Anti- Money Laundering Policy

Contents

Statement of Board of Directors

Banex Capital LTD., formed under the registration number 2024-00259, has a board of directors dedicated to maintaining the greatest standards of corporate integrity. This dedication guarantees moral behavior in all facet of the business's activities, fostering long-term stakeholder value and confidence.

The Board has put in place a strong Anti-Money Laundering (AML) Policy to support this. By outlining precise protocols for identifying and reporting questionable activity, this policy aims to stop money laundering and the funding of terrorists.

Senior management and all other staff members are required to read and abide by the AML Policy and its associated protocols. Compliance is required, and infractions will be dealt with appropriately.

By adhering to these principles, Banex Capital LTD safeguards its reputation, maintains stakeholder trust, and contributes to a safer and more secure financial environment.

Scope of Application

All Banex Capital LTD employees and senior management are subject to the AML Policy. With the exception of situations when more stringent procedures are in place, it takes precedence over any conflicting internal regulations. This policy reflects our unwavering dedication to stopping the financing of terrorism and money laundering. By putting compliance first, maintaining moral principles, and creating a safe financial environment, we reaffirm our commitment to preserving the integrity of our business processes and preserving stakeholder confidence.

Regulatory Framework

Banex Capital LTD demonstrates unwavering commitment to upholding the highest standards of compliance by rigorously adhering to the AML/CFT laws and regulations stipulated in Saint Lucia. Our resolute dedication to compliance is driven by the recognition that any deviation from these paramount laws can lead to severe repercussions, encompassing substantial penalties, potential legal ramifications, and irreparable harm to our esteemed reputation.

Listed hereunder are the meticulously observed laws and regulations governing company incorporation and vigilant monitoring in the esteemed jurisdiction of Saint Lucia:

Companies Act, 1996	This is the primary legislation governing the incorporation, operation, and dissolution of companies in Saint Lucia. It outlines the requirements for company formation, shareholder rights, director duties, and other essential corporate matters.
International Business Companies Act, 1999	This act governs the establishment and regulation of International Business Companies (IBCs) in Saint Lucia. IBCs enjoy certain tax advantages and are subject to specific regulatory provisions.
Limited Liability Company Act, 2009	This act provides for the formation and management of Limited Liability Companies (LLCs) in Saint Lucia. LLCs offer limited liability to their members and are subject to specific legal provisions.
Companies (Amendment) Act, 2011	An amendment to the Companies Act, introducing changes and improvements to the original act.
Registration of Business Names Act, 1959	This legislation governs the registration and usage of business names in Saint Lucia by individuals or partnerships.
Partnership Act, 1998	The Partnership Act regulates the establishment, operation, and dissolution of partnerships in Saint Lucia.
Securities Act, 2001	This act deals with the regulation and oversight of securities and capital markets in Saint Lucia.
Financial Services Regulatory Authority Act, 2013	This legislation established the Financial Services Regulatory Authority (FSRA) in Saint Lucia, which oversees financial services and certain types of companies operating within the financial sector.

Money Laundering & Terrorist Financing

Money laundering is the process of concealing the origins of illegally obtained funds to make them appear legitimate. This involves channeling proceeds from criminal activities, such as drug trafficking, fraud, corruption, or other illegal actions, through a series of complex financial transactions. The primary objective is to obscure the illegal source of the money, making it difficult for authorities to trace it back to its criminal origins.

The money laundering process typically involves three key stages:

- Placement: Introducing illicit funds into the financial system.
- Layering: Conducting multiple transactions to obscure the money's trail.
- Integration: Reintroducing the "cleaned" money into the legitimate economy.

Terrorist financing, on the other hand, involves providing financial support or resources to facilitate terrorist activities, including planning, preparation, and execution. Unlike money laundering, terrorist financing may involve funds from both legitimate and illegitimate sources, including donations, criminal enterprises, or state sponsorship. These funds are used to recruit members, train operatives, purchase weapons, and execute terrorist agendas.

Disrupting the financial networks that support terrorist organizations is crucial for undermining their operations and protecting global security.

Both money laundering and terrorist financing pose severe risks to the global financial system and national security. To counter these threats, regulatory bodies, financial institutions, and law enforcement agencies collaborate globally to enforce strict Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) measures. These efforts aim to:

- Detect and prevent illicit activities.
- Safeguard the integrity of the financial system.
- Uphold ethical standards.
- Protect societies from the devastating consequences of financial crimes and terrorism.

Through vigilance and cooperation, the global community strives to ensure a more secure and transparent financial landscape.

Risk Management

Effective risk management for money laundering and terrorist financing involves identifying, assessing, and mitigating associated risks to maintain the integrity of the financial system. Key strategies include:

- Client Due Diligence (CDD): Verifying client identities, assessing financial activities, and conducting enhanced checks for high-risk clients such as politically exposed persons (PEPs) or those from high-risk jurisdictions.
- Transaction Monitoring: Employing advanced systems to detect suspicious transactions and activities in real-time, enabling timely reporting of potential illicit behavior.
- Suspicious Activity Reporting (SAR): Establishing mechanisms for reporting suspicious activities to relevant authorities, facilitating investigations into potential criminal activities.
- Compliance and Oversight: Ensuring strict adherence to AML and CTF regulations through audits and continuous improvement of compliance processes.
- Training and Awareness: Educating employees on identifying red flags and their reporting obligations to strengthen organizational vigilance.
- Risk-Based Approach (RBA): Allocating resources to focus on higher-risk clients, products, and jurisdictions.

- Technology and Data Analytics: Leveraging advanced tools to identify patterns linked to money laundering or terrorist financing.
- Sanctions Screening: Regularly screening clients and transactions against global sanctions lists to block prohibited entities.
- Internal Controls: Promoting a strong compliance culture and implementing robust internal controls to uphold ethical practices.
- Information Sharing: Encouraging collaboration among financial institutions, regulators, and law enforcement to share insights and best practices.

Stages of Money Laundering

Money laundering involves three primary stages:

- Placement: Introducing illicit funds into the financial system, often through small, structured transactions or deposits.
- Layering: Concealing the origin of funds via complex transactions such as offshore transfers, wire transactions, or shell companies.
- Integration: Reintroducing the "cleaned" money into the legitimate economy through investments, luxury purchases, or business ventures.

Sophisticated AML measures and international cooperation are essential to disrupt this process and prevent financial crime. The financial support for criminal enterprises and protect the integrity of the global financial system.

Risk Matrix & Methodology

A risk matrix combines the likelihood and impact of events to assess their severity.

- Probability Ratings
- Improbable: Extremely unlikely to occur.
- Remote: Unlikely but possible.
- Occasional: Likely to occur at some point.
- Probable: Will occur several times.
- Frequent: Expected to occur often.

Impact Levels

- Insignificant: Minimal disruptions or financial loss.
- Minor: Moderate disruptions requiring straightforward mitigation.
- Moderate: Significant consequences requiring strategic response.
- Major: Severe disruptions affecting operations or reputation.

- Severe: Catastrophic consequences threatening organizational survival.

Risk Prioritization:

Probability	Insignificant	Minor	Moderate	Major	Severe
Improbable	Extremely Low	Low	Low	Medium	High
Remote	Low	Low	Medium	high	Very high
Occasional	Low	Medium	Medium	High	Very High
Probable	Medium	Medium	High	High	Critical
Frequent	High	High	High	Critical	Critical

This structured approach enables organizations to prioritize and allocate resources effectively, ensuring resilience against uncertainties and threats.

Know Your Clients

Definition of Client

In our Anti-Money Laundering (AML) policy, understanding the concept of "client" is paramount. A "client" refers to any individual, organization, or entity that engages in transactions with our company, including purchasing goods, accessing services, or performing financial activities. As a financial institution committed to upholding the highest standards of integrity and compliance, we view our clients as key stakeholders. We recognize our responsibility to ensure that all interactions with clients adhere to the relevant AML and Counter-Terrorist Financing (CTF) regulations.

Type of Client

This policy is implemented through specific procedures, established in accordance with the requirements of applicable legislation and includes the utilization of relevant information systems for monitoring of transactions and development of Know Your Client («KYC») policy.

The Company apart from establishing the identity of its clients, also monitors account activity to determine those transactions that do not conform with the normal or expected transactions for that client or type of account. KYC constitutes a core feature of services' risk management and control procedures. The intensity of KYC programs beyond these essential elements is tailored to the degree of risk. KYC policy used by the Company is aimed at prevention of Money Laundering and limitation of inherent risks, its main components are Client Acceptance Policy, Client Identification procedures,

monitoring of transactions and accounts and risk management.

Our client base is diverse, and it is essential to categorize clients based on their characteristics and associated risks. These categories include:

- Individual Clients: Natural persons engaging in personal transactions, such as opening accounts, making purchases, or conducting financial activities for personal purposes.
- Corporate Clients: Legal entities, such as businesses, companies, and partnerships, that engage in transactions for commercial or business-related activities.
- Politically Exposed Persons (PEPs): Individuals holding significant public roles or positions of influence. Due to their vulnerability to corruption and financial crimes, PEPs are classified as high-risk and require enhanced due diligence.
- High Risk Clients: Clients who may present higher risks based on factors such as geographic location, business activities, or sources of funds. These clients undergo more robust scrutiny and risk management measures.
- Medium Risk Clients: Clients who exhibit minimal risks in terms of money laundering or terrorist financing activities but requires manual verification or additional KYC documentation while onboarding.
- Low Risk Clients: Clients who exhibit minimal risks in terms of money laundering or terrorist financing activities. Standard due diligence procedures apply to this group.

Client Acceptance Policy

Our Client Acceptance Policy governs the criteria and procedures for onboarding new clients and establishing business relationships. We define the following risk levels with applicable actions The key components of this policy include:

- Risk-Based Approach: We evaluate and accept clients based on their risk profile, applying a higher level of due diligence to clients perceived as higher-risk.
- Client Due Diligence (CDD): As part of the acceptance process, we verify the client's identity, understand the nature of their business, and assess the source of their funds.
- Enhanced Due Diligence (EDD): For higher-risk clients, such as PEPs or certain business entities, we implement more stringent measures to assess their backgrounds and evaluate potential risks associated with the relationship.
- Ongoing Monitoring: The policy includes provisions for continuous monitoring of client relationships to ensure that any changes in behavior or risk profile are identified and addressed.
- By adhering to this policy and categorizing clients based on risk, we ensure that we build trusted relationships while maintaining a secure and compliant business environment.

Our client acceptance policy includes the following key principles:

- Proper Identification: Clients must undergo thorough identification processes. Those who cannot be properly identified will not be accepted.
- Blacklisted Clients: We do not establish business relationships with clients who are blacklisted or categorized as "Unwanted Clients." This measure protects us from associating with individuals or entities involved in suspicious activities.
- OFAC SDN and UN Consolidated List: Clients on the Office of Foreign Assets Control (OFAC) Specially Designated Nationals (SDN) list or the United Nations "Consolidated List" will not be accepted.
- No Anonymous or Fictitious Names: We will not engage with anonymous clients or those using fictitious names. Transparency and proper identification are prerequisites for all client relationships.
- Legitimacy of Business and Funds: We will not accept clients whose business activities or funds cannot be verified or whose sources are inconsistent with their financial status.
- Submission of Relevant Documentation: Clients must submit necessary documentation in proper form. Failure to comply will result in non-acceptance.
- Suspected Criminal Activities: Clients involved in criminal activities, such as drug trafficking, terrorism, or organized crime, will not be accepted. This ensures we maintain a compliant and secure financial environment.

Based on the above we have built the following acceptance approach

- Low Risk Clients: accepted per se.
- Medium Risk Clients: additional KYC arrangements imply.
- High Risk Clients: Enhance due diligence applied, clients can be refused in service.
- Unacceptable Risk Clients: refused in service.

Policy for Categorizing Client Risk

The "Policy for Categorizing Client Risk" is a structured approach that our organization uses to assess and categorize clients based on their risk profiles in relation to money laundering and terrorist financing. This policy enables us to effectively manage and reduce potential risks linked to our client base. Below is a detailed explanation of the key components of the policy:

Risk Factors Assessment: We evaluate factors like geography, business activity, source of funds, and transaction patterns to determine risk levels.

PEPs Identification: Special attention is given to Politically Exposed Persons (PEPs), who undergo enhanced due diligence due to their higher corruption and financial crime risks.

Risk Categorization**:** Clients are classified into:

- Low Risk: Minimal risk factors.

Clients who successfully passed KYC from the first attempt.

- Medium Risk: Moderate risk requiring additional monitoring.

Clients who provided cropped or low readable documents.

- High Risk: Significant risk, including PEPs and clients from high-risk areas.

Clients that have had discrepancies in provided ID Information and documents without proper explanations. Clients qualified as PEPs (Politically Exposed Persons) or persons known to be close associates of PEPs.

- Unacceptable Risk:

Clients who have been prosecuted for financial crimes;

Clients who are citizens of or reside in territories under FATF Increased Monitoring (https://www.fatf-gafi.org/content/fatf-gafi/en/publications/High-riskand-other-monitored-jurisdiction s/Increased monitoring-february-2024.html)

Clients on a terrorist wanted and/or other sanction lists: the United Nations (UN) Security Council consolidated sanctions list, the EU's consolidated list of persons, groups, and entities, the US Department of the Treasury, Office of Foreign Assets Control (OFAC) sanctions lists, the US Department of the Treasury, Financial Crimes Enforcement Network (FinCEN) list, the UK HM Treasury (HMT), Office of Financial Sanctions Implementation, "consolidated list of targets")

Due Diligence:

- Low Risk: Basic registration form and ID.
- Medium Risk: ID, proof of address, and additional document upon Company's consideration.
- High Risk: Enhanced due diligence, detailed report, and supporting documentation, client can be refused in service.
- Unacceptable Risk: Client is refused in service.

Enhanced Monitoring: High-risk clients are subject to continuous monitoring and additional verification.

Compliance: This policy ensures compliance with Anti-Money Laundering (AML) and Counter Terrorism Financing (CTF) regulations.

Special Cases: Documentation is required for specific fund sources, such as real estate sales or severance payments.

Client Identification

Clients must provide valid ID documents (e.g., passport, driver's license). Expired or deteriorated documents are not accepted.

Watchlists & Verification

Clients are screened against relevant lists like the OFAC and UN sanctions lists, as well as internal "Unwanted Clients" and PEPs lists.

Monitoring Policy & Suspicious Transactions Report

Definition of Suspicious Transactions

A suspicious transaction is any financial activity that deviates from a client's usual behavior or expected norms for legitimate business. Such transactions may indicate potential illegal activities and require further investigation.

- Unusual Nature: Large, frequent, or irregular transactions that differ significantly from normal behavior.
- Inconsistent with Client Profile: Transactions not matching a client's known activities (e.g., sudden large international transfers).
- Lack of Business Purpose: Transactions with no clear rationale, such as unexplained third party payments.
- Involvement in Illegal Activities: Potential signs of money laundering, fraud, or terrorism financing.
- Fraud or Financial Crimes: Indicators of scams, embezzlement, or tax evasion.
- Concealment: Transactions designed to evade detection thresholds.
- High-Risk Jurisdictions: Involvement of parties from jurisdictions with weak AML controls.

Identifying suspicious transactions does not imply illegal activity but signals the need for investigation.

Control of Suspicious Transactions

Effective controls ensure that suspicious activities are detected, reported, and addressed promptly.

- Transaction Monitoring System: Use systems to detect suspicious transactions based on predefined rules.
- Threshold Reporting: Set transaction limits, triggering alerts when exceeded.
- Automated Alerts & Flagging: Ensure timely responses to potential suspicious activities.
- Enhanced Due Diligence (EDD): Apply additional scrutiny for high-risk clients or jurisdictions.
- Suspicious Transaction Reporting (STR): Report suspicious activities to authorities.
- Compliance Oversight: Assign a dedicated officer to monitor compliance and reporting.
- Training & Awareness: Regular training to recognize suspicious transactions.
- Internal Investigation Procedures: Establish protocols for investigating flagged transactions.
- Client Due Diligence (CDD): Collect and update client information to detect anomalies.
- Record Keeping: Maintain transaction records for compliance and potential investigations.

Red Flags

Indicators that may suggest suspicious activity include:

- Large Cash Transactions: Inconsistent with typical client behavior.
- Frequent Structuring: Transactions split to avoid reporting limits.
- Rapid Fund Movement: Sudden or frequent transfers with no clear purpose.
- High-Risk Jurisdictions: Transactions involving high-risk regions.
- Politically Exposed Persons (PEPs): Increased risk due to possible corruption.
- Incomplete or Inconsistent Information: Difficulty verifying client details.
- Unusual Business Activities: Transactions unrelated to the client's business.
- Third-Party Payments: Payments from unrelated third parties.
- Geographic Anomalies: Involvement of tax havens or weak regulations.
- Anonymous Transactions: Transactions involving concealed beneficiaries.
- Unusual Client Behavior: Reluctance to provide necessary information.

Suspicious Transactions Report (STR)

An STR is filed when suspicious activity is detected, aiming to alert authorities and prevent financial crime.

- Purpose: Report transactions linked to money laundering, fraud, or terrorism financing.
- Content: Includes client details, transaction specifics, and a narrative of suspicious behavior.
- Filing: STRs are promptly submitted to the relevant authorities.
- Confidentiality: STRs are kept confidential to protect the investigation and parties involved.
- Impact: Authorities investigate the report and take appropriate action.
- Compliance Obligation: Failure to report suspicious activities can lead to penalties.

Record Keeping

All relevant documentation must be securely stored for a minimum of 7 years for regulatory compliance.

- KYC Documentation: Retain identification and transaction records.
- Transaction Records: Keep certified copies of all executed transactions.
- Unusual Operations Reports (UORs): Maintain records of suspicious activities.
- STRs & Supporting Documentation: Store STRs and related information for 7 years.

Confidentiality

Strict confidentiality is maintained in all aspects of suspicious transaction management:

- Non-Disclosure: Information regarding STRs must not be shared with unauthorized parties.
- Confidentiality of Actions: All actions related to anti-money laundering efforts are confidential.
- Exclusion from Client Files: STRs are not included in client files.
- Compliance Oversight: The Compliance Officer ensures confidentiality protocols are followed.
- Disciplinary Measures: Non-compliance with confidentiality rules will lead to disciplinary actions.
- Non-compliance will result in strict disciplinary actions, including potential criminal sanctions.

We consider confidentiality vital in preserving trust, regulatory compliance, and protecting our clients' interests.

Know Your Employee Policy (KYE Policy)

Implementation:

Our KYE policy is designed to ensure that each employee undergoes a comprehensive and rigorous onboarding process, aimed at verifying their identity and suitability for their respective roles. This process requires employees to submit accurate self-declarations of their qualifications, experience, and any potential conflicts of interest. In addition to self-declarations, we rigorously verify the authenticity of educational qualifications and professional experience provided by employees, ensuring that the information presented during recruitment is both truthful and accurate. To maintain up-to-date and precise records, regular reviews and updates of employee information are conducted. As part of their orientation, employees undergo training that emphasizes the importance of compliance, ethical behavior, and a clear understanding of the KYE policy, reinforcing our commitment to transparency and integrity across the organization.

Performance Evaluation and Rewards:

Adherence to the KYE policy, alongside compliance with other organizational policies, is an essential aspect of employee performance evaluation. Employees who consistently uphold ethical standards, demonstrate compliance, and contribute positively to the workplace culture are formally recognized and rewarded. We encourage employees to actively promote compliance and to report any suspicious activities, with structured incentives and recognition provided to those who go above and beyond in fostering a culture of accountability. This not only strengthens the workforce’s commitment to ethical conduct but also incentivizes proactive engagement in upholding the company's high standards.

Disciplinary Measures:

Any breach of the KYE policy, such as providing false information, omitting relevant details, or engaging in deceptive practices, will be thoroughly investigated. When a violation is suspected, an internal inquiry is immediately initiated to collect and assess all facts and determine the extent of the breach. Depending on the severity and nature of the violation, corrective actions will be implemented, following a fair and progressive disciplinary approach. These actions may include counseling, additional training, suspension, or, in extreme cases, termination of employment. Our policy also emphasizes the protection of whistleblowers, ensuring that employees who report violations in good faith are shielded from any form of retaliation or adverse consequences, thereby fostering a secure and supportive environment for individuals who bring concerns to light.

Staff Training Policy

Our staff training program is a cornerstone of cultivating a highly skilled and compliant workforce. Led by our experienced Compliance Officer, these comprehensive training sessions are designed to equip employees with the essential knowledge and skills needed to navigate the complexities of regulatory frameworks and industry standards.

Throughout the training process, employees gain an in-depth understanding of our internal policies, legal obligations, and regulatory requirements. They are trained to identify and effectively mitigate potential risks, particularly those associated with financial crimes such as money laundering, fraud, and terrorist financing. Employees are taught how to recognize suspicious activities and the correct protocols for reporting such activities, including filing Suspicious Transaction Reports (STRs) and Unusual Operations Reports (UORs) in a timely and accurate manner.

A strong focus is placed on data privacy, confidentiality, and client due diligence to ensure the protection of sensitive information and guarantee ongoing compliance with legal and regulatory standards. Practical exercises, including role-playing scenarios and real-life case studies, empower employees to apply their knowledge in realistic situations, reinforcing their ability to act swiftly and effectively when necessary.

To ensure our team remains up-to-date and fully prepared to manage emerging risks, we conduct regular refresher training sessions and provide timely updates on regulatory changes. This continuous investment in staff development ensures that our employees uphold the highest standards of integrity, ethics, and compliance.

Through robust training, we foster a proactive and vigilant workforce that consistently builds trust among our stakeholders. By maintaining a high level of preparedness, we reinforce our reputation as a responsible and compliant organization in the industry.

Annex I - KYC Documents & Checks Samples

The following personal information is collected from “individual or retail” clients:

1. Client's true name and/or names used as these are stated on the official identity card or passport.
2. Client's date and place of birth (DOB)
3. Address and country of residence
4. Mobile/phone number
5. E-mail address
6. Copy of the passport or ID card
7. Copy of a document confirming residential address as per the example below

POI accepted	POR accepted (Validity 6 months)
Passport	Government Organization - Tax Bill
ID Card	Government Organization - Other (these can be temporary registration sheets, arrival sheets, certificates of state registration of rights, certificates of family composition issued at the State Services, affidavits, vehicle registration certificates.)
Driving License	Utility Provider - bill (electricity, water supply, heating, gas, sewerage, household waste disposal, house/elevator maintenance)
Residence Permit	Utility Provider - Telecom (home phone, internet, TV bills (but not for satellite TV and other wireless services)
Work Permit	Utility Provider - Other (other documents that show the receipt and payment of utility and maintenance bills in the home of residence)
	Bank statement
	Identity document with address on if another document was provied as POI

In the case of “corporate or institutional” clients, the following details are required:

- Full company name
- Company registration number
- Country of registration/incorporation
- Company’s address
- Mobile/phone number
- E-mail address

Note that some corporate documents may contain multiple pieces of the information as per below list:

- Memorandum and Articles of Incorporation
- Certificate of Incorporation
- Applicant business description, if regulated activity - copy of the license
- List of Directors and Shareholders
- Details of the registered office and place of business
- Copy of latest audited accounts; Or an explanation why these are absent. If the company is older than 2 years - signed by the director management's accounts
- Certificate of Good Standing or similar
- Structural chart of the company
- Complete set of documents for ubo/shareholders/directors per the list below
- Signed and dated board resolution authorising the person who acts on its behalf (Annex II) Plus for each UBO/shareholder (holding 20% or more of the voting power directly or indirectly of the

applicant for business)

- Copies of documents required on the Individual per the list for individual/ retail clients *And*
- Signed declaration of source of funds.

Client Screening

The Company utilises the **online third-party KYC verification tools (SumSub)** system to aid in the automated screening of clients, in order to detect and assess whether the client is subject to EU/UN and international sanctions, politically exposed person (PEP), convicted or suspected criminal and negative adverse media.

The Company ensures that the screening system is appropriate to the nature, size and ML/TF risks of the Company. Screening is performed on clients before:

- The establishment of a business relationship
- The provision of any services; and
- Undertaking any transactions for a client.

Thereafter, monitoring is undertaken on an ongoing basis for clients and clients' related entities, directors and beneficial owners. Further to this the Company ensures:

- That client's data used for ongoing screening is up to date and correct
- That there is a full understanding of the capabilities and limits of the automated screening system
- That the automated screening system can be tailored in line with the Company's risk appetite and perform regular reviews of the calibration and rules to ensure its effective operation.

The Company has implemented controls that require referral to the AMLCO prior to dealing with flagged persons.

Upon identification of a match using verification tools, the Back-Office officers investigate the potential match to ascertain if it is an actual match to the client or if it is a false positive. The Back Office officers are further checking the client via WolrdCheck's system or similar. If a potential match is found, Back Office officers refer to the AMLCO for further direction. The AMLCO will:

- Notify senior management
- Freeze accounts where appropriate and where an actual target match is identified
- Keep a clear, documented audit trail of the investigation of potential target matches and the decisions and actions taken, such as the rationale for deciding that a potential target match is a false positive
- Instruct to refund and terminate business relationships with such clients if necessary. • PEP and Sanctions screening is undertaken on a daily basis using the software of a third-party provider (SumSub).

After the collection of the data, the following documents can be requested in order to verify the identity of the client:

- Individual client: a high resolution scanned copy or photo of a passport or any other national ID issued by competent authorities of their country of origin, indicating family name and name, date and place of birth, passport number, issue and expiry dates, country of issue and Client's signature
- Corporate client: a high-resolution copy of documents showing the existence of the entity, such as: Certificate of Incorporation, Certificate of Good Standing, Articles of incorporation, a government issued business license (if applicable), etc.

As a proof of address of the individual/corporate client, one of the following documents can be requested:

- A copy of a utility bill (fixed-line phone or mobile phone bill, home internet bill, water bill, electricity bill) issued within the last 6 months
- A copy of a bank statement. Or Credit Card statement issued within the latest 6 months
- A copy of a bank reference letter that is no more than 6 months old
- Signed Tenancy Agreement
- Latest tax notification

Please see herewith a summary of the POI & POR Documents which are acceptable:

POI accepted	POR accepted (Validity 6 months)
Passport	Government Organization - Tax Bill
ID Card	Government Organization - Other (these can be temporary registration sheets, arrival sheets, certificates of state registration of rights, certificates of family composition issued at the State Services, affidavits, vehicle registration certificates.)
Driving License	Utility Provider - bill (electricity, water supply, heating, gas, sewerage, household waste disposal, house/elevator maintenance)
Residence Permit	Utility Provider - Telecom (home phone, internet, TV bills (but not for satellite TV and other wireless services)
Work Permit	Utility Provider - Other (other documents that show the receipt and payment of utility and maintenance bills in the home of residence)
	Bank statement
	Identity document with address on if another document was provied as POI

Once the KYC documents have been verified, a monitoring activity of financial transactions and accounts is required in order to understand the nature of the client's activities and identify those clients who may pose a potential high risk of money laundering.

Enhanced Due Diligence

Further documentation, explanations or details might be needed in case of:

- Identified "high risk" accounts or suspected "high risk" accounts or
- Client's total deposits exceeding 75,000 USD or
- Total monthly deposits exceeding 50,000 USD

In such a case, Versus Trade must:

- Seek further information directly from the client, from online research and/or third-party sources in order to obtain any additional information to clarify the nature and purpose of the client's activities
- Obtain information and supporting documents and Complete the Source of the funds/wealth form per the Appendix samples.

A verified profile is created for each new client that contains all relevant KYC information and all documents submitted by the client, stored in electronic format in a designated directory on the Company's servers.

The client's profile is frequently reviewed and updated throughout the operation of the account and all the information contained therein, and other information related to the operation of the account that is kept in electronic form is retained for a period of five years after the business relationship with the client has ended or the last transaction was carried out.

The Company screens all clients during the commencement of business relationship with the clients but also on an ongoing basis. As such, automated solutions check all clients on a daily basis versus all updated lists, regardless of their activities within their accounts. The Company takes further actions according to the results of the automated screenings.