Sun Wave LLC

AML/CFT Manual

Table of Contents

Introduction

The purpose of the Anti-Money Laundering Procedures Manual (hereinafter the "AML Manual" or "Manual") is to provide instructions, measures, rules, and procedures that are to be implemented and maintained by Sun Wave LLC (the "Company") registered address at Lighthouse Trust Nevis Ltd, Suite 1, A.L. Evelyn Ltd Building, Main Street, Charlestown, Nevis, Saint Kitts and Nevis in order to counter the risk and reduce the extent to which it is possible for the Company to be used for money laundering and terrorist financing activities.

This Manual contains, in particular, the policies and procedures, which all employees of the Company need to understand and acknowledge, in order to prevent the business from being used to launder the proceeds of crime or terrorist financing.

At the heart of this document is a risk-based approach, meaning the Company focuses their resources on the areas of greater risk.

The Company has set out policies and procedures for preventing money laundering and terrorist financing activities. Those procedures, which are implemented by the Company, are the following:

- Identification and due diligence procedures of clients.
- Record keeping procedures in relation to clients' identity and their transactions.
- Internal reporting procedures to a competent person (e.g. Anti-Money Laundering Compliance Officer) appointed to receive and consider information that gives rise to knowledge or suspicion that a client is engaged in money laundering activities.
- Appropriate procedures of internal control, risk management, with the purpose of preventing money laundering activities.
- The detailed examination of every transaction that due to its nature is considered vulnerable to money laundering, and especially for complicated or unusually large transactions and transactions that are taken place without an obvious financial or legal purpose.
- Measures for making employees aware of the above-mentioned procedures to prevent money laundering and of the legislation relating to money laundering.
- Provision of regular training to their employees in the recognition and handling of transactions suspected to be associated with money laundering.

Money Laundering: Definition

Money Laundering is a generic term used to describe the methods used by criminals to conceal the origins of illegally obtained funds by making such funds appear to have derived from a legitimate source. The process typically takes place in three stages:

- PLACEMENT: This is the stage at which illegally obtained funds are introduced into the financial system
- LAYERING: This is the fundamental stage where criminals 'wash' the funds by creating a complex network of transactions with the intention of muddying the initial entry point.
- INTEGRATION: This is the final stage where the laundered funds have successfully been made to appear as legitimate.

Illegally obtained funds are not laundered through the financial industry alone, however billions a year are, some examples include but are not limited to:

- purchases of monetary instruments (e.g. traveller's cheques or money orders;
- structured deposits or withdrawals from bank accounts;
- false identities, using close family members;
- wire transfers from non-existent individuals, etc.

Terrorist Financing: Definition

Terrorist financing is described as techniques, similar to those used by money launderers, where funds are provided for terrorist activity by individuals who wish to conceal the ultimate beneficiaries and the sponsors of the funds. It involves both funds raised from legitimate sources as well as criminal sources.

Risk-Based Approach

The Company applies a risk-based approach, meaning it concentrates its efforts and resources on areas where the risk of money laundering and terrorist financing are considered greater, and reduces requirements where the risk is considered low.

The adopted risk-based approach has the following general characteristics:

- It recognizes that the threat of money laundering or terrorist financing varies across clients, countries, services and financial instruments;
- It allows the BOD to differentiate between the Company's clients in a way that matches the risk of its particular business;
- It allows the BOD to apply its approach in the formulation of policies, procedures, and controls in response to the Company's particular circumstances and characteristics;
- It helps to produce a more cost-effective system;
- It promotes the prioritization of effort and actions of the Company in response to the likelihood of money laundering or terrorist financing occurring through the use of services provided by the Company.

The Company's risk-based approach involves specific measures and procedures in assessing the most cost-effective and proportionate way to manage the money laundering and terrorist financing risks faced by the Company. These include:

- identifying and assessing the money laundering and terrorist financing risks emanating from particular customers, financial instruments, services, and geographical areas of operation of the Company and its clients;
- documenting the policies, measures, procedures, and controls to ensure their uniform application across the Company by individuals specifically appointed for that purpose by the board of directors;
- managing and mitigating the assessed risks by the application of appropriate and effective measures, procedures, and controls;
- Continuous monitoring and improvements in the effective operation of the policies, procedures, and controls.

Identification of Risks

The Company assesses the risk it faces, for usage of services provided for the purpose of money laundering or terrorist financing, it then determines the suitable procedures and measures that need to be applied to counter and manage the risk, dependent on the Company's particular circumstances.

In cases where the services and the financial instruments that the Company provide are simple, i.e. involving customers with similar characteristics, then the Company will apply procedures that focus on those customers who fall outside the 'norm'.

The following risks identified are those that may be applicable to the Company:

Risks posed by clients		
I	Complexity of ownership structure of legal persons	N/A
II	Companies with bearer shares	N/A
III	Companies incorporated in offshore centres	N/A
Risks posed by clients		
IV	Politically exposed persons	Applicable
V	Clients engaged in transactions which involve significant amounts of cash	N/A
VI	Clients from countries known for a high level of corruption or organized crime	Applicable

The Company screens all clients against a global database on AML risk exposures covering sanctions/watchlists, PEPs and adverse media. As such, the Company is able to identify PEPs and/or relations to PEPs, and take appropriate actions.

The Company does not accept cash deposits from its clients.

Risks posed by client's behaviour		
I	Transactions with no apparent financial/commercial rational	N/A
II	Situations where the origin of wealth and/or source of funds cannot be easily verified	Applicable
III	Unwillingness of clients to provide information on the beneficial owners of a legal person	N/A

The Company faces the risk that it may not be able to verify the source of funds it received from its clients. As such, and in order to mitigate the risk, supporting documentation may be requested to support payments made by clients.

The Company only accepts payments from accounts held in the name of the client and will not allow third-party transfers.

Risks posed by communication		
I	Non-face-to-face clients	Applicable

The Company accepts transactions over the internet via electronic means, as such the client is not present so as to verify the authenticity of his/her signature or that he/she is the real owner of the trading account (non-face-to-face).

Further to this, the Company requests up-to-date documentation for client's in order to confirm their identity.

Risk posed by financial instruments		
I	Services that allow payments to third parties	N/A
II	Large cash deposits or withdrawals	N/A

The Company does not allow payments to be made to third parties/persons, and it is the Company's practise to return funds to the same source, as such the Company does not incur the above risk i.

Clients Risk Classification

The Company has set out the criteria for categorization of customers on a risk basis in line with its Customer Acceptance Policy. All the Company's Clients are classified as High Risk since Clients are not present either before the establishment of a business relationship and/or when carrying occasional transactions with the Company. In addition, the Company, taking into account other relevant factors, including Clients' country of origin, background, and information from international organizations, has categorized its Clients into the following subcategories:

High-Low Risk

Clients falling in this category include all Clients who do not fall in the High-High Risk category. The Company applies enhanced due diligence measures for Clients falling under this category by performing the following:

- Requesting KYC documents from the Client, consisting of copy of identification document;
- Utilizing software and electronic databases for the purpose of detecting potential negative information regarding the Client and/or for additional verification of its proof of identification when needed;

- Exercising enhanced monitoring procedures in order to detect transactions which fall outside the regular pattern of an account's activity or to identify complex or unusual transactions or transactions without obvious economic purpose or clear legitimate reason.

High-High Risk

The following Clients fall under this category:

- Politically exposed persons ("PEPs") as these are defined in the Enhanced Client Due Diligence section. A business relationship with any PEP must be approved by Senior Management or the AMLCO;
- Clients whose country of origin has been identified as high-risk by the FATF.

Dynamic Risk Management

Risk management is a continuous process, carried out on a dynamic basis. Risk assessment is not only made as an isolated event that lasts for a limited duration. All measures, procedures, and controls are kept under regular review so that risks resulting from change in the characteristics of existing clients, new clients, services and financial instruments are managed and countered effectively.

From time to time, the AMLCO will amend the risk-based procedures, policies, and controls by consulting information from relevant international organizations including, but not limited to:

- Financial Action Task Force (FATF) – www.fatf-gafi.org
- The International Money Laundering Information Network (IMOLIN) – www.imolin.org
- The Council of Europe Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL) – www.coe.int/moneyval
- The International Monetary Fund (IMF) – www.imf.org

- UN Security Council Sanctions Committees – www.un.org/sc/committees
- the EU Common Foreign & Security Policy(CFSP) – http://ec.europa.eu/external_relations/cfsp/sanctions/list/consol-list.html

The Company shall apply the following measures and procedures described below related to the Sanctions Regimes:

In order for the Company to be aware and up to date with the Sanctions Regimes and facilitate the prompt implementation of the sanctions and/or restrictions, the Company assesses and collects the relevant information through the following sources:

- The official website of the UN which contains all the necessary information regarding the Decisions/Resolutions of the SC/UN which are related to the imposition of sanctions per year is: https://www.un.org/securitycouncil/sanctions/information ;
- UN Sanctions: https://www.un.org/sc/suborg/en/sanctions/information ;
- Consolidated United Nations Security Council Sanctions List: https://www.un.org/sc/suborg/en/sanctions/un-sc-consolidated-list
- OFAC sanctions' list - https://sanctionssearch.ofac.treas.gov/
- The consolidated list of persons, groups and entities subject to EU financial sanctions - https://webgate.ec.europa.eu/fsd/fsf
- The UK Sanctions' list - https://www.gov.uk/government/publications/the-uk-sanctions-list

The Company does not enter into business relationships with sanctioned persons and must submit, prior to the performance of such activity, the relevant request to the AML Compliance Officer in order to approve or reject it. In case the relationship is already in course, all assets of the sanctioned person are subject to the immediate freeze and are reported to competent authorities.

Customer Acceptance Policy

The Company maintains clear policies relating to the acceptance of clients and which clients are likely to pose a higher risk. When accepting a client, the Company examines factors including the client's background/experience, country of origin, public or high-profile position and takes adequate measures to verify the identity of the client through its KYC and due diligence procedures.

A decision to enter into business relationships with higher risk clients, i.e. politically exposed persons or close relations to PEPs, can only be taken by Senior Management with advice from the AMLCO. These accounts are subject to an annual review in order to determine whether to allow the continuance of their operation. For this purpose, the AMLCO prepares a short report on these clients for consideration and approval by Senior Management.

No cash is accepted as a means of trading when accepting clients or in the settlement of accounts. All documents and checks are made by the Back-Office Department, who undergo additional AML training throughout the year.

Customer Identification Procedures

Customer identification is made on any individual who registers for a trading account with the Company. The business relationship is considered to begin upon the signing of the Company's Terms & Conditions (hereinafter the "Agreement").

Until a deposit is made, and the client has signed the Agreement, the client has access to a demo account which can be used for practising or gaining experience in trading the financial instruments offered by the Company. Upon registration, the client accepts the Company's Demo Terms & Conditions only. The client is then given the option to proceed with utilizing their practice demo account (which holds within it $10,000 of virtual funds). If the client proceeds only with the demo account, they are not required to fulfil the below verification steps.

Alternatively, the client may choose to deposit funds and trade on a real account. If the client selects the real account, they are redirected and must complete the below verification steps.

Email Confirmation: The client must ensure to validate and confirm their email address. The client is unable to confirm the same email address twice, which limits access to the opening of multiple accounts, which can be used as a means to separate transactions so that they are not considered on a cumulative basis.

Verify Personal Data: The information gathered in this section related to the client's personal information and includes:

- Full name
- Gender
- Date of Birth
- Residential address including Country, City, Postal Code
- Citizenship
- US reportable person: the client is asked during verification if they are considered a US reportable person.

A US reportable person is defined, for the client's reference, as anyone who holds one of the following: US Citizenship, residency, tax identification number, or Mailing/ Residential Address, Telephone number, as well as anyone who has instructions to send funds to an account maintained in the United States. If the client answers yes, they will be informed that they are not able to open an account.

Verification process

Clients are requested to verify their identity by submitting a proof of identity.

Proof of Identity: A coloured copy of the client's passport (or copies of the front and back of the client's identity card) can be provided by the client as proof of identity. The copies must clearly show the client's full name, photo, date of birth, expiry date, official document number and the signature of the client. Copies of these documents must be clear and legible, or they will not be accepted.

The client is able to provide their proof of identity in one of two ways, either by uploading scanned copies of photographs that they have already saved or by using the camera function on their mobile or desktop to verify their identity in real time.

The Company utilizes Jumio's Netverify document authentication service to verify client identity as part of the anti-money laundering (AML) Know Your Customer compliance requirements. It should be noted that the Company also accepts other Government issued identity documents, such as driving licences or residents permits, as long as these fulfil the above requirements. Drivers licences, depending on region, may be electronically verified using the Netverify system. It is at the discretion of the Head of Back Office, or the AMLCO, to determine if such documents are acceptable. Should a document not be verified using the above service, it will be passed on for manual verification by the Back-Office Department.

The Company reserves the right, as per its Terms & Conditions, to request additional supporting documents in order to verify the clients' trading account. Additional documents may be requested depending on the deposit method used by the client, in order to verify the source of a deposit, or to clarify/support information provided by the client throughout the verification process. Other documents may be requested by the AML/Compliance Function when investigating Suspicious Transactions.

PEP/Sanctions Screening

The Company uses a tool for screening a database of Politically Exposed Persons (PEPs) and heightened risk individuals to help identify and manage financial, regulatory and reputational risk.

Screening is being performed on all the clients whose proof of identity is being verified to ensure that they are not PEPs, RCAs, Sanctioned persons, criminals, or have any history of fraudulent or money laundering activity.

Specific Client Due Diligence Procedures

Client Due Diligence procedure shall comprise the following:

- Identification of the client and taking risk-based and adequate measures for verification of the client's identity on the basis of information obtained from a reliable and independent source;
- Obtaining information on the purpose and intended nature of the business relationship;
- Conducting ongoing monitoring of the business relationship, including scrutiny of transactions undertaken throughout the course of the relationship, to ensure that the transactions being conducted are consistent with the data and information held by the firm in connection with the client.

When there is a suspicion of money laundering or terrorist financing, irrespective of the amount of the transaction; or when there are doubts about the veracity or adequacy of previously obtained client identification data, due diligence procedures will be applied.

Failure or refusal by a client to submit the requisite data and information for the verification of his/her identity and/or his/her economic profile, without adequate justification, constitutes elements that may lead to the creation of a suspicion that the client is involved

in money laundering or terrorist financing activities. In such an event, the Company does not proceed with the establishment of the business relationship.

Enhanced Client Due Diligence

PEPs are individuals who are or have been entrusted with prominent public functions in a foreign country and/or who are closely associated or have a close relationship with someone who is a PEP. Where the client is determined to be a Politically Exposed Person (PEP) the Company adopts additional due diligence measures to determine whether a prospective client is a politically exposed person:

- Have appropriate risk-based procedures to determine whether the client is a PEP;
- Approval from Senior Management prior to the establishment of the business relationship with the client;
- Take appropriate measures for the establishment of the origin of the client's assets and the source of funds that are related to the establishment of the business relationship or transaction;
- Conduct enhanced and continuous monitoring of the business relationship.

The Company detects and monitors the activity of Politically Exposed Persons. The company has a risk management system in place to determine whether prospective or existing clients are PEPs, and conducts regular searches and checks for this purpose.

The company will search for information from a PEP/sanction screening services provider. The Company will also rely on public information in determining whether persons are within the definition of "Close Associates" (for example, partners or joint ventures), and will conduct regular searches and checks for this purpose.

Enhanced CDD and enhanced ongoing monitoring (on a risk-sensitive basis) are required whenever a customer is or becomes a Politically Exposed Person (PEP).

If a customer is identified as a high-risk individual or Politically Exposed Person, the company will perform the following procedures:

- ascertain and verify his/her identity with the help of supporting KYC documents;
- in case of PEP client, obtain the approval of senior management before the establishing or continuing a business relationship with the customer;

- take reasonable measures to establish the person's Source of Wealth and/or Source of Funds;
- conduct regular enhanced monitoring throughout the business relationship (ongoing monitoring in case of high-risk clients; at least semi-annual in case of PEP clients).

Database Screening (ComplyAdvantage)

The Company additionally uses a screening database of Politically Exposed Persons (PEPs) and heightened risk individuals (i.e. Sanctions ‘ lists) to help identify and manage financial, regulatory and reputational risk. A NAME CHECK is made automatically on ALL clients whose proof of identity has been verified in order to ensure that they are not PEPs, close relations to PEPs, Sanctioned persons, criminals or have any history of money laundering or terrorist financing.

The screening system will automatically identify any matches to the client’s name and list them on a report that can be extracted through the Company’s CRM system. Only clients who have matches to their name will be present in the report. All clients that have no matches will be automatically approved on the system. It is the responsibility of the back office and the compliance department to review all matches and manually verify and approve the client.

In addition to this, all clients, upon uploading their proof of identity, will undergo automatic document verification and MRZ checks, as well as additional identity and passport checks. The purpose of these checks is to scrutinize the validity of the document.

If the automatic check reveals that the document is not valid or acceptable, the client will be informed accordingly and must upload another identity document in order to verify their account.

Ongoing Monitoring

Ongoing monitoring of accounts is a crucial tool used to effectively determine the risk of money laundering and terrorist financing.

The Company is required to have a full understanding of the 'normal' and 'reasonable' account activity of its clients as well as have an understanding of their client's economic profile, whilst having the means of identifying transactions which fall outside the regular pattern of an account's activity or to identify complex or unusual transactions or transactions without obvious economic purpose or clear legitimate reason.

The Company collects the relevant information needed for the construction of the client's economic profile as mandatory in order to identify whether the client's activity or transactions deviate from expected or anticipated movement of that client's account.

Significant deviations are examined further to determine any suspicion of money laundering and/ or terrorist financing. The AMLCO investigates the suspicion received via the 'Internal Suspicions Report' and determines whether further action should be taken.

The procedures and intensity of monitoring customers and examining transactions will be based on the level of assessed risk, with the objective to:

- detecting of unusual or suspicious transactions that are inconsistent with the economic profile of the customer for the purposes of further investigation;
- investigating unusual or suspicious transactions: the results of the investigations are recorded in a separate memo and kept in the file of the customer concerned. Based on the investigation's findings, the MLCO decides appropriate measures and actions to be taken;
- ascertaining the source and origin of the funds.

FATCA (US Reportable persons)

The Foreign Account Tax Compliance Act ("FATCA") is focused on strengthening information reporting and withholding compliance with respect to US persons that invest through non-US entities.

As per FATCA requirements, the Company is obligated to employ enhanced due diligence procedures in order to identify, document and report on all US persons to the Inland Revenue Service (“IRS”).

The Company states clearly in its Terms & Conditions agreed to by all clients that they do not provide services to clients who are identified or identify themselves as US reportable persons.
By definition, a US reportable person can be classified as anyone who holds one of the following:

- US Citizenship (including dual citizenship);
- US residency or resident alien document for tax purposes;
- US Tax Identification Number;
- US Mailing/Residential address;
- US telephone number;
- Anyone who has instructions to fund as account maintained in the US.

The client is asked to identify if they fall into one of the above categories, any client who answers ‘yes’ will be unable to proceed with registration.

Additional checks are made by the Back Office team in order to ensure that the Company is doing everything in their power to identify any clients who may be considered US Reportable. These checks include the checking of client questionnaires, KYC documents as well as IP checks. If any client has a connection to the US, the BO department will inform Compliance, who will advise BO on how to investigate further.

Employees Responsibilities

Employees of the Company are responsible for reading the AML manual and understanding their respective responsibilities. They must ensure that the Company’s anti-money laundering procedures are adhered to and that they will not offer any assistance to those clients who wish to violate them.

Employees will and must make themselves available, at least annually, to receive education and training on any updates or new developments in the field of preventing money laundering and terrorist financing that the Company will organize for them.

Employees shall report immediately any suspicion of money laundering activity to the Company's AMLCO through the Company's internal communication channels.

APPENDIX: EXAMPLES OF SUSPICIOUS TRANSACTIONS/ACTIVITIES RELATED TO MONEY LAUNDERING AND TERRORIST FINANCING

MONEY LAUNDERING

- Transactions with no discernible purpose or are unnecessarily complex.

    - Use of foreign accounts of companies or group of companies with complicated ownership structure, which is not justified based on the needs and economic profile of the customer.
    - The transactions or the size of the transactions requested by the customer do not comply with his usual practice and business activity.

- Large volume of transactions, and/or money deposited or credited into, an account when the nature of the customer's business activities would not appear to justify such activity.

- The business relationship involves only one transaction, or it has a short duration.

- There is no visible justification for a customer using the services of a particular Financial Organization. For example, the customer is situated far away from the particular Financial Organization and in a place where he could be provided services by another Financial Organization.

- There are frequent transactions in the same financial instrument without obvious reason and in conditions that appear unusual (churning).

- There are frequent small purchases of a particular financial instrument by a customer who settles in cash, and then the total number of the financial instrument is sold in one transaction with settlement in cash or with the proceeds being transferred, with the customer's instructions, to an account other than his usual account.

- Any transaction of the nature, size or frequency appear to be unusual, e.g. cancellation of an order, particularly after the deposit of the consideration.

- Transactions which are not in line with the conditions prevailing in the market, in relation, particularly, with the size of the order and the frequency.

- The settlement of any transaction, but mainly large transactions, in cash.

- Settlement of the transaction by a third person which is different from the customer who gave the order.

- Instructions of payment to a third person who does not seem to be related with the instructor. - Transfer of funds to and from countries or geographical areas which do not apply, or they apply inadequately FATF's recommendations on money laundering and terrorist financing.

- A customer is reluctant to provide complete information when it establishes a business relationship about the nature and purpose of its business activities, anticipated account activity, prior relationships with Financial Organizations, names of its officers and directors, or information on its business location. The customer usually provides minimum or misleading information that is difficult or expensive for the Financial Organization to verify.

- A customer provides unusual or suspicious identification documents that cannot be readily verified.

- A customer's home/business telephone is disconnected.

- A customer who makes frequent or large transactions and has no record of past or present employment experience.

- Difficulties or delays on the submission of the financial statements or other identification documents, of a customer/legal person.

- A customer who has been introduced by a foreign Financial Organization, or by a third person whose countries or geographical areas of origin do not apply, or they apply

inadequately FATF's recommendations on money laundering and terrorist financing.

- Shared address for individuals involved in cash transactions, particularly when the address is also a business location and/or does not seem to correspond to the stated occupation (e.g. student, unemployed, self-employed, etc).

- The stated occupation of the customer is not commensurate with the level or size of the executed transactions.

- Financial transactions from non-profit or charitable organizations 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.

    - Unexplained inconsistencies arising during the process of identifying and verifying the customer (e.g. previous or current country of residence, country of issue of the passport, countries visited according to the passport, documents furnished to confirm name, address and date of birth etc).
    - Complex trust or nominee network.
    - Transactions or Company structures established or working in an unneeded commercial way. e.g. companies with bearer shares or bearer financial instruments or use of a postal box.
    - Use of general nominee documents in a way that restricts the control exercised by the Company's board of directors.
    - Changes in the lifestyle of employees of the Financial Organization, e.g. luxurious way of life or avoiding being out of office due to holidays.
    - Changes the performance and the behaviour of the employees of the Financial Organization.

TERRORIST FINANCING

A. Sources and methods

The funding of terrorist organizations is made from both legal and illegal revenue generating activities. Criminal activities generating such proceeds include kidnappings (requiring ransom), extortion (demanding "protection" money), smuggling, thefts, robbery and narcotics trafficking. Legal fund-raising methods used by terrorist groups include:

- collection of membership dues and/or subscriptions,
- sale of books and other publications,
- cultural and social events,
- donations,
- community solicitations and fund-raising appeals.

Funds obtained from illegal sources are laundered by terrorist groups by the same methods used by criminal groups. These include cash smuggling by couriers or bulk cash shipments, structured deposits to or withdrawals from bank accounts, purchases of financial instruments, wire transfers by using "straw men", false identities, front and shell companies as well as nominees from among their close family members, friends and associates.

B. Non-profit organizations

Non–profit and charitable organizations are also used by terrorist groups as a means of raising funds and/or serving as cover for transferring funds in support of terrorist acts. The potential misuse of non-profit and charitable organizations can be made in the following ways:

- Establishing a non-profit organization with a specific charitable purpose, but which actually exists only to channel funds to a terrorist organization.
- A non-profit organization with a legitimate humanitarian or charitable purpose is infiltrated by terrorists who divert funds collected for an ostensibly legitimate charitable purpose for the support of a terrorist group.
- The non-profit organization serves as an intermediary or cover for the movement of funds on an international basis.
- The non-profit organization provides administrative support to the terrorist movement.

Unusual characteristics of non-profit organizations indicating that they may be used for the purpose are the following:

- Inconsistencies between the apparent sources and amount of funds raised or moved.
  • A mismatch between the type and size of financial transactions and the stated purpose and activity of the non-profit organization.
- A sudden increase in the frequency and amounts of financial transactions for the account of a non-profit organization.

- Large and unexplained cash transactions by non-profit organizations.
- The absence of contributions from donors located within the country of origin of the non-profit organization.