

# [ADINATH STOCK BROKING PVT LTD]

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

---

### **1. Firm Policy**

It is the policy of the firm to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities. 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.

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

The firm designates [Vijay Ginodiya] as its Anti-Money Laundering Program Compliance Officer, with full responsibility for the firm's AML program. [Vijay Ginodiya] is qualified by experience, knowledge and training, The duties of the AML Compliance Officer will include monitoring the firm's compliance with AML obligations, 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 [Vijay Ginodiya ] will ensure Suspicious Activity Reports (SAR-) are filed.

The firm will provide FIU-IND 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 FIU-IND of any change to this information.

### **3. Giving AML Information to FIU-IND and Other Financial Institutions**

Under FIU-IND's final regulations , we will respond to a FIU-IND request about accounts or transactions by immediately searching our records, at our head office, 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 FIU-IND 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 FIU-IND'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 FIU-IND by completing FIU-IND's subject information form. This form can be sent to FIU-IND by facsimile transmission.

We will not disclose the fact that FIU-IND 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 FIU-IND, such as those established to satisfy the requirements of PMLA 2002.

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 FIU-IND for any purpose other than (1) to report to FIU-IND as required under PMLA 2002; (2) to determine whether to establish or maintain an account, or to engage in a transaction;

#### **a. 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 FIU-IND an initial notice before any sharing occurs and annual notices afterwards. 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 FIU-IND, either by obtaining confirmation from the financial institution or by consulting a list of such financial institutions that FIU-IND 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.

In addition to sharing information with other financial institutions about possible terrorist financing and money laundering, we will also share information about particular suspicious transactions with our clearing broker for purposes of determining whether one of us will file a STR. In cases in which we file a STR for a transaction that has been handled both by us and by the clearing broker, we may share with the clearing broker a copy of the filed STR, unless it would be inappropriate to do so under the circumstances, such as where we filed a STR concerning the clearing broker or one of its employees.

#### **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, and is not from, or engaging in transactions with people or entities from, embargoed countries.

In the event that we determine a customer, or someone with or for whom the customer is transacting, is or from or engaging in transactions with a person or entity located in an embargoed country or region, we will reject the transaction

## **5. Customer Identification and Verification**

*Note that this regulation applies only to "customers" who open new "accounts" with a the firm. A "customer" is defined as (1) a person that opens a new account or (2) an individual who opens a new account for an individual who lacks legal capacity or for an entity that is not a legal person. ("Customer" does not refer to persons who fill out account opening paperwork or who provide information necessary to establish an account, if such persons are not the accountholder as well. The definition of "customer" also does not include persons with authority over accounts.)*

*The following entities, however, are excluded from the definition of "customer:" a financial institution regulated by a Reserve Bank of India or a Company regulated by Companies Act; any entity established under the laws of the India, and a person that has an existing account with the Firm, provided that the firm/company has a reasonable belief that it knows the true identity of the person.*

*Company will not be required to verify the identities of persons with existing accounts at the firm, as long as the company has a reasonable belief that it knows the true identity of the customer.*

*For purposes of this rule, an "account" is defined as a formal relationship with a firm/company established to effect transactions in securities, including, but not limited to, the purchase or sale of securities, and the holding of securities for safekeeping or as collateral.*

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 address (for an individual), an 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 (PAN) or one or more of the following:; passport number and country of issuance.*

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 FIU-IND(i.e., file a Form STR).

## **b. 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 (if provided), date of birth, and Permanent account 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, 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 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 STR 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 law 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:

#### **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 STR 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 have been closed; we will retain records made about verification of the customer's identity for TEN 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 PMLA We will use the following method to provide notice to customers: *[describe notice you will provide for each method of account-opening your firm uses (i.e., telephone, online, walk-in, etc.); the final rule provides the following sample language for notice to be provided to a firm's customers, if appropriate:*

**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 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 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.

**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 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: *[describe.]*

- 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**

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) 10,000 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 the 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 and will file a SAR-SF with FIU IND.

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 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 FIU IND, 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 FIU IND, 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 FIU IND of any such request and our response.

*l*

## **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 FIU IND 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, and relevant documentation on customer identity and verification and funds transfers and transmittals as well as any records related to customers listed on the OFAC list. 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. 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 FIU IND.

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. 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 PARESH RUNWAL, personnel of our firm. Their qualifications include C.A To ensure that they remain independent, we will separate their functions from other AML activities

#### **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. The AML Compliance Officer's accounts will be reviewed by [PARESH RUNWAL – *MANAGING DIRECTOR*.]

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

Employees will report any violations of the firm's AML compliance program to the AML Compliance Officer, unless the violations implicate the Compliance Officer, in which case the employee shall report to [PARESH RUNWAL]. Such reports will be confidential, and the employee will suffer no retaliation for making them.

#### **16. Additional Areas of Risk**

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.

#### **17. 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 BSA and the implementing regulations under it.

Signed: Paresh Runwal

Title: Managing Director