# RaiseFX Detailed Anti-Money Laundering (AML) Program: Compliance and Supervisory Procedures

---


**1. RaiseFx Policy** **2**

**2. AML Compliance Person Designation and Duties** **3**

**3. Giving AML Information to Regulatory Bodies** **4**

**4. Customer Identification Program** **4**

b. Customers Who Refuse to Provide Information 5

c. Verifying Information 5

f. Notice to Customers 8

**7. Monitoring Accounts for Suspicious Activity** **9**

Emergency Notification to Law Enforcement by Telephone 9

Red Flags 9

8. **Potential Red Flags in Customer Due Diligence/ Interactions with Customers** **10**

**9. Potential Red Flags in Securities Trading** **12**

**10/ Potential Red Flags in Money Movements** **14**

**11. Other Potential Red Flags** **17**

c.Responding to Red Flags and Suspicious Activity 18

**12. Suspicious Transactions and Reporting** **18**

**13. AML Recordkeeping** **20**

Responsibility for Required AML Records and Filings 20

Filings Maintenance and Confidentiality 20

Additional Records 21

**15. Training Programs** **22**

**16. Program to Independently Test AML Program** **22**

**17. Monitoring Employee Conduct and Accounts** **23**

# RaiseFX Detailed Anti-Money Laundering (AML) Program: Compliance and Supervisory Procedures

---

**18. Confidential Reporting of AML Non-Compliance** 23

**19. Additional Risk Areas** 23

**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. At this stage, no other risk has been identified.** 23

**20. Senior Manager Approval** 23

## 1. RaiseFx 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 international requirements.

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.

Although cash is rarely deposited into securities accounts, the securities industry is unique in that it can be used to launder funds obtained elsewhere, and to generate illicit funds within the industry itself through fraudulent activities. Examples of types of

fraudulent activities include insider trading, market manipulation, ponzi schemes, cybercrime and other investment-related fraudulent activity.

Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal either the origin of the funds or their intended use, which could be for criminal purposes. Legitimate sources of funds are a key difference between terrorist financiers and traditional criminal organizations. In addition to charitable donations, legitimate sources include foreign government sponsors, business ownership and personal employment. Although the motivation differs between traditional money launderers and terrorist financiers, the actual methods used to fund terrorist operations can be the same as or similar to methods used by other criminals to launder funds. Funding for terrorist attacks does not always require large sums of money and the associated transactions may not be complex.

Our AML policies, procedures and internal controls are designed to ensure compliance with all applicable regulations 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 David Bottin as its Anti-Money Laundering Program Compliance Person (AML Compliance Person), with full responsibility for the firm's AML program.

David Bottin has a working knowledge of the AML regulations and its implementing regulations and is qualified by experience, knowledge and training, including extensive experience in the brokerage industry.

The duties of the AML Compliance Person will include monitoring the firm's compliance with AML obligations, overseeing communication and training for employees.

The AML Compliance Person will also ensure that the firm keeps and maintains all of the required AML records and will ensure that Suspicious Activity Reports (SARs) are filed with the relevant authorities. The AML Compliance Person is vested with full responsibility and authority to enforce the firm's AML program.

# RaiseFX Detailed Anti-Money Laundering (AML) Program: Compliance and Supervisory Procedures

## 3. Giving AML Information to Regulatory Bodies

RaiseFx will supply all relevant information to regulatory bodies.

It will also voluntarily provide information to the relevant regulatory bodies when a suspicious activity is detected.

## 4. Customer Identification Program

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 the required adequate CIP notice to customers that we will seek identification information to verify their identities.

We will collect information to determine whether any entity opening an account would be excluded as a "customer," .

### a. Required Customer Information

At the opening of an account, David Bottin 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).

If the full information is not received within 3 weeks, we will cancel the account. All operations will be forbidden and all funds will be blocked until we receive the full information.

In the event that a customer has applied for, but has not received, a taxpayer identification number, we will ensure with the customer 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**

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 Person will be notified so that we can determine whether we should report the situation to the relevant authorities.

**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. David Bortin 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 source;

- 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 complaint 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 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, by calling the customer directly.

### 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 depending on the specific situation : (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 complaint 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. Notice to Customers

We will provide notice to customers that the firm is requesting information from them to verify their identities, as required by international laws. We will provide this information on our website and by email.

# RaiseFX Detailed Anti-Money Laundering (AML) Program: Compliance and Supervisory Procedures

## 6. Customer Due Diligence Rule

We do not open or maintain accounts for legal entity customers. 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 procedures.

We will conduct ongoing monitoring to identify and report suspicious transactions and, on a risk basis, maintain and update customer information, including information regarding the beneficial ownership of legal entity customers, using the customer risk profile as a baseline against which customer activity is assessed for suspicious transaction reporting. Our suspicious activity monitoring procedures are detailed below.

## 7. 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. Monitoring will be conducted through our CRM system. The customer risk profile will serve as a baseline for assessing potentially suspicious activity. The AML Compliance Person or his or her designee will be responsible for this monitoring, will review any activity that our monitoring system detects, will determine whether any additional steps are required, will document when and how this monitoring is carried out, and will report suspicious activities to the appropriate authorities.

We will document our monitoring and reviews in a specific document. The AML Compliance Person or his or her designee will conduct an appropriate investigation and review relevant information from internal or third-party sources before a complaint 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.

### b. Red Flags

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 company[10] 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.

**Potential Red Flags in Securities Trading**

- 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.)

- There is a sudden spike in investor demand for, coupled with a rising price in, a thinly traded or low-priced security.

- The customer's activity represents a significant proportion of the daily trading volume in a thinly traded or low-priced security.

- A customer buys and sells securities with no discernable purpose or circumstances that appear unusual.

- Individuals known throughout the industry to be stock promoters sell securities through the broker-dealer.

- A customer accumulates stock in small increments throughout the trading day to increase price.

- A customer engages in pre-arranged or other non-competitive securities trading, including wash or cross trades, with no apparent business purpose.

- A customer attempts to influence the closing price of a stock by executing purchase or sale orders at or near the close of the market.

- A customer engages in transactions suspected to be associated with cyber breaches of customer accounts, including potentially unauthorized disbursements of funds or trades.

- A customer engages in a frequent pattern of placing orders on one side of the market, usually inside the existing National Best Bid or Offer (NBBO), followed by the

customer entering orders on the other side of the market that execute against other market participants that joined the market at the improved NBBO (activity indicative of "spoofing").

- A customer engages in a frequent pattern of placing multiple limit orders on one side of the market at various price levels, followed by the customer entering orders on the opposite side of the market that are executed and the customer cancelling the original limit orders (activity indicative of "layering").

- Two or more unrelated customer accounts at the firm trade an illiquid or low-priced security suddenly and simultaneously.

- The customer makes a large purchase or sale of a security, or option on a security, shortly before news or a significant announcement is issued that affects the price of the security.

- The customer is known to have friends or family who work at or for the securities issuer, which may be a red flag for potential insider trading or unlawful sales of unregistered securities.

- The customer's purchase of a security does not correspond to the customer's investment profile or history of transactions (*e.g.*, the customer may never have invested in equity securities or may have never invested in a given industry, but does so at an opportune time) and there is no reasonable explanation for the change.

- The account is using a master/sub structure, which enables trading anonymity with respect to the sub-accounts' activity, and engages in trading activity that raises red flags, such as the liquidation of microcap issuers or potentially manipulative trading activity.

- The firm receives regulatory inquiries or grand jury or other subpoenas concerning the firm's customers' trading.

- The customer engages in a pattern of transactions in securities indicating the customer is using securities to engage in currency conversion. For example, the customer delivers in and subsequently liquidates American Depository Receipts (ADRs) or

dual currency bonds for U.S. dollar proceeds, where the securities were originally purchased in a different currency.

- The customer engages in mirror trades or transactions involving securities used for currency conversions, potentially through the use of offsetting trades.
- The customer appears to buy or sell securities based on advanced knowledge of pending customer orders.

**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.
- 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 nostro[14] 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 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 the AML Compliance Person. 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 complaint.

## 12. Suspicious Transactions and Reporting

We will file complaints to the relevant authorities 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 notify the appropriate law enforcement authority in situations involving violations that require immediate attention, such as terrorist financing or ongoing money laundering schemes.

We will not notify any person involved in the transaction that the transaction has been reported.

When we are the transmittor's financial institution in funds of $3,000 or more, we will retain either the original or a copy of the transmittal order. We will also record on the transmittal order the following information: (1) the name and address of the transmittor; (2) if the payment is ordered from an account, the account number; (3) the amount of the transmittal order; (4) the execution date of the transmittal order; and (5) the identity of the recipient's financial institution. In addition, we will include on the transmittal order as many of the following items of information as are received with the transmittal order: (1) the name and address of the recipient; (2) the account number of the recipient; (3) any other specific identifier of the recipient; and (4) any form relating to the transmittal of funds that is completed or signed by the person placing the transmittal order.

We will also verify the identity of the person placing the transmittal order (if we are the transmitting firm), provided the transmittal order is placed in person and the transmittor is not an established customer of the firm (*i.e.*, a customer of the firm who has 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). If a

transmittor or recipient is conducting business in person, we will obtain: (1) the person's name and address; (2) the type of identification reviewed and the number of the identification document (*e.g.,* driver's license); and (3) the person's taxpayer identification number (*e.g.,* Social Security or employer identification number) or, if none, alien identification number or passport number and country of issuance, or a notation in the record the lack thereof. If a transmittor or recipient is not conducting business in person, we shall obtain the person's name, address, and a copy or record of the method of payment (*e.g.,* check or credit card transaction). In the case of transmittors only, we shall also obtain the transmittor's taxpayer identification number (*e.g.,* Social Security or employer identification number) or, if none, alien identification number or passport number and country of issuance, or a notation in the record of the lack thereof. In the case of recipients only, we shall obtain the name and address of the person to which the transmittal was sent.

## 13. AML Recordkeeping

### a. Responsibility for Required AML Records and Filings

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

In addition, as part of our AML program, our firm will create and maintain filings and and relevant documentation on customer identity and verification and funds transmittals. We will maintain filings and their accompanying documentation for at least five years. We will keep other documents and other recordkeeping requirements according to international laws.

### b. Filings Maintenance and Confidentiality

We will hold filings and any supporting documentation confidential. We will not inform anyone outside of appropriate law enforcement or regulatory agency.

We will segregate filings and copies of supporting documentation from other firm books and records to avoid disclosing filings. Our AML Compliance Person will handle all subpoenas or other requests for filings. We may share information with another financial

institution about suspicious transactions in order to determine whether we will jointly file a filing.

### 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

- A record of each advice, request or instruction given to another financial institution (which includes broker-dealers) or other person 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

- Each document granting signature or trading authority over each customer's account;

- 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

- 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

# RaiseFX Detailed Anti-Money Laundering (AML) Program: Compliance and Supervisory Procedures

## 14. 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, filings of complaints); (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.

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 through in person and recorded presentation. 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.

## 15. Program to Independently Test AML Program

The testing of our AML program will be performed at least annually by a person who is not the Compliance Person and does not report to him/her.

Findings will be reported to senior management [*or to an internal audit committee*]. We will promptly address each of the resulting recommendations and keep a record of how each noted deficiency was resolved.

# RaiseFX Detailed Anti-Money Laundering (AML) Program: Compliance and Supervisory Procedures

## 16. 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 Person. We will also review the AML performance of supervisors, as part of their annual performance review. The AML Compliance Person's accounts will be reviewed by the Company Director or a key shareholder.

## 17. 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.

## 18. 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. At this stage, no other risk has been identified.

## 19. 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: David BOTTIN

Title: CEO

Date: 13th April 2022