Kudo AML POLICY

Kudo Trade (Mauritius) Ltd

COMPANY NUMBER: C215955

1. Introduction

1.1. Kudo Trade (Mauritius) Ltd (hereinafter referred to as the "Company" or "Kudo"), is regulated by the Financial Services Commission of the Republic of Mauritius with an Investment Dealer license GB24203599, having its registered office at 6 St Denis Street, 1/F River Court, Port Louis, Mauritius. The Company operates in accordance with Securities Act (SA). The Mauritius Securities Act sets the legal and corporate framework for companies to meet the conditions of the license.

1.2. The objects of the Company are all subject matters not forbidden by the Securities Act

(SA) of Mauritius, but not exclusively all commercial, financial, lending, borrowing, trading, service activities and the participation in other enterprises as well as to provide brokerage, training and managed account services in currencies, commodities, indexes, CFDs and leveraged financial instruments.

1.3. The Company is committed to combating money laundering and for this reason it has

appointed a dedicated Anti-Money Laundering Compliance Officer (the "AMLCO") who is accountable to the Board of Directors and Senior Management of the Company. The AMLCO is further responsible for the training of employees with respect to the Anti-Money Laundering Law and any amendments thereof as well as for the preparation of the internal procedures of the Company.

2. KeyPrinciples

2.1. All the Company's employees are required to read and acknowledge the AntiMoney

Laundering Manual of the Company and shall at all times act under the 'Key Principles' set out therein.

- Take appropriate steps to protect the Company and its domain from any activities which involve money laundering and terrorist financing.
- The Company must maintain and implement written policies and procedures with

respect to combating money laundering, a system of internal controls to ensure ongoing compliance with applicable laws reviewed and monitored by a designated person and to take appropriate action, once suspicious activity is detected, through the reporting of such transactions in line with the guidelines set out by Global AntiMoney Laundering regulations.

- Comply with applicable anti-money laundering and terrorist financing laws and regulations as established by the Global Anti-Money Laundering guidelines.
- All business units of the Company shall follow the AML policies and procedures.
- Report all identified suspicious activities to the extent that it can do so under all applicable foreign and domestic laws.
- Compliance with the Company's AML policies will be monitored through a combination of internal audit and regulatory reviews of compliance with relevant antimoney laundering legislation and/or regulations.
- Retaining all the customer-related documents for a period specified as per the Financial Services Commission of the Republic of Mauritius.
- The Company does not offer services of opening anonymous accounts.
- Full cooperation with law enforcement and regulatory agencies to the extent that it can do so under all applicable laws.
- Train staff on Know Your Customer and Anti-Money Laundering policies and new AML laws and regulations.
- The AML Compliance Committee is responsible for initiating Suspicious Activity Reports ("SARs") or other required reporting to the appropriate law enforcement or regulatory agencies. Any contacts by law enforcement or regulatory agencies related to the Policy shall be directed to the AML Compliance Committee.

  The committee shall:
  - Receive internal reports of (suspicions of) money laundering.
  - Investigate reports of suspicious events.
  - Make reports of relevant suspicious events to the relevant authorities.
  - Ensure the adequacy of arrangements made for the awareness and training of staff and advisers.
  - Report at least annually to the firm's governing body on the operation and effectiveness of the firm's systems and controls.

- Monitor the day-to-day operation of anti-money laundering policies in relation to the development of new products; the taking on of new customers; and changes in the firm's business profile

3. Policy

It is the policy of Kudo to actively pursue the prevention of money laundering and any activity
that facilitates money laundering or the funding of terrorist or criminal activities. Kudo is committed to AML compliance in accordance with applicable law and requires its officers, employees and appointed producers to adhere to these standards in preventing the use of its products and services for money laundering purposes. For the purposes of the Policy, 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 been derived from legitimate origins or constitute legitimate assets.

4. What is Money Laundering?

Money laundering is the process by which criminally obtained money or other assets (criminal property) are exchanged for "clean" money or other assets with no obvious link to their criminal origins. Criminal property may take any form, including money or money's worth, securities, tangible property and intangible property. It also covers money, however come by, which is used to fund terrorism.
Money laundering activity includes:

- Acquiring, using or possessing criminal property
- Handling the proceeds of crimes such as theft, fraud and tax evasion
- Being knowingly involved in any way with criminal or terrorist property
- Entering arrangements to facilitate laundering criminal or terrorist property
- Investing the proceeds of crimes in other financial products
- Investing the proceeds of crimes through the acquisition of property/assets
- Transferring criminal property.

There is no single stage of money laundering; methods can range from the purchase and resale of luxury items such as a car or jewelry to passing money through a complex web of legitimate operations. Usually, the starting point will be cash, but it is important to

appreciate
that money laundering is defined in terms of criminal property.
The money laundering process follows three stages:

- Placement – Disposal of the initial proceeds derived from illegal activity e.g. into a bank account.
- Layering – The money is moved through the system in a series of financial transactions to disguise the origin of the cash with the purpose of giving it the appearance of legitimacy.
- Integration – Criminals are free to use the money as they choose once it has been removed from the system as apparently "clean" funds.

5. What is Counter Terrorist Financing (CTF)?

Terrorist financing is the process of legitimate businesses and individuals that may choose to provide funding to resource terrorist activities or organizations for ideological, political or other reasons.
Firms must therefore ensure that:

- Customers are not terrorist organizations themselves; and
- They are not providing the means through which terrorist organizations are being funded. 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.

6. Risk Based Approach

The level of due diligence required when considering anti-money laundering procedures within the firm should take a risk-based approach. This means the amount of resources spent in conducting due diligence in any one relationship that is subject to risk should be in proportion to the magnitude of the risk that is posed by that relationship
These can be broken down into the following areas:
Customer Risk
Different customer profiles have different levels of risks attached to them – a basic Know Your Customer (KYC) check can establish the risk posed by a customer. Corporate

structures can be used by criminals to introduce layers within transactions to hide the source
of the funds, and like that, clients can be categorized into different risk bands.

Product Risk

This is the risk posed by the product or service itself. The product risk is driven by its functionality as a money laundering tool. Products can be categorized into three risk bands –
reduced, intermediate and increased. Additionally, a factor that will contribute to the classification of the risk category is the sales process associated with the product. If the transaction in the product takes place on an advisory basis because of a KYC, this will carry less risk than an execution only transaction.

Country Risk

The geographic location of the client or origin of the business activity has a risk associated with it. Countries around the globe have different levels of risk attached to them. A firm would determine the extent of their due diligence measures required initially and on an ongoing basis using the above risk areas.

6.1 Customer Risk Assessment (CRA)

A Customer Risk Assessment must be conducted before establishing a business relationship or carrying out a transaction. The CRA determines: the extent of identification information required; additional information to be requested; verification methods; and the extent of ongoing monitoring. CRA review frequency is as follows:

- Risk Classification Review Frequency
- High Risk At least annually
- Medium Risk At least every 2 years
- Low Risk At least every 3 years
- Material Change At the point of any material change in the customer's profile or circumstances.

6.2 Client Onboarding and Customer Due Diligence

The Company's onboarding process requires all prospective clients to complete Customer Due Diligence (CDD) before any business relationship is established or services are made available. No client shall be permitted to access the Company's services until the onboarding process has been initiated and the applicable verification requirements have been satisfied In accordance with this Policy.

Identification and Verification

A key element of AML/CFT prevention is the ability to identify customers and their beneficial owners and verify their identities. The Company's CDD measures include:

- Identifying and verifying the identity of each applicant for business.
- Identifying and verifying the identity of the customer's beneficial owner(s).
- Identifying all natural persons who ultimately have a controlling ownership interest in the customer.
- Obtaining information on the purpose and intended nature of the business relationship.
- Conducting ongoing due diligence and scrutiny of transactions throughout the relationship.
- Using reliable, independently sourced documents, data, or information.
- Ensuring all CDD material is kept relevant and up to date.
- Determining whether the applicant is acting on behalf of a third party and recording the relevant details.

6.3 KYC Documentation – Natural Persons

The following data and documentation are required for natural person clients:

Data Required:

- Legal name (full legal name and any other names, including marital name, former name, or alias).
- Sex, date of birth, place of birth, and nationality.
- Current and permanent residential address (PO Box addresses are not acceptable).
- Any public position held, nature of employment, and name of employer.
- Government-issued personal identification number or other government-issued unique identifier.
- Tax Identification Number (if applicable).
  Documentation Required:
- Current valid Passport or National Identity Card (must incorporate photographic evidence of identity).

- Current valid Driving License (where the licensing authority verifies identity before issuance and must incorporate photographic evidence).
- A recent utility bill (within the last 3 months) issued to the individual by name, as proof of current or permanent residential address.
- A recent bank or credit card statement (not more than 3 months old, not printed from the internet).
- A recent bank reference.

6.4 KYB Documentation – Legal Persons

The following data and documentation are required for private companies, partnerships, foundations, trusts, and other legal persons:
Data Required:

- Legal status, legal name, and any trading names of the body.
- Nature of business, date and country of incorporation/registration, and official
- identification number.
- Registered office address, mailing address, and principal place of business/operations.
- Ownership and control structure, and the identity of all natural persons who ultimately have an ownership interest.
- For trusts: identity of the settlor, trustee, beneficiaries or class of beneficiaries, protector or enforcer, and any other natural person exercising ultimate effective control.
- Bank account details and Tax Identification Number (if applicable).
  Documentation Required:
- Certificate of Incorporation (or other appropriate certificate of registration or licensing).
- Memorandum and Articles of Association (or equivalent).
- UBO and Shareholder registry (or equivalent).
- Director Registry (or equivalent).
- Latest Audited Financial Statements and Annual Report (if available).
- Partnership deed, Trust Deed, Charter of Foundation, or equivalent instrument.

6.5 Certification of KYC Documentation

Where the Company relies upon non-original identity documents, documentation must be appropriately certified as true copies. Certified copies may be provided by: attorneys, lawyers, notaries, actuaries, accountants or other professionally qualified persons; directors or secretaries of regulated financial institutions; members of the judiciary; or senior civil servants. The certifier must sign, date, and indicate their name, address, position, and, where available, professional registration number.

6.6 Electronic Identification and Verification

The Company utilizes Sumsub as its third-party verification provider to assist with customer
identity verification, sanctions screening, and ongoing compliance monitoring. Verification procedures include biometric liveness testing to confirm that the applicant is a real and present individual. The reliance and effectiveness of the electronic verification system shall be tested periodically and reported to the Board as part of the Annual BRA Report.

6.7 Incomplete CDD

The registration process may not be completed before the full KYC documentation set has been provided. If a client fails to provide all required KYC documentation, no business relationship will be established, or the client's account shall be suspended (for existing accounts) until the complete KYC set has been received.

6.8 Client Verification and Account Restrictions

The Company applies a tiered access model based on a client's verification status. Access to account functions is determined by whether the client has successfully completed the Company's KYC requirements.

1. Non-Verified Clients

A client who has registered but not yet completed the full KYC verification process is

classified as a Non-Verified Client. The following restrictions apply:
Deposits: Permitted. However, if the client fails to complete the full KYC documentation set within seven (7) calendar days from the date of the deposit, the deposit will be refunded to the original source of funding. No interest or benefit shall accrue on refunded amounts.
Trading: Not permitted. A Non-Verified Client may not place, execute, or otherwise engage in any trading activity until full verification is completed.
Withdrawals: Not permitted. A Non-Verified Client may not request or process any withdrawal until full verification is completed.

2. Verified Clients

A client who has successfully completed the full KYC verification process is classified as a Verified Client. The following access applies:
Deposits: Permitted up to a cumulative net deposit threshold of USD 25,000. Once net deposits reach or exceed USD 25,000, Enhanced Due Diligence (EDD) requirements shall apply, including Source of Funds and Source of Wealth documentation, before further deposits are processed.
Trading: Permitted, subject to ongoing compliance monitoring and any account-level restrictions applied by the Compliance team.
Withdrawals: Permitted, subject to the Company's withdrawal policy, including the applicable FIFO principle and any AML/CTF holds applied by the Compliance team.
General
The Company reserves the right to restrict, suspend, or reverse any account function at any time where AML/CTF concerns are identified, verification is found to be incomplete or unsatisfactory, or where required by applicable law or regulatory guidance.

7. Enhanced Due Diligence (EDD)

7.1 When EDD Must Be Performed

Enhanced Due Diligence procedures shall be applied in the following circumstances:

- A higher risk of ML/TF has been identified.
- Through supervisory guidance, a high risk of ML/TF has been identified.

- A client or applicant is from a high-risk third country.
- Business relations, transactions, or persons are established in jurisdictions without adequate ML/TF systems.
- The client or applicant is a Politically Exposed Person (PEP).
- An individual or entity is named on a Sanctions List.
- The client has provided false or stolen identification documentation and the Company proposes to continue the relationship.
- Unusual or suspicious activity has been identified.
- Net deposits exceed USD 25,000 for corporate and retail clients (single transaction or aggregated over time). The Company reserves the right to apply EDD at lower thresholds where higher risks are identified.

7.2 EDD Measures

EDD measures that may apply for higher-risk business relationships include:

- Requesting additional information on the client, including occupation, volume of assets, and information from public databases.
- Obtaining additional information on the intended nature of the business relationship and source of funds/wealth.
- Obtaining information on intended or performed transactions.

Where the Company is unable to perform EDD as required, the business relationship shall be terminated and an STR filed with the FIU pursuant to applicable legislation.

7.3 Source of Funds (SOF)

Source of funds refers to the origin of the particular funds or assets that are the subject of the business relationship or transaction. SOF documentation is required when net deposits reach or exceed USD 25,000, for both retail and corporate clients, whether through a single transaction or aggregated over time:

Client Type SOF Required When
Natural Person (Individual) Net deposits reach or exceed USD 25,000 (single
transaction or aggregated over time)
Corporate / Entity / Trust / Net deposits reach or exceed USD 25,000 (single
Legal Body transaction or aggregated over time)

Kudo

7.4 Source of Wealth (SOW)

Source of wealth describes the origins of a customer's financial standing or total net worth. SOW documentation is required for all higher-risk customers, foreign PEPs, and other relationships where the product or service risk profile makes it appropriate. SOW documentation is required when net deposits reach or exceed USD 25,000, for both retail and corporate clients, whether through a single transaction or aggregated over time:

Client Type SOW Required When
Natural Person (Individual) Total transaction amount reaches or exceeds USD 25,000
Corporate / Entity / Trust / Net deposits reach or exceed USD 25,000 (single
Legal Body transaction or aggregated over time)

7.5 Crypto-Asset Activity

The Company recognizes that crypto-asset activity presents heightened ML/TF risk due to the pseudonymous nature of blockchain transactions, the speed of cross-border transfers, and the potential use of obfuscation techniques such as mixing and layering. Where a client's funds originate from, or are directed to, crypto-asset activity, Enhanced Due Diligence measures shall be applied in addition to standard CDD requirements.
The following circumstances shall automatically trigger EDD for crypto-related activity:

- The client transacts via a centralised or decentralised crypto-asset exchange, whether regulated or unregulated.
- The client uses a self-hosted (unhosted) wallet, including hardware wallets or software wallets not custodied by a regulated entity.
- The client's funds are traced to or from blockchain addresses flagged as high-risk, illicit, or sanctioned, as identified through DeusX blockchain analysis.
  Where crypto-asset activity is identified, the Company shall conduct blockchain analysis using DeusX, the Company's appointed blockchain analytics provider, to assess the risk profile of wallet addresses and transaction history. DeusX provides on-chain intelligence including wallet risk scoring, exposure analysis, and transaction tracing to support the Company's AML/CTF obligations.

The blockchain analytics assessment shall be documented, retained on the client file, and reviewed as part of ongoing monitoring. Where a wallet address is assessed as high-risk or severe, the Company shall: escalate the matter to the AMLCO and AML Compliance Committee; suspend processing of the transaction pending review; and consider filing a Suspicious Transaction Report (STR) with the FIU if the risk cannot be adequately mitigated.

The Company shall not process transactions connected to: sanctioned wallet addresses; mixer or tumbling services; unhosted wallets presenting an unacceptably high risk score without adequate client explanation; or jurisdictions subject to FATF call to action or enhanced monitoring where crypto-asset AML controls are identified as deficient.

7.6 EDD Documentation Completion

Where requested EDD documentation is not satisfactorily provided within seven (7) Calendar days from the date of request, the Company reserves the right to restrict, suspend, or freeze the client's account and related services until the required information has been received and reviewed

8. Politically Exposed Persons (PEPs)

PEPs are individuals who are or have been entrusted with prominent public functions (e.g., Heads of State or Government, Senior Politicians, Senior Government, Judicial or Military Officials, Senior Executives of State-owned Corporations, and important Political Party Officials) in foreign, domestic, or international organisations, as well as their family members and close associates.

Business relationships with PEPs pose a greater than normal money laundering risk by virtue of the possibility of having benefited from proceeds of corruption or other crimes.

The Company applies enhanced scrutiny and monitoring measures to all PEPs, their immediate family members, and close associates, using the Sumsub screening system and internal procedures.

9. Sanctions Screening

The Company conducts sanctions screening on all customers, beneficial owners, authorised representatives, directors, shareholders, counterparties, payees, payment beneficiaries, and

other relevant connected parties, both prior to onboarding and on an daily basis throughout the business relationship. Screening is conducted against: the United Nations Security Council (UNSC) sanctions lists; Mauritius domestic Targeted Financial Sanctions requirements under the United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019; and other relevant international sanctions lists maintained by the Company's screening provider, Sumsub.
The Company uses the Sumsub screening system for automated sanctions screening and ongoing monitoring.
The Company shall not knowingly establish or maintain a business relationship or process a transaction involving a sanctioned person, entity, jurisdiction, or prohibited activity. All sanctions screening alerts, investigations, decisions, escalations, and reports shall be documented and retained.

9.1 Targeted Financial Sanctions (TFS) – Freezing Obligations

The Company is required to immediately and without delay freeze the assets of designated persons upon identification. Freezing obligations extend to all assets owned or controlled, directly or indirectly, by designated persons, including non-cash assets. New freezes are implemented immediately and without prior notice to the designated person. The account of any designated person must not be closed, as this could result in funds being made available to the designated person. Freezing and unfreezing of assets shall take place within 24 hours of identifying and verifying the relevant Sanctions, in line with Sections 3 and 4 of the United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Act 2019. True sanctions matches and any associated asset freezing shall be reported immediately to the National Sanctions Secretariat Enforcement Committee (NSSEC) and the FSC, and an STR shall be filed with the FIU.

10. Customer Identification Program

Kudo has adopted a Customer Identification Program (CIP). We will provide notice that they will seek identification information; collect certain minimum customer identification information from each customer, record such information and the verification methods and results.

11. Notice to Customers

Kudo will provide notice to customers that it is requesting information from them to verify their identities, as required by applicable law.

12. Know Your Customers

When a business relationship is formed, to establish what might constitute normal activity later in the relationship, it is necessary for the company to ascertain the nature of the business a client expects to conduct.
Once an ongoing business relationship has been established, any regular business undertaken for that customer can be assessed against the expected pattern of activity of the customer. Any unexplained activity can then be examined to determine whether there is a suspicion of money laundering or terrorist financing.
Information regarding a client's income, occupation, source of wealth, trading habits and The economic purpose of any transaction is typically gathered as part of the provision of advice. At the start of the relationship personal information is also obtained, such as nationality, Date of birth, and residential address. These pieces of information should also be considered in respect to the risk of financial crime (including AML and CTF). For high-risk transactions, it might be appropriate to seek verification of the information the client has provided.

14. Identification

The standard identification requirement for customers who are private individuals are generally governed by the circumstances relating to the customer and the product type that is being dealt in, i.e. the level of risk attributed to the product whether it is a reduced risk, intermediate risk or an increased risk product. Taking that into account for reduced risk and intermediate risk products the following pieces of information are required as a standard ofidentification purposes:

- Full name
- Residential Address

15. Verification

Verification of the information obtained must be based on reliable and independent sources which might either be documents produced by the customer, or electronically by the firm, or by a combination of both. Where business is conducted face-to-face, firms should see originals of any documents involved in the verification.
If the identity is to be verified from documents, this should be based on either a government issued document which incorporates:

A. The customer's full name, and
B. Their residential address
C. Photographic Government issued documents or valid passport
D. National identity card; alternatively, this can be done by a non-photographic government issued document which incorporates the customer's full name, supported by a second document, which incorporates the customer's full name and their residential address.

16. Evidence of Address

A. Current bank statements, or credit/debit card statements, issued by a regulated financial sector firm (but not ones printed off the internet and not less than 3 months old)
B. Utility bills (not including mobile phone bills, not ones printed off the internet and not less than 3 months old)

For increased risk level products, in addition to obtaining the standard information detailed above, the following know your customer information should be obtained and recorded:

- Employment and income details
- Source of wealth (i.e. source of the funds being used in the transaction)

17. Transaction Monitoring and Reporting

Transaction based monitoring will occur within the appropriate business units of Kudo. Monitoring of specific transactions will include but is not limited to net deposits aggregating $25,000 or more and those with respect to which Kudo has a reason to suspect suspicious activity. All reports will be documented.

17.1 Transaction Monitoring

The Company uses Sumsub Transaction Monitoring to assess transactions in real time against configured AML/CTF rules, including transaction amount, frequency, repeated transactions, behavioural patterns, screening results, and transaction history. Transaction monitoring applies to all transactions, including those aggregating USD 25,000 or more. Rules add points to the transaction risk score, apply tags, place a transaction on hold for Manual review, or reject a transaction where high-risk criteria are met. Low-risk transactions are generally approved automatically. Medium-risk or held transactions are manually reviewed. High-risk transactions may be rejected or escalated.

17.2 Applicant Risk Scoring

The Company uses Sumsub to assess applicant risk based on configured AML/CTF rules, including onboarding information, customer profile, expected activity, screening results, geographic exposure, and other applicant risk indicators. Applicant risk scoring identifies low, medium, and high-risk applicants for appropriate review, monitoring, EDD, or Escalation.

17.3 Ongoing Monitoring

Existing business relationships are continuously monitored to identify and prevent potential ML/TF activity and to ensure consistency with the stated nature of the relationship. There are two types of ongoing monitoring:

- Transaction monitoring: Scrutiny of transactions to ensure they are consistent with the Company's knowledge of the client, its business, and risk profile (including source of funds).
- CDD maintenance: Ensuring that CDD data collected is kept up to date and relevant, through reactive reviews triggered by events and regular planned reviews at intervals determined by risk rating.

Additional monitoring arrangements for high-risk relationships include: more frequent CDD reviews; more regular transaction reviews; lower monetary thresholds for monitoring; reviews by persons not directly managing the relationship; and appropriate approval procedures for high-value transactions.

18. Suspicious Activity

There are signs of suspicious activity that suggest money laundering. These are commonly referred to as “red flags”. If a red flag is detected, additional due diligence will be performed before proceeding with the transaction. If a reasonable explanation is not determined, the suspicious activity shall be reported to the AML Compliance Committee.

18.1 Definition of Suspicious Transactions

A suspicious transaction is one where there are reasonable grounds to know or suspect that the transaction involves: laundering of money or proceeds of any crime; funds linked to or related to terrorism or terrorist activities; unjustifiable complexity; lack of economic or lawful objective; inability to identify the transacting party; or any other reason giving rise to suspicion.

18.2 Red Flag Indicators

Examples of red flags include:

- The customer exhibits unusual concern regarding the firm’s compliance with government reporting requirements and the firm’s AML policies, particularly with respect to 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 suspect 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 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 equivalents, or asks for exemptions from the firm's policies relating to the deposit of cash and cash equivalents.
- For no apparent reason, the customer has multiple accounts under a single name or multiple names, with many inter-account or third-party transfers.
- The customer's account has unexplained or sudden extensive activity, especially in accounts that had little or no previous activity.
- The customer's account has many 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 requests that a transaction be processed in such a manner to avoid the firm's normal documentation requirements.

18.3 Know Your Customer – The Basis for Recognising Suspicions

A suspicious transaction will often be one which is inconsistent with a customer's known, legitimate business or personal activities or with the normal business for that type of customer. Therefore, the first key to recognition is knowing enough about the customer's

business to recognise that a transaction, or series of transactions, is unusual.
Questions you must consider when determining whether an established customer's transaction might be suspicious are:

- Is the size of the transaction consistent with the normal activities of the customer?
- Is the transaction rational in the context of the customer's business or personal activities?
- Has the pattern of transactions conducted by the customer changed?

18.4 Suspicious Transaction Report (STR) Procedures

All staff members are required to submit an internal STR to the MLRO when encountering a suspicious transaction, client, or activity. The MLRO shall assess the information, determine whether there are reasonable grounds for suspicion, and forthwith report to the FIU where required.

- All staff submit internal STRs to the MLRO (via the CO where appropriate).
- An internal registry is maintained for all STRs whether or not submitted to the FIU, and updated monthly.
- An external registry is maintained for STRs submitted to the FIU.
- A maximum delay of five (5) working days applies for reporting the STR to the FIU after the MLRO becomes aware of suspicious activity.
- Failure to report within the prescribed period constitutes a criminal offence under the FIAMLA, liable to a fine not exceeding one million rupees and/or imprisonment for up to five years.
- STRs may be submitted to the FIU electronically or at the FIU building, 7th Floor, Ebene Heights, 34, Ebene Cybercity, Ebene, Republic of Mauritius (fax: +230 466 2431).

Following an STR, the Company shall: inform the relevant law enforcement agency or supervisory body; consider discontinuing or monitoring the business relationship; and commence an internal investigation on the client's accounts/business. Investigation results shall not be disclosed to anyone other than those with a legitimate need to know.

18.5 Tipping Off

Section 16(1) of the FIAMLA prohibits any person directly or indirectly involved in

reporting a suspicious transaction from informing any person involved in the transaction, or any unauthorised third party, that the transaction has been reported or that information has Been provided to the FIU.
The MLRO shall acknowledge receipt of all internal disclosures and provide guidance on avoiding tipping off the customer. If the Company reasonably believes that completing the CDD process will tip off the customer, it shall stop the CDD process and file an STR with the FIU. Great care shall be taken in the wording of any communications with clients when terminating relationships subject to STR filings.

18.6 Freezing of Accounts

Where it is known that the funds in an account derive from criminal activity, or that they arise from fraudulent instructions, the account must be frozen. Where it is believed that the account holder may be involved in the fraudulent activity that is being reported, the account may need to be frozen.

19. Withdrawal Policy

The Company applies a First-In, First-Out (FIFO) withdrawal policy as part of its AML/CTF and fraud prevention controls. Withdrawals shall, where applicable, be processed back to the original source of funding before alternative payment methods are used. Third-party funding and third-party withdrawals are strictly prohibited.The Company reserves the right to request additional verification documentation, delay processing, reject, or escalate withdrawal requests where suspicious activity, inconsistencies, or AML/CTF concerns are Identified.

20. Payment Processing

Kudo Systems Ltd (Cyprus, registration number HE 462202) acts as an appointed payment processing service provider for Kudo Trade (Mauritius) Ltd. Kudo Systems Ltd processes funds strictly in accordance with the instructions and oversight of Kudo Trade (Mauritius) Ltd.
All client onboarding, KYC, AML/CTF checks, transaction monitoring, and compliance oversight remain the responsibility of Kudo Trade (Mauritius) Ltd. Any suspicious activity

identified in connection with payment flows shall be escalated to the relevant Compliance Officer or MLRO immediately.

21. Record Keeping

The Company maintains comprehensive records in accordance with the FIAMLA and FIAML Regulations 2018. All records are available for inspection by the FSC at all times during office hours. The joint authorisation of the CO and one Director is required before destruction of any record.
Record Type Minimum Retention Period
Client verification, due diligence, client 7 years from the date on which the business
agreements, complaints, and other client- relationship ended
related documentation
Financial statements and reports 7 years from the date on which the statement
or report was provided
Transaction records (domestic and 7 years after completion of the transaction
international)
Copies of all STRs and related At least 7 years from the date the report was
documentation submitted to the FIU made
All other records not specifically mentioned Minimum 7 years

22. Enquiries

For further AML/CFT related queries, please contact: contact@kudo.com