Nilfee Anti-Money Laundering Policy Statement & Evaluation Procedures

Compliance and Supervisory Procedures

for Nilfee, Inc

447 Broadway, 2nd Floor Suite #466, New York, New York 10013, United States

https://nilfee.com/

1. Company Anti-Money Laundering Policy Statement

Nilfee, Inc has a strict policy against and actively works to prevent money laundering, as well as any activities that aid money laundering, terrorism financing, or criminal endeavors.

Money laundering is broadly described as participating in actions designed to hide or alter the true source of unlawfully acquired proceeds, making them appear to come from legitimate sources or constitute lawful assets. Typically, money laundering unfolds in three phases:

- **Placement:** Illicitly generated cash is converted into monetary instruments like money orders or traveler's checks, digital money, crypto assets, or it is deposited into financial institution accounts.

- **Layering:** Funds are moved or transferred to other accounts or financial institutions, enhancing the separation between the money and its criminal origins.

- **Integration:** Funds are reintroduced into the economic system, used to acquire lawful assets, or employed to finance other criminal activities or legitimate businesses. While terrorist financing may not always involve the proceeds of criminal activities, it often entails attempts to conceal the funds' origin or intended use, which will later be directed toward criminal purposes.

2. AML Compliance Officer Designation and Duties

As required under the USA Patriot Act of 2001 (PATRIOT Act), the Company designates AMLCO (Anti-Money Laundering Program Compliance Officer), with full responsibility for the Company's anti-money laundering (AML) program. The AML Compliance Officer will also ensure that proper AML records are kept. When warranted, the AML Compliance Officer will ensure Suspicious Activity Reports are filed with the Financial Crimes Enforcement Network (FinCEN) or the Company's designated self-regulatory agency (DSRO).

3. Sharing AML Information with Federal Law Enforcement Agencies and Other Financial Institutions

Under the U.S. Treasury's final regulations (published in the Federal Register on September 26, 2002), we will respond to any FinCEN request about accounts or transactions by immediately searching our records to determine whether we maintain or have maintained any account for, or have engaged in any transaction with, each individual, entity, or organization named in FinCEN's request. Upon receiving an information request, the AMLCO is to be responsible regarding the request and similar requests in the future. Unless otherwise stated in FinCEN's request, we are required to search current accounts and transactions, 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 in a timely manner. If we search our records and do not uncover a matching account or transaction, then we will not reply as allowed under Section 314(a) of the PATRIOT Act.

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, as required by Section 501 of the Gramm-Leach-Bliley Act. 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 Company in complying with any requirement of Section 314 of the PATRIOT Act.

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 an initial notice with FinCEN before any sharing occurs and annual notices afterwards.

We will use the notice form found at http://www.fincen.gov or use a paper notification mailed to FinCEN, P.O. Box 39, Mail Stop 100, Vienna, VA 22183. 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.

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

Before engaging in any money service activity (including but not limited to ACH transfers, Debit or Credit Card payments, check cashing, money orders, Crypto deposits and wire transfers) which potentially may involve money laundering, and on an ongoing basis, we will check to ensure that a customer does not appear on the Treasury's OFAC “Specifically Designated Nationals and Blocked Persons” List, SDN List, and is not from, or engaging in transactions with people or entities from, embargoed countries and regions listed on the OFAC website (see https://home.treasury.gov/).

Because the OFAC Website is updated frequently, we will consult the list on a regular basis and subscribe to receive updates when they occur. We may, if necessary, 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 may also call the OFAC Hotline at 1-800-540-6322.

5. Customer Identification and Verification

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 engages in any money service activity with the Company; utilize risk-based measures to verify the identity of each customer who engages in any money service activity; 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 as mentioned above in Section 3.

A. Required Customer Information

Prior to engaging in any money service activity which potentially may involve money laundering, we will collect the following information for all customers: the name; an address, (which will be a residential or business street address for an individual), email verification, phone number, In -APP KYC upload (Driving License/ Passport/ Equivalent Government Issued ID/ Tax ID), Banking Details, Selfie with KYC Document (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).

We will refuse any money service transaction in the event that a customer has applied for, but has not received a taxpayer identification number and cannot prove his/her identity to the satisfaction of the AMLCO. All the above documents will also be verified through third party KYC verification tools or Account linking tools. If successful, the users will be given verified tick in their profile else the customer KYC will be rejected and restricted from any of our services. If needed we will block the user access and report it to FinCEN.

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, the Company will not conduct any further money service transactions with that entity. 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-MSB).

C. Verification of 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 nondocumentary 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, User’s IP address, User’s Mobile device ID 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, Bank Account Information and bearing a photograph or similar safeguard, such as a driver's license or passport; and
- For an entity, 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. However, if 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 may use any or all of 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, employer, or other source;
- Checking references with financial institutions;

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 Company is unfamiliar with the documents the customer presents for identification verification; (3) when there are other circumstances that increase the risk that the Company will be unable to verify the true identity of the customer through documentary means.

We will verify the information within a reasonable time before a transaction is completed. Depending on the nature of the requested transaction, 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-MSB in accordance with applicable law and regulation.

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 perform any money service transaction; (B) impose terms under which a customer may conduct transactions while we attempt to verify the customer's identity; (C) file a SAR-MSB 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 and readily accessible for the first two years. We will retain records made about verification of the customer's identity for five years after the record is made.

We will continue to comply with Treasury's OFAC rules prohibiting transactions with certain foreign countries or their nationals as mentioned in Section 3.

G. Notice to Customers

We will provide notice to customers that the Company is requesting information from them to verify their identities, as required by Federal law. We will give notice to customers regarding the policy either verbally or as a plainly posted notice such as:

In compliance with Federal law aimed at combating the funding of terrorism and money laundering, we are obligated to collect, verify, and document information identifying every individual involved in domestic or cross border payments, merchant payments, wiring funds, or utilizing other financial services at this establishment. We will request details such as your name, address, and other pertinent information to ensure proper identification. Additionally, we may require the presentation of your driver's license or other relevant identifying documents.

H. Reliance on another Financial Institution for Identity Verification

Under the following circumstances we may rely on the performance by another financial institution of some or all of the elements of our customer identification program with respect to any customer that is engaging in a money service transaction 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.

6. Foreign Correspondent Accounts and Foreign Shell Banks

It is our policy that the Company will not engage in any money service transactions when we have a reasonable cause to believe a foreign bank or foreign financial institution is involved in any way.

7. Monitoring Accounts for Suspicious Activity

We will digitally or manually monitor a sufficient amount of money service 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 7. A. 1 below. The AML Compliance Officer 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-MSB 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.

A. Emergency Notification to the Government

When conducting due diligence 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 may contact the OFAC via its hotline at 1-800-540-6322 or electronically through its website at www.treas.gov

1. Detecting 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 Company's compliance with government reporting requirements and the firm's AML policies (particularly concerning his or her identity, type of business), or is reluctant or refuses to reveal any information concerning business activities, or furnishes unusual or suspicious identification or documents.
- The customer wishes to engage in a transaction that lack business sense or is inconsistent with the customer's stated business.
- 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 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.
- The customer attempts to conduct frequent or large transactions, or asks for exemptions from the Company's AML policies.
- 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 has unexplained or sudden extensive money service activity, especially when they that had little or no previous activity.
- The customer has a large number of wire transfers to unrelated third parties inconsistent with the customer's legitimate business purpose.
- The customer has financial activity with no apparent business purpose to or from a country identified as a money laundering risk or a bank secrecy haven.
- 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 requests that a transaction be processed to avoid the Company’s normal documentation requirements.
- The customer uses multiple accounts, or maintains accounts in the names of family members or corporate entities, with no apparent purpose.
- The customer has inflows of funds or other assets well beyond the known income or resources of the customer.

2. Responding to Red Flags and Suspicious Activity

When a member of the Company 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-MSB.

8. Suspicious Transactions and BSA Reporting

A. Filing a Form SAR-MSB

We will file Form SAR-MSBs for any activity (including deposits and transfers) conducted or attempted through our Company involving (or in the aggregate) $2,000 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 Company to facilitate criminal activity.

We will not base our decision on whether to file a SAR-MSB solely on whether the transaction falls above a set threshold. We will file a SAR-MSB 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 appropriate government agency immediately and will file a SAR-MSB with FinCEN.

We will report suspicious transactions by completing a SAR-MSB and we will collect and maintain supporting documentation as required by the BSA regulations. We will file a SAR-MSB no later than 30 calendar days after the date of the initial detection of the facts that constitute a basis for filing a SAR-MSB. If no suspect is identified on the date of initial detection, we may delay filing the SAR-MSB 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-MSB filed and the original or business record equivalent of any supporting documentation for five years from the date of filing the SAR-MSB. We will identify and maintain supporting documentation and make such information available to FinCEN, any other appropriate law enforcement agencies, or federal or state 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-MSB or the information contained in the SAR-MSB, except where disclosure is requested by FinCEN, or other appropriate law enforcement or regulatory agency or an SRO, will decline to produce to the SARMSB or to provide any information that would disclose that a SAR-MSB was prepared or filed. We will notify FinCEN of any such request and our response.

B. Currency Transaction Reports (CTR)

If we receive currency, 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. We will use the Form CTR at www.fincen.gov

9. AML Record Keeping

A. SAR-MSB Maintenance and Confidentiality

We will hold SAR-MSBs and any supporting documentation confidential. We will not inform anyone outside of a law enforcement or regulatory agency about a SAR-MSB. We will refuse any subpoena requests for SAR-MSBs or SAR-MSB information and immediately tell FinCEN of any such subpoena we receive. We will segregate SAR-MSB filings and copies of supporting documentation from other Company books and records to avoid disclosing SAR-MSB filings. Our AML Compliance Officer will handle all subpoenas or other requests for SAR-MSBs. We will share information with our bank about suspicious transactions in order to determine when a SAR-MSB should be filed – unless it would be inappropriate to do so under the circumstances, such as where we file a SAR-MSB concerning the bank 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 any SARs are filed as required.

C. Records Required

As part of our AML program, the Company will create and maintain SAR-MSBs, and other relevant documentation on customer identity and verification (see Section 4 above) and funds transfers and transmittals as well as any records related to customers listed on the OFAC list. We will maintain SAR-MSBs and their accompanying documentation for at least five years.

10. Bank / Company Relationship

We will work closely with our payment processor, BaaS provider, banking firm to detect money laundering. We will exchange information, records, data and exception reports as necessary to comply with AML laws. The appropriate notification forms can be found at www.fincen.gov Generally we have agreed that the Company will monitor customer activity including proper customer identification information as required.

11. Training Programs

We developed ongoing employee training under the leadership of the AML Compliance Officer. Our training will occur on at least an annual basis. We will send our compliance team to various conferences, events, etc. from time to time so that they will be in sync with industries new policies or screening techniques.

The training course includes, 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 Company's record retention policy; and the disciplinary consequences (including civil and

criminal penalties) for non-compliance with the PATRIOT Act. The training program offered by Exchange Analytics, Inc. includes the maintenance of the records to show the persons trained, the dates of training, and the subject matter of their training.

Training will also include educational pamphlets, videos, intranet systems, in-person lectures, and explanatory memos as necessary. 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.

12. Program to Test AML Program

Annual testing of our AML program will be performed either by an independent third party which is primarily focused on PATRIOT Act compliance matters or other qualified independent third party or internally by a qualified member of the Company's staff. The annual testing will include an audit of our compliance with our AML program.

The auditor will issue a report of the auditor's findings upon completion their audit to senior management. We will address each of the resulting recommendations.

13. Monitoring Employee Conduct and Accounts

We will subject employee money service transactions 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 a qualified member of the Company staff.

14. 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 an appropriate member of senior management. Such reports will be confidential, and the employee will suffer no retaliation for making them.

15. Additional Areas of Risk

The Company has reviewed all areas of its business to identify potential money laundering risks that may not be covered in the procedures described above and is continually working to improve its AML program.

16. Senior Manager Approval

I have approved this AML program as reasonably designed to achieve and monitor the Company's ongoing compliance with the requirements of the AML regulatory authority and the implementing regulations under it.

Signed: 

Name: Lalithbabu Logeshwarrao

Title: CEO