financial institutions with whom we are affiliated, and so we will obtain the requisite notices from affiliates and follow all required procedures.

We will employ strict procedures both to ensure that only relevant information is shared and to protect the security and confidentiality of this information, including segregating it from the firm's other books and records and limiting access to this information to the greatest reasonable extent.

4. Checking the Office of Foreign Assets Control ("OFAC") List

Before opening an account, and on an ongoing basis, we will check to ensure that a customer does not appear on Treasury's OFAC "Specifically Designated Nationals and Blocked Persons" List (SDN List) (See the OFAC Web Site at https://ofac.treasury.gov, which is also available through an automated search tool on https://sanctionssearch.ofac.treas.gov/), and is not from, or engaging in transactions with people or entities from, embargoed countries and regions listed on the OFAC Web Site. Because the OFAC Web Site is updated frequently, we will consult the list on a regular basis and subscribe to receive updates when they occur. We may access these lists through various software programs to ensure speed and accuracy. We will also review existing accounts against these lists when they are updated and we will document our review.

In the event that we determine a customer, 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, we will reject the transaction and/or block the customer's assets and file a blocked assets and/or rejected transaction form with OFAC. We will also call the OFAC Hotline at 1-800-540-6322.

5. Customer Identification and Verification

In addition to the information we must collect under FINRA Rules 2010 (Standards of Commercial Honor and Principles of Trade), 2111 (Suitability), and 4510 Series (Books and Records), we have established, documented, and maintained a written Customer Identification Program (or CIP). We will collect certain minimum customer identification information from each customer who opens an account; utilize risk-based measures to verify the identity of each customer who opens an account; record customer identification information and the verification methods and results; provide notice to customers that we will seek identification information and compare customer identification information with government-provided lists of suspected terrorists.

a. Required Customer Information

Prior to opening an account, we will collect the following information for all accounts, if applicable, for any person, entity or organization who is opening a new account and whose name is on the account: the name; date of birth (for an individual); an address, which will be a residential or business street address (for an individual), an Army Post Office ("APO") or Fleet Post Office ("FPO") number, or residential or business street address of next of kin or another contact individual (for an individual who does not have a residential or business street address), or a principal place of business, local office or other physical location (for a person other than an individual); 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).

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

If a potential or existing customer either refuses to provide the information described above when requested, or appears to have intentionally provided misleading information, our firm will not open a new account and, after considering the risks involved, consider closing any existing account. In either case, our AML Compliance Officer will be notified so that we can determine whether we should report the situation to FinCEN (i.e., file a Form SAR-SF).

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. In verifying customer identity, we will analyze any logical inconsistencies in the information we obtain.

We will verify customer identity through documentary evidence, non-documentary evidence, 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 possible. We may also use such non-documentary means, after using documentary evidence, if we are still uncertain about whether we know the true identity of the customer. In analyzing the verification information, we will consider whether there is a logical consistency among the identifying information provided, such as the customer's name, street address, zip code, telephone number, date of birth, and social security number.

Appropriate documents for verifying the identity of customers include, but are not limited to, the following:

> For an individual, an unexpired government-issued identification evidencing nationality, 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:

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

We will use non-documentary methods of verification in the following situations: (1) when the customer is unable to present an unexpired government-issued identification document with a photograph or other similar safeguard; (2) when the firm is unfamiliar with the documents the

customer presents for identification verification; (3) when the customer and firm do not have face-to-face contact; and (4) when there are other circumstances that increase the risk that the firm will be unable to verify the true identity of the customer through documentary means.

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 or terrorist financing activity, we will, after internal consultation with the firm's AML compliance officer, file a SAR-SF in accordance with applicable law and regulation.

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 concern or has been designated as non-cooperative by an international body. We will identify customers that pose a heightened risk of not being properly identified. Therefore, we will 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:

- **Enhanced Documentation Requests:** We may obtain notarized or certified copies of documents that establish the entity's existence and ownership structure, such as articles of incorporation, partnership agreements, trust agreements, or operating agreements. Additionally, we will request a detailed list of officers, directors, or trustees managing the account.
- **Beneficial Ownership Identification:** We may require information about the beneficial owners of the account—individuals who ultimately own or control the entity. Identification documents, such as passports, national IDs, or driver's licenses, will be required for these individuals.
- **Verification of Key Individuals:** We may collect identification and proof of address for individuals with significant authority or control over the account, such as CEOs, CFOs, trustees, partners, or authorized users. This ensures clarity about the individuals who have control over the entity's operations.
- **Third-Party Verification:** We may use independent verification services to confirm the entity's registration status in its home jurisdiction and check whether the entity or its associated individuals have been flagged in anti-money laundering (AML) or politically exposed persons (PEP) databases.
- **Obtain Additional Financial Information:** We may request recent financial statements or proof of financial activity to verify the legitimacy of the entity's business operations and assess whether they align with the customer's claims.
- **Enhanced Screening:** We may cross-check customer information against global sanction

lists, high-risk country designations, and negative media databases. Additionally, we will implement more frequent monitoring of transactions to identify unusual patterns.

- **Written Certifications:** We may require a signed certification from individuals with authority over the account, confirming the accuracy and completeness of the information provided.

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: (A) not open an account; (B) impose terms under which a customer may conduct transactions while we attempt to verify the customer's identity; (C) close an account after attempts to verify customer's identity fail; and (D) file a SAR-SF in accordance with applicable law and regulation.

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 discrepancy in the identifying information. 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 maintain 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 and Other Criminals

From time to time, we may receive notice that a Federal government agency has issued a list of known or suspected terrorists. 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), we will 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 with Treasury's Office of Foreign Asset Control 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 provide the following notice to customers online via our website or our mobile application.

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.

What this means for you: When you open an account, we will ask for your name, address, date of birth and other information that will allow us to identify you. We may also ask to see your driver's license or other identifying documents.

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 customer identification program 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. Foreign Correspondent Accounts and Foreign Shell Banks

a. Detecting and Closing Correspondent Accounts of Unregulated Foreign Shell Banks

We will detect correspondent accounts (any account that permits the foreign financial institution to engage in securities or futures transactions, funds transfers, or other types of financial transactions) for unregulated foreign shell banks using a comprehensive due diligence process that includes verifying the foreign financial institution's licensing and regulatory status against reputable government and international registries, reviewing public and commercial databases for any indication of shell bank characteristics (e.g., no physical presence, unknown beneficial ownership, or questionable business purpose), requiring formal certifications or attestations from the foreign institution regarding its regulatory oversight, and continuously monitoring account activity, transaction patterns, and changes in beneficial ownership to promptly identify and flag any potential shell bank relationships. Upon finding or suspecting such accounts, firm employees will notify the AML Compliance Officer, who will terminate any verified correspondent account in the United States for an unregulated foreign shell bank. We will also terminate any correspondent account that we have determined is not maintained by an unregulated 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.

b. Certifications

We will require our foreign bank account holders to complete model certifications issued by the Treasury. We will send the certification forms to our foreign bank account holders for completion, which requires them to certify that they are not shell banks and to provide ownership and agent information. We will re-certify when we believe that the information is no longer accurate and at least once every three years.

c. Recordkeeping for Foreign Correspondent Accounts

We will keep records identifying the owners of foreign banks with U.S. correspondent accounts and the name and address of the U.S. agent for service of legal process for those banks.

d. Summons or Subpoena of Foreign Bank Records; Termination of Correspondent Relationships.

When we receive a written request from a federal law enforcement officer for information concerning correspondent accounts, we will provide that information to the requesting officer not later than 7 days after receipt of the request. We will close, within 10 days, any account for a bank that we learn from Treasury or the Department of Justice has failed to comply with a summons or has contested a summons. We will scrutinize any account activity during that 10-day period to ensure that any suspicious activity is appropriately reported and to ensure that no new positions are established in these accounts.

7. Private Banking Accounts/Foreign Officials

We do not open or maintain private banking accounts and, to prevent any attempts to do so, we have implemented strict internal controls that include explicit instructions in our new account procedures to flag any account request that meets or exceeds the $1,000,000 minimum deposit threshold, involves non-U.S. persons, or exhibits characteristics consistent with a "private banking" relationship as defined by our policies. All prospective accounts that trigger these red flags are immediately escalated to a senior compliance officer and subjected to enhanced scrutiny. We also conduct ongoing training for customer-facing personnel to recognize requests that may constitute a private banking account, and we utilize automated monitoring systems to identify patterns or conditions indicative of such accounts. If any attempt is detected, the account opening process is immediately halted, and senior management is notified.

8. Monitoring Accounts for Suspicious Activity

We will manually monitor a sufficient amount of account activity to permit identification of patterns of unusual size, volume, pattern or type of transactions, geographic factors such as whether jurisdictions designated as "non-cooperative" are involved, or any of the "red flags" identified in Section 8. b. below. We will look at transactions, including 16 trading and wire transfers, in the context of other account activity to determine if a transaction lacks financial sense or is suspicious because it is an unusual transaction or strategy for that customer. The AML Compliance Officer or his or her designee will be responsible for this monitoring, will document when and how it is carried out, and will report suspicious activities to the appropriate authorities. Among the information we will use to determine whether to file a Form SAR-SF are exception reports that include transaction size, location, type, number, and nature of the activity. We will create employee guidelines with examples of suspicious money laundering activity and lists of high-risk clients whose accounts may warrant further scrutiny. Our AML Compliance Officer will conduct an appropriate investigation before a SAR is filed. Our monitoring of specific transactions includes regular manual reviews of customer account activity logs, the application of pre-established transaction thresholds (e.g., dollar amount, frequency, volume) that trigger additional scrutiny, and the use of internal watchlists or screening tools to identify activity linked to high-risk geographic regions, entities, or counterparties. We will cross-reference incoming and outgoing funds, verify the legitimacy of counterparties where feasible, and closely review any transactions that appear out of alignment with the customer's known business profile, anticipated activity levels, or stated source of funds. Additionally, we will compare identified transactions against established red-flag indicators—such as unusually large wire transfers, repeated incoming wires from known tax havens, or patterns suggestive of layering—documenting all findings and escalating suspicious cases to the AML Compliance Officer for further investigation and potential SAR filing.

a. Emergency Notification to the Government by Telephone

When conducting due diligence or opening an account, we will immediately call Federal law enforcement when necessary, and especially in these emergencies: a legal or beneficial account holder or person with whom the account holder is engaged in a transaction is listed on or located in a country or region 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, we have reason to believe the customer is trying to move illicit cash out of the government's reach, or we have reason to believe the customer is about to use the funds to further an act of terrorism. We will first call the OFAC Hotline at 1-800-540-6322. The other contact numbers we will use are: Financial Institutions Hotline (1-866-556-3974), local U.S. Attorney's Office (1-512-916-5858), and local FBI Office (1-210-225-6741).

b. Red Flags

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

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

- The customer's account has unexplained or sudden extensive wire activity, especially in accounts that had little or no previous activity.
- The customer's account shows numerous currency or cashiers check transactions aggregating to significant sums.
- The customer's account has a large number of wire transfers to unrelated third parties inconsistent with the customer's legitimate business purpose.
- The customer's account has wire transfers that have no apparent business purpose to or from a country identified as a money laundering risk or a bank secrecy haven.
- The customer's account indicates large or frequent wire transfers, immediately withdrawn by check or debit card without any apparent business purpose.
- The customer makes a funds deposit followed by an immediate request that the money be wired out or transferred to a third party, or to another firm, without any apparent business purpose.
- The customer makes a funds deposit for 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.
- The customer engages in excessive journal entries between unrelated accounts without any apparent business purpose.
- The customer requests that a transaction be processed to avoid the firm's normal documentation requirements.
- The customer, 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 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.)
- The customer's account shows an unexplained high level of account activity with very low levels of securities transactions.
- The customer maintains multiple accounts, or maintains accounts in the names of family members or corporate entities, for no apparent purpose.
- The customer's account has inflows of funds or other assets well beyond the known income or resources of the customer.

c. Responding to Red Flags and Suspicious Activity

When a member of the firm detects any red flag he or she will investigate further under the direction of the AML Compliance Officer. This may include gathering additional information internally or from third-party sources, contacting the government, freezing the account, or filing a Form SAR-SF.

9. Suspicious Transactions and BSA Reporting

a. Filing a Form SAR-SF

We will file Form SAR-SFs for any account activity (including deposits and transfers) conducted or attempted through our firm involving (or in the aggregate) $5,000 or more of funds or assets 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 we know, after examining the background, possible purpose of the transaction and other facts, of no reasonable explanation for the transaction, or 4) the transaction involves the use of the firm to facilitate criminal activity.

We will not base our decision on whether to file a SAR-SF solely on whether the transaction falls above a set threshold. We will file a SAR-SF and notify law enforcement of all transactions that raise an identifiable suspicion of criminal, terrorist, or corrupt activities. In high-risk situations, we will notify the government immediately (See Section 8 for contact numbers) and will file a SAR-SF with FinCEN. Securities law violations that are reported to the SEC or a Self-Regulatory Organization (SRO) may also be reported promptly to the local U.S. Attorney, as appropriate.

We will not file SAR-SFs to report violations of Federal securities laws or SRO rules by our employees or registered representatives that do not involve money laundering or terrorism, but we will report them to the SEC or SRO.

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

We will report suspicious transactions by completing a SAR-SF and we will collect and maintain supporting documentation as required by the BSA regulations. We will file a SAR-SF no later than 30 calendar days after the date of the initial detection of the facts 20 that constitute a basis for filing a SAR-SF. If no suspect is identified on the date of initial detection, we may delay filing the SAR-SF for an additional 30 calendar days pending identification of a suspect, but in no case, will the reporting be delayed more than 60 calendar days after the date of initial detection.

We will retain copies of any SAR-SF 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, or federal or state securities regulators, 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-SF or the information contained in the SAR SF, except where

disclosure is requested by FinCEN, the SEC, or another appropriate law enforcement or regulatory agency or an SRO registered with the SEC, will decline to produce to the SAR-SF or to provide any information that would disclose that a SAR-SF was prepared or filed. We will notify FinCEN of any such request and our response.

b. Currency Transaction Reports (CTR)

Our firm prohibits the receipt of currency and has the following procedures to prevent its receipt: All transactions are conducted electronically through our platform, which only supports digital payment methods such as ACH transfers, wire transfers, and digital wallet services. Our platform does not provide any functionality to accept cash deposits or facilitate transactions involving physical currency. We explicitly state this policy in our terms of service, user agreements, and onboarding materials. Additionally, our system is designed to reject any attempted deposit or payment not originating from an approved electronic payment method. Customer service teams are trained to identify and report any inquiries or attempts to circumvent this policy. Any instances of unauthorized receipt of currency are escalated immediately to our compliance team for investigation and appropriate action. If we discover currency has been received, we will file with FinCEN CTRs for transactions involving currency that exceed $10,000. Multiple transactions will be treated as a single transaction if they total more than $10,000 during any one business day.

c. Currency and Monetary Instrument Transportation Reports (CMIR)

Our firm prohibits the receipt of currency and has the procedures described in the previous subsection to prevent its receipt. If we discover currency has been received, we will file with the Commissioner of Customs a CMIR whenever the firm transports, mails, ships or receives or causes or attempts to transport, mail, ship or receive monetary instruments of more than $10,000 at one time (on one calendar day or, if for the purposed of evading the reporting requirements, on one or more days) in or out of the U.S. We will file a CMIR for all such shipments or receipts of monetary instruments, except for currency or monetary instruments shipped or mailed through the postal service or by common carrier. We will, however, file a CMIR for such receipts of currency and monetary instruments and for shipments and deliveries made by the firm by means other than the postal service or common carrier, even when such shipment or transport is made by the firm to an office of the firm located outside the U.S.

d. Foreign Bank and Financial Accounts Reports (FBAR)

We will file with FinCEN an 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. Transfers of $3,000 or More Under the Joint and Travel Rule

When we transfer funds of $3,000 or more, we will record on the transmittal order at least the following information: the name and address of the transmitter and recipient, the amount

of the transmittal order, the identity of the recipient's financial institution, and the account number of the recipient. We will also verify the identity of transmitters and recipients who are not established customers of the firm (i.e., customers of the firm who have not previously maintained an account with us or for whom we have not obtained and maintained a file with the customer's name, address, taxpayer identification number, or, if none, alien identification number or passport number and country of issuance).

10. AML Record Keeping

a. SAR-SF Maintenance and Confidentiality

We will hold SAR-SFs and any supporting documentation confidential. We will not inform anyone outside of a law enforcement or regulatory agency or securities regulator about a SAR-SF. We will refuse any subpoena requests for SAR-SFs or SAR-SF information and immediately tell FinCEN of any such subpoena we receive. We will segregate SAR-SF filings and copies of supporting documentation from other firm books and records to avoid disclosing SAR-SF filings. Our AML Compliance Officer will handle all subpoenas or other requests for SAR-SFs. We will share information with our clearing broker about suspicious transactions in order to determine when a SAR-SF should be filed. As mentioned earlier, we may share with the clearing broker a copy of the filed SAR-SF – unless it would be inappropriate to do so under the circumstances, such as where we file a SAR-SF concerning the clearing broker or its employees.

b. Responsibility for AML Records and SAR Filing

Our AML Compliance Officer and his or her designee will be responsible to ensure that AML records are maintained properly and that SARs are filed as required.

c. Records Required

As part of our AML program, our firm will create and maintain SAR SFs, CTRs, CMIRs, FBARs, and relevant documentation on customer identity and verification (See Section 5 above) and funds transfers and transmittals as well as any records related to customers listed on the OFAC list. We will maintain SAR-SFs and their accompanying documentation for at least five years. We will keep other documents according to existing BSA and other record keeping requirements, including certain SEC rules that require six-year retention.

11. Clearing/Introducing Firm Relationships

We will work closely with our clearing firm to detect money laundering. We will exchange information, records, data and exception reports as necessary to comply with AML laws. Both our firm and our clearing firm have filed (and kept undated) the necessary annual certifications for such information sharing. As a general matter, we have agreed that our clearing firm will monitor customer activity on our behalf, and we will provide our clearing firm with proper customer identification information as required to successfully monitor customer transactions.

We have allocated these functions and set them forth in a written document. We understand that the allocation of functions will not relieve either of us from our independent obligation to comply with AML laws, except as specifically allowed under the PATRIOT Act and its implementing regulations.

12. Training Programs

We will develop ongoing employee training under the leadership of the AML Compliance Officer 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. Our training will include, at a minimum: how to identify red flags and signs of money laundering that arise during the course of the employees' duties; what to do once the risk is identified; what employees' roles are in the firm's compliance efforts and how to perform them; the firm's record retention policy; and the disciplinary consequences (including civil and criminal penalties) for non-compliance with the PATRIOT Act. We will develop training in our firm, or contract for it. Delivery of the training may include educational pamphlets, videos, intranet systems, in-person lectures, and explanatory memos. Currently our training program is: "all registered representatives must complete the Udemy course entitled *Anti Money Laundering / Combating Terrorism Financing* within two weeks of being hired". We will maintain records to show the persons trained, the dates of training, and the subject matter of their training.

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

13. Program to Test AML Program

a. Staffing

The testing of our AML program will be performed by Connor Funk, one of the personnel of our firm. To ensure that they remain independent, we will separate their functions from other AML activities by ensuring that Connor Funk does not participate in the day-to-day implementation, monitoring, or enforcement of AML policies and procedures. Connor Funk will not be involved in transaction monitoring, SAR filings, or client onboarding processes. Additionally, their role will report directly to a senior executive outside of the compliance department to avoid any influence from individuals responsible for AML operations.

b. Evaluation and Reporting

After we have completed the testing, staff will report its findings to senior management. We will address each of the resulting recommendations.

14. Monitoring Employee Conduct and Accounts

We will subject employee accounts to the same AML procedures as customer accounts, under the supervision of the AML Compliance Officer. We will also review the AML performance of supervisors, as part of their annual performance review.

15. Confidential Reporting of AML Non-Compliance

Employees will report any violations of the firm's AML compliance program to the AML Compliance Officer. Such reports will be confidential, and the employee will suffer no retaliation for making them.

16. Senior Manager Approval

I have approved this AML program as reasonably designed to achieve and monitor our firm's ongoing compliance with the requirements of the AML Laws

Signed:
Name:
Title:
Date:

Revisions

Revision	Revision Date	Effective Date	Description of Changes	Approved By
v1.0	January 2025	January 2025	Initial Release	David Trost
v1.1	February 2025	TBD	- Switch to md - fix typos - add revisions	