DIRECTIVE ON COMBATING MONEY LAUNDERING AND TERRORIST FINANCING

Company Name: Foxchange AG
Directive Version: 1.0
Effective Date: [Draft]

Prepared in accordance with:
Art. 82 VQF SRO Regulations
VQF Guideline Doc. No. 913.1e

EXECUTIVE SUMMARY

These Internal Directives set out F AG's policies and procedures to comply with the Swiss Anti-Money Laundering Act (AMLA) and the Self-Regulatory Organization (SRO) Regulations of VQF. Key areas covered include:

- Due diligence obligations for customer onboarding and monitoring
- Risk assessment and management of increased-risk relationships and transactions
- Special measures for handling Politically Exposed Persons (PEPs)
- Responsibilities of employees, management, and the AMLA Special Department
- Clear assignment of reporting obligations to MROS
- Structured training for all AML-relevant personnel
- Proper use and oversight of third-party service providers (e.g., Ondato, UAB – “Ondato”, Crystal Blockchain B.V - Crystal Intelligence, Sum and substance LTD - “Sumsub”)

The Directive applies to all employees, departments, and any third parties engaged for compliance functions. It establishes a strong compliance framework that meets the standards of VQF Doc. No. 913.1e and ensures that the Company’s business operations align with Swiss regulatory expectations.

TABLE OF CONTENTS

DEFINITIONS AND ABBREVIATIONS

AMLA	The Swiss Anti-Money Laundering Act (SR 955.0), which establishes obligations for financial intermediaries to prevent and detect money laundering and terrorist financing.
VQF SRO Regulations	Binding regulatory framework issued by the VQF Self-Regulatory Organisation, applicable to its members operating under AMLA.
Company	Foxchange AG - the financial intermediary to which this Directive applies, including its Board of Directors, Executive Management, and operational departments.
Customer	Any natural or legal person with whom the Company enters into a business relationship, either directly or through an intermediary.
Business Relationship	A contractual or factual relationship of ongoing nature between the Company and the customer, typically involving repeated or continuous transactions.
Beneficial Owner	The natural person who ultimately owns or controls a customer or on whose behalf a transaction is conducted, as defined in Articles 4 and 31–51 of the VQF SRO Regulations.
Politically Exposed Person (PEP)	A person who is or has been entrusted with prominent public functions, including their close family members and associates. Foreign PEPs are always treated as increased risk; domestic PEPs may be depending on other risk indicators.
Increased Risk Customer	A customer whose profile or behavior presents elevated money laundering or terrorist financing risk, requiring enhanced due diligence in accordance with Articles 55–61 of the SRO Regulations.
Customer Due Diligence (CDD)	The process of identifying and verifying the identity of customers and beneficial owners, understanding the purpose of the relationship, and performing ongoing monitoring.
Enhanced Due Diligence (EDD)	Additional controls applied to increased risk customers or transactions, including more extensive verification of source of funds, business activity, and transaction plausibility.
Risk-Based Approach	A regulatory principle requiring that controls and monitoring intensity be proportionate to the customer’s risk profile and the nature of the relationship.
Threshold Amount	A transaction amount or frequency used to determine whether a transaction deviates significantly from the customer's expected activity, as per Article 59 para. 2 of the SRO Regulations.
Tipping-Off (Ban on Information)	The legal prohibition against informing a customer or third party that a suspicious activity report has been or may be filed, in accordance with AMLA Art. 10a and Art. 68 of the SRO Regulations.

AMLA Officer	The person responsible for implementing and overseeing AMLA compliance, reporting suspicious activity to MROS, freezing assets, and enforcing the ban on information.
Compliance Committee	An internal body composed of the AMLA Officer and the Board of Directors, responsible for oversight of escalated AML cases and approval of increased risk customer relationships.
MROS	The Money Laundering Reporting Office Switzerland, the central reporting body under AMLA for receiving and processing suspicious activity reports.
Forms and Documentation	- **VQF Form 902.4**: Customer Risk Profile
	- **VQF Form 902.5**: Customer Profile
	- **Form A/T**: Declaration of beneficial ownership or third-party control, as required.

1. PURPOSE/BASIC PRINCIPLES OF THE INTERNAL DIRECTIVE

This Anti-Money Laundering (AMLA) Directive establishes the foundational principles, risk-based approach, and internal responsibilities adopted by Foxchange AG ("the Company") in the prevention of money laundering and terrorist financing. It is designed to ensure compliance with the Swiss Anti-Money Laundering Act (AMLA), the Anti-Money Laundering Ordinance of FINMA (AMLO-FINMA), and the directives of the Company's Self-Regulatory Organisation (SRO), such as the VQF.

This Directive reflects the Company's proactive commitment to preventing the misuse of its services for illicit financial activities and to maintaining the integrity of the financial system. It outlines the framework for detecting, managing, and escalating potential money laundering risks, as well as the assignment of internal roles and responsibilities.

The AMLA Directive serves as the overarching compliance document within the Company's internal control system and is binding upon all employees, officers, and representatives. It forms the legal and procedural basis for the implementation of subordinate Instructions, including the Customer Onboarding Instruction and the Order Execution Instruction, which operationalize the regulatory obligations defined herein.

The Company acknowledges that the nature of its services—particularly involving virtual asset exchanges and cross-border transactions—may inherently carry Increased money laundering and reputational risks. As such, it adopts a robust, risk-based approach, consistent with international standards as set out by the Financial Action Task Force (FATF).

This Directive applies to all business relationships and transactions processed by the Company, and to all natural persons and legal entities acting on behalf of or in connection with the Company in its regulated activities. It also governs the behavior and accountability of employees and decision-making bodies with respect to client due diligence, transaction monitoring, reporting obligations, and record-keeping.

2. SCOPE OF THE INTERNAL DIRECTIVES

This AMLA Directive applies to all business activities conducted by the Company that fall under the scope of the Swiss Anti-Money Laundering Act (AMLA) and relevant Self-Regulatory Organisation (SRO) regulations, particularly those of VQF.

The Directive is binding for all employees, departments, and third-party agents acting on behalf of the Company, specifically those involved in:

- Establishing or managing business relationships;
- Conducting customer due diligence (CDD) and ongoing monitoring;
- Processing or executing financial or virtual asset transactions;
- Performing compliance checks, reporting obligations, or risk assessments;
- Maintaining customer records and internal controls related to AML compliance.

In cases where only part of the Company's business activities are subject to AMLA, this Directive applies exclusively to those operational areas, services, and roles where AMLA obligations are triggered. This includes, in particular, the onboarding of natural persons and legal entities, the exchange of fiat and virtual assets, and related financial intermediation services.

Employees must be fully aware of whether their function falls within the AMLA-regulated scope and must comply with all procedures and responsibilities outlined in this Directive and its subordinate Instructions — specifically, the Instruction on Establishing Customer Relationships and the Instruction on Order Execution.

Any updates to the scope of regulated activity, business model, or relevant regulatory interpretations must be reflected in an updated version of this Directive and immediately communicated to affected staff.

3. DUE DILIGENCE OBLIGATIONS PURSUANT TO THE AMLA AND SRO REGULATIONS

In compliance with the Anti-Money Laundering Act (AMLA) and the Regulations of the VQF Self-Regulatory Organisation (Doc. No. 400.1.2, effective 1 January 2025), the Company has implemented a full due diligence framework that governs all aspects of the customer lifecycle. This chapter outlines the procedures and operational practices by which the Company ensures the proper identification of customers and beneficial owners, creation of customer profiles, ongoing monitoring of business relationships, and fulfillment of reporting and recordkeeping duties. These practices apply to all business relationships, both permanent and occasional, and are designed to detect and prevent money laundering, terrorist financing, and related risks.

General Principles of Customer Acceptance and Prohibited Relationships

The Company approaches each prospective business relationship with caution, professionalism, and a firm commitment to legal and reputational integrity. In line with the

VQF SRO Regulations, a business relationship will only be established if the Company can verify the customer's identity, assess the origin of their funds and wealth, and conclude that the relationship presents no unacceptable legal or reputational risk. This also includes a forward-looking assessment of potential misuse for criminal, fraudulent, or deceptive purposes.

As part of its commitment to proper business conduct, the Company will not enter into a business relationship if any doubts remain after clarifications are completed, or if the origin of assets or the customer's intentions cannot be established beyond reasonable doubt. These standards reflect the Company's internal Customer Acceptance Principles and Articles 8 and 9 of the VQF SRO Regulations.

Prohibited Assets and Transactions

The Company will not accept any assets where there is reason to believe — or even to assume — that such assets originate from criminal conduct, including:

- Crimes as defined under Swiss law,
- Qualified tax offences, even if committed abroad,
- Acts of financing terrorism, or
- Transactions lacking economic justification or clarity regarding the source of funds.

The negligent acceptance of such assets may compromise the Company's ability to uphold proper business conduct and will be treated as a serious compliance breach.

Prohibited Business Relationships

The Company will not establish or continue business relationships under any of the following conditions:

- Where there is credible reason to believe the customer is engaged in, financing, or otherwise associated with terrorism, criminal organisations, or their support networks;
- Where the customer is a fictitious bank, defined as a bank without a physical presence in its place of incorporation, unless it belongs to a supervised and consolidated financial group;
- Where the assets or the business activities are linked to sanctioned individuals or entities as per the Swiss State Secretariat for Economic Affairs (SECO);
- Where the customer has refused or failed to provide information required for due diligence and profile creation without valid justification;
- Where the customer demands anonymous or numbered accounts;
- Where the customer operates through shell banks or similar opaque structures;

Prohibited Customer Types and Jurisdictions

The Company will not accept business from individuals or entities who fall into one or more of the following categories:

- Minors under the age of 18;
- Companies with bearer shares;

- Customers acting on behalf of undisclosed third parties;
- Customers who fail to disclose or clarify beneficial ownership;
- Potential customers requiring accounts from restricted jurisdictions, including but not limited to:
    - Afghanistan, Algeria, Bangladesh, Bolivia, Cambodia, Central African Republic, Cuba, Democratic Republic of Congo, DPRK, Egypt, Ghana, Iran, Iraq, Lebanon, Libya, Mali, Morocco, Myanmar, Nepal, Pakistan, Palestine, Saudi Arabia, Somalia, South Sudan, Sudan, Syria, Venezuela, Yemen, Zimbabwe, and the United States of America;
    - Any other countries blacklisted by the FATF or designated as restricted under the Company's internal risk appetite.

This list is regularly reviewed and updated based on emerging typologies, geopolitical changes, or updated FATF recommendations.

Prohibited Sectors and Business Models

In accordance with its internal policy and reputational risk assessment, the Company does not accept customers whose principal activity falls within the following categories:

- Investment and Credit Services: including unlicensed securities brokers, speculative real estate schemes, and unregulated investment clubs;
- Unregulated or high-risk financial services: such as check cashing outlets, bail bonds, or debt collection agencies;
- Intellectual Property Infringement: including distribution of counterfeit software, music, or other digital goods;
- Counterfeit or Grey Market Goods: including the resale of luxury goods without authorisation, or sale of stolen or fraudulently obtained goods;
- Products with Regulatory Restrictions: including firearms, ammunition, explosives, radioactive materials, or unlicensed pharmaceutical distribution;
- Illegal Drugs and Paraphernalia: including synthetic substances, precursors, or related paraphernalia;
- Adult Entertainment and Services;
- Multi-level Marketing (MLM) and Pyramid Schemes;
- Pseudo-pharmaceuticals and Unverified Health Claims;
- High-risk speculative platforms: such as HYIP (high-yield investment programs), unregulated forex, or algorithmic trading platforms not subject to regulatory oversight;
- Any business model considered predatory, deceptive, or damaging to consumers or financial stability.

Where the nature of a prospective customer's business cannot be immediately categorised, or where ambiguity exists regarding legal permissibility, the Compliance Officer will escalate the case to the Compliance Committee for review. The Compliance Committee reserves the right to reject any application based on risk appetite or alignment with internal ethical standards.

Identification of the Contracting Party

Prior to accepting any customer, the Company conducts a complete identification of the contracting party. This applies to both natural persons and legal entities.

For natural persons, the following information is collected:

- Full legal name
- Date of birth
- Nationality
- Residential address

Verification is conducted using a valid government-issued identification document that includes a photograph and is difficult to falsify (e.g. passport, national identity card). The document is either inspected in person or verified through a secure compliant electronic method. Where remote identification is used, it follows the requirements of FINMA Circular 2016/7

For remote onboarding, the Company works with certified identification partners such as Ondato and Sumsub, which perform real-time document checks, biometric verification, and live presence detection.

In some cases, identification may be performed using a qualified electronic signature through a ZertES-compliant certification provider, strictly for the purpose of signing contractual documents — not as a standalone identity verification method.

For legal entities, the Company verifies the following:

- Legal name and registered form
- Domicile and registered address
- Commercial register number or equivalent identification
- Country of incorporation and business activity

Verification is supported by official registry extracts, articles of incorporation, or equivalent legal documents. Additionally, the person acting on behalf of the legal entity (e.g. a director or authorised signatory) is identified and verified individually, using the same procedures applied to natural persons. Power of attorney or board resolutions are examined and retained in the customer file.

Where an individual or entity has previously been identified by the Company and is involved in a subsequent relationship, the identification does not need to be repeated if the earlier documents are referenced and remain valid, in line with Article 15(3) of the VQF Regulations.

Establishing the Identity of the Beneficial Owner and Controlling Person

The Company establishes the identity of the beneficial owner and, if applicable, the controlling person behind the assets or the legal structure, in accordance with Articles 31 to 51 of the VQF Regulations.

A beneficial owner is defined as the natural person who ultimately owns or controls the contracting party or the assets involved. The customer is required to complete a written declaration disclosing the beneficial ownership, supported where necessary by ownership charts, shareholder registries, trust deeds, or other legal/corporate documents.

Where the customer is a legal entity, the Company identifies:

- Any natural person holding, directly or indirectly, 25% or more of the capital or voting rights
- Any person otherwise exercising control over the management or decision-making of the entity
- In the absence of identifiable ownership or control, the most senior managing officer (fallback rule)

The identity of each beneficial owner is verified using the same standards and procedures as for the contracting party. Supporting documents are collected and reviewed for plausibility. Where the structure involves offshore vehicles, nominee arrangements, or entities from jurisdictions lacking transparency, the Company undertakes enhanced verification and clarifications to establish the true ownership.

To verify beneficial owners, the Company:

- Collects identification documents (passport, ID, address proof)
- Reviews ownership structures, share registers, trust deeds, or control charts
- Screens for sanctions, adverse media, and PEP status

Each beneficial owner and controlling person is recorded using:

- VQF Form 902.9 (Beneficial Owner Declaration – A Form)
- VQF Form 902.11 (Controlling Person Declaration – K Form), where applicable

Additional forms are used where the structure involves:

- Foundations or similar constructs: VQF Form 902.12 (S Form)
- Trusts: VQF Form 902.13 (T Form)

All information is reviewed for plausibility and updated upon any change in the ownership or control structure.

Customer Risk Categorisation and Profile Creation

The Company employs a structured and risk-based approach to customer categorisation and monitoring, in accordance with Articles 52 to 54 of the VQF SRO Regulations. As part of this approach, the Company introduces a risk scoring model designed to assess each customer’s potential exposure to money laundering, terrorist financing, and reputational risk.

At the time of onboarding, each customer is assigned a risk score, based on weighted criteria that take into account both inherent risk indicators and mitigating controls. This risk score determines the customer's risk category, which guides the level of scrutiny applied both during onboarding and throughout the business relationship.

The Company applies a two-tier risk classification model, in line with VQF expectations:

- Regular customers are those for whom no material Increased risk factors are identified during the scoring process. These customers demonstrate transparent structures, operate in low-risk jurisdictions, and engage in straightforward, documented activities.
- Increased risk customers are those for whom one or more Increased risk indicators are present. These may include exposure to high-risk jurisdictions, complex or opaque legal structures, politically exposed persons (PEPs), unregulated industries, or high transaction volumes inconsistent with the customer's profile.

The risk scoring process incorporates objective criteria such as:

- Country of origin and residence
- Legal entity structure and complexity
- Customer type and business sector
- Source of wealth and origin of funds
- Anticipated transaction activity and channels used
- PEP status, sanctions exposure, or negative media

Each of these factors is assigned a risk weighting, and the total risk score is calculated to determine the customer's classification. The scoring model is periodically reviewed and adjusted by the Compliance Department to reflect evolving typologies, regulatory updates, and internal experience.

In parallel with risk scoring, a detailed customer profile is created. This includes:

- The purpose and intended nature of the relationship
- A documented source of wealth and expected origin of incoming funds
- Expected account turnover, frequency, and type of transactions
- Customer's professional, business, or operational background
- Countries or markets in which the customer operates or transacts

The customer profile is established using information gathered through structured onboarding questionnaires and supporting documents. The Company documents these assessments using:

- VQF Form 902.4 (Risk Profile), which captures the risk scoring outcome and rationale
- VQF Form 902.5 (Customer Profile), which documents the customer's general background and relationship rationale

The final profile and assigned risk score are reviewed by the Compliance office prior to activation of the business relationship. Customers classified as "increased risk" require enhanced due diligence, more frequent monitoring, and periodic profile reassessment as stipulated under Articles 58 to 61 of the VQF Regulations.

This categorisation and scoring framework provides the basis for tailored transaction monitoring, risk alerts, periodic reviews, and ongoing compliance oversight throughout the lifecycle of the customer relationship.

Ongoing Monitoring and Special Clarifications

Following onboarding, the Company continuously monitors all business relationships to ensure that activity remains consistent with the customer's profile and risk classification.

Monitoring focuses on identifying activity that deviates from the expected behaviour recorded in the customer profile. Indicators that may trigger closer review include:

- Transactions exceeding expected volume or frequency
- Transfers involving high-risk or sanctioned jurisdictions
- Transactions with unclear economic purpose

Where unusual or potentially suspicious activity is detected, the Company initiates a special clarification process, during which:

- Additional information is requested from the customer (e.g., invoices, contracts)
- Background checks are updated (e.g., sanctions, PEP screening)
- An internal plausibility assessment is conducted

For increased risk customers, clarifications are triggered more readily and must be documented in greater detail. The Compliance Officer reviews each case and decides on the appropriate course of action, which may include updating the customer profile, reclassifying risk level, or initiating a formal report. The results are documented using VQF Form 902.14 (Special Clarifications Form) and evaluated by the AMLA Officer and, where needed, the Compliance Committee.

Suspicious Activity Reporting and Freezing of Assets

If the Company, after completing its internal clarifications, identifies grounds to suspect that a transaction or business relationship is connected to money laundering, terrorist financing, or other criminal conduct, a suspicion report is submitted to MROS (Money Laundering Reporting Office Switzerland) without delay.

Concurrently, the Company freezes all assets involved, in accordance with Articles 66 to 70 of the VQF Regulations. The affected customer is not informed of the report or freeze, in strict adherence to the ban on information (Article 71). The case is documented comprehensively in the AMLA file and escalated to the Compliance Committee where appropriate.

Rejection and Termination of Business Relationships

The Company reserves the right to refuse to enter into or terminate any business relationship that presents an unmanageable risk or that fails to meet the standards of due diligence and transparency set forth in this Directive. Reasons for refuse or termination may include:

- Refusal or failure to complete identification or provide necessary documents
- Attempted use of fictitious names or anonymous services
- Refusal to provide requested documents or clarifications
- Inability to clarify beneficial ownership or source of funds
- Association with prohibited sectors, jurisdictions, or sanctioned persons
- Activity inconsistent with the declared purpose of the account

- Reputational or legal risks identified
- Detection of links to criminal activity, sanctioned entities, or blacklisted jurisdictions
- Excessive complexity or opacity of the ownership structure
- Negative results from background checks or media screening
-

In such cases, the AMLA Officer may suspend account activity and refer the matter to the Compliance Committee, which may decide to close the account and report the termination in accordance with regulatory requirements. All rejections and terminations are documented, and, where necessary, reported to MROS and VQF.

Documentation and Retention of Records

The Company maintains full documentation of all due diligence activities, including identification, verification, beneficial ownership declarations, customer profiles, clarifications, and any correspondence or decisions. This documentation is retained for a minimum of ten years after the end of the business relationship or the execution of a transaction.

The AMLA file for each customer is maintained in an electronic document management system that guarantees integrity, traceability, and secure access. The system complies with the standards for digital storage outlined in Articles 62 to 65 of the VQF Regulations. Upon request, the Company can provide timely and complete access to supervisory authorities, auditors, or law enforcement bodies. The Company also maintains an up-to-date file list in accordance with VQF Form 902.8 (List of Files Relevant to the AMLA – Excel or Word format)

4. IDENTIFICATION, LIMITATION AND MONITORING OF INCREASED RISKS

Identification of Increased Risk Relationships and Transactions

The process of identifying increased risk business relationships is integrated into the Company's broader customer risk scoring model and onboarding framework, as outlined in Chapter 3. During the establishment of a new business relationship, each customer is assessed using a structured set of risk indicators and assigned a risk score accordingly. If this score reaches the designated threshold for increased risk, the relationship is flagged, documented, and reviewed before any services may be activated.

Increased risk may be identified based on several relevant factors. These include, but are not limited to:

- the domicile of the customer or beneficial owner in a jurisdiction identified by the FATF as high-risk or non-cooperative;
- the customer's involvement in a business sector associated with high AML exposure;
- the presence of politically exposed persons (PEPs) in the ownership or control structure;

- unusually complex or opaque legal arrangements such as trusts or foundations;
- circumstances in which the source of funds or wealth cannot be reliably explained or verified.

Where any of these indicators apply, or where a deviation from standard due diligence procedures is warranted, the relationship is marked as increased risk and recorded in the customer's AMLA file using the VQF Risk Profile Form (902.4). This form is used to capture both the objective basis for the classification and any internal justification or supporting documentation collected during onboarding.

The AMLA Officer is responsible for assigning and confirming the increased risk classification based on all available information. If the AMLA Officer concludes that the relationship can be accepted with appropriate safeguards, they will document the rationale and proceed. Where the case involves heightened concerns or unclear risk mitigation, it is escalated to the Compliance Committee for second-level review and decision-making.

Enhanced Due Diligence and Limitation of Risk Exposure

Once a business relationship has been classified as increased risk, the Company applies enhanced due diligence (EDD) measures in order to establish a greater level of transparency and control. The EDD process is commensurate with the nature and severity of the identified risk and follows the requirements set forth in Articles 59 and 60 of the VQF Regulations.

The AMLA Officer ensures that the customer's source of wealth and origin of funds are reviewed in greater detail and supported by documentary evidence such as tax returns, audited financials, or contractual agreements. Where the business model, income stream, or assets appear inconsistent with the declared profile, further clarification is obtained before the relationship proceeds.

Additional verification steps may include more rigorous background screening, periodic document updates, and enhanced plausibility checks. The decision to accept an increased risk customer must be based on a clear and justified risk-benefit evaluation, and documented comprehensively in the AMLA file.

No increased risk relationship is accepted without approval from the Compliance Committee, which has the final authority to approve or reject the relationship.

Monitoring of Increased Risk Relationships

Increased risk relationships are monitored on a continuous and more intensive basis than standard customer relationships. This reflects the duty under Article 55 of the VQF SRO Regulations to maintain up-to-date knowledge of the customer and to detect any divergence from the declared profile or expected behaviour.

The monitoring process involves regular review of transaction patterns, ongoing screening against sanctions and watchlists, and review of any external signals that might affect the customer's risk classification, such as adverse media or regulatory alerts. These reviews are documented and performed at least annually, or more frequently if changes in the customer's structure or behavior warrant earlier intervention.

All alerts generated through monitoring systems — whether due to abnormal transaction patterns, newly identified PEP status, or changes in the ownership structure — are reviewed by the AMLA Officer. Where needed, the Officer initiates a special clarification procedure in line with Articles 56 and 57, collecting additional information or requesting clarification from the customer. The outcome of such clarifications is formally recorded, and the customer's profile is updated accordingly.

Where the result of ongoing monitoring leads to a reassessment of risk — whether an escalation or de-escalation — the AMLA Officer updates the VQF Risk Profile Form (902.4) and ensures that all documentation remains current and internally consistent.

Identification and Handling of Increased Risk Transactions

Increased risk is not only applicable to customer relationships but also to specific transactions. In accordance with Article 59 of the VQF Regulations, the Company defines and monitors indicators of unusual or suspicious transactions that may require further investigation, even if the customer is not categorised as increased risk.

The Company applies an internal threshold-based mechanism adapted to its role as a crypto ramp and off-ramp provider. Specifically, a transaction is flagged for review if a customer initiates a fiat-to-crypto or crypto-to-fiat exchange that exceeds the customer's declared monthly turnover by more than 50% within a 7-day period, unless a justified and documented update to the customer profile has been recorded.

This internal control is designed to capture situations in which a customer’s behavior suddenly and significantly deviates from their previously declared activity level. Such deviations may indicate attempts at structuring, third-party use of the account, or use of the account for criminal purposes.

Flagged transactions are reviewed by the AMLA Officer and, if necessary, subjected to clarification or escalation. Where a transaction is found to lack plausible economic justification, the Company may proceed with a suspicious activity report (SAR) to MROS and apply additional restrictions or terminations as necessary.

Documentation and Escalation Procedures

Every stage of the increased risk process — from identification to final decision-making — is fully documented within the AMLA file. The VQF Risk Profile Form (902.4) serves as the central record of classification, rationale, and review history. Any clarifications, approvals, and updated screenings are appended to this form or referenced within the Company’s secure compliance system.

The AMLA Officer is responsible for ensuring that all documentation remains current, traceable, and compliant with audit requirements. Where escalation to the Compliance Committee occurs, the case file must include all supporting documentation, a formal risk statement, and a recommendation based on the AMLA Officer’s assessment.

The Compliance Committee, in turn, reviews the case in light of applicable laws, the Company’s internal policy, and its risk appetite. Decisions of the Committee are recorded in meeting minutes and added to the customer’s AMLA file.

Where no acceptable mitigation is possible, the Company retains the right to reject or terminate the relationship in accordance with its risk tolerance, and may report the situation to the relevant authorities as necessary.

The Company will identify and document increased risk business relationships and transactions in compliance with Articles 55–61 of the SRO Regulations. Increased risks may arise due to customer characteristics, geographic origin, transaction types, or business sectors.

The Company will implement a formal risk assessment framework using either the VQF standard risk profile form (Document No. 902.4) or an equivalent internal form that Customer acceptance principalstures:

- Customer nationality and domicile
- Business activity and sector
- Source of funds and wealth
- Politically exposed person (PEP) status
- Geographic exposure (e.g. high-risk countries)
- Nature and volume of expected transactions

Risk scoring for classification will be conducted during onboarding and reassessed periodically, to identify Increased risk Customers and business activities. The AMLA Officer is responsible for establishing the risk scoring and ensuring it reflects all available information.

5. INCREASED RISK BUSINESS RELATIONSHIPS

In accordance with the VQF SRO Regulations, any member institution maintaining more than twenty permanent business relationships is required to define its own internal criteria for identifying relationships that present increased risk of money laundering or terrorist financing. These criteria may either be set out uniformly in the institution’s internal directives or applied individually to each business relationship through a structured risk profile, such as the VQF standard form 902.4 or an equivalent internal tool.

The Company meets this requirement by combining clearly articulated internal thresholds with the documented use of the VQF risk profile form. This dual approach allows for both standardised consistency and customer-specific assessment. The criteria defined by the Company reflect the specific risk exposure associated with its operational focus and client base, and are applied consistently during onboarding and throughout the course of each business relationship.

Internal Criteria and Thresholds for Increased Risk

The Company recognises that increased risk can arise from a variety of customer characteristics, transactional behaviors, or structural factors. As such, increased risk is not treated as a static label but rather as a designation informed by facts, patterns, and continuous assessment.

While the ultimate risk scoring of each customer is documented individually using the VQF risk profile form (Doc. No. 902.4), the Company has established core internal criteria that signal increased exposure. These include the presence of a politically exposed person (PEP) as either a customer or beneficial owner; the involvement of jurisdictions identified by the FATF as high-risk or non-cooperative; business activity in sectors associated with high cash turnover or criminal exploitation; or the use of legal structures such as trusts, foundations, or domiciliary companies designed to obscure ownership or control.

A business relationship may also be classified as increased risk where the declared source of wealth cannot be reliably verified, or when the expected volume or frequency of transactions significantly exceeds the standard benchmarks for the customer's type or profile. These indicators do not operate in isolation but are assessed collectively in the context of the full customer profile and any mitigating information provided.

All such criteria are applied and evaluated by the AMLA Officer, who holds primary responsibility for assigning the increased risk classification and updating the risk profile throughout the lifecycle of the relationship.

Application of the Risk Profile and Assessment Process

The Company applies the increased risk identification criteria during the customer onboarding phase using the VQF Risk Profile Form (902.4). This form captures the customer's exposure to geographic, structural, transactional, and reputational risk based on documented responses, source verification, and screening outputs.

The form allows the AMLA Officer to record not only the presence of individual risk factors, but also the overall rationale for the assigned risk level. Where the risk score meets or exceeds the defined threshold for increased risk, the classification is recorded and the appropriate controls are initiated. Throughout the relationship, any material change in the customer's circumstances — including changes to ownership, business activity, or jurisdictions of operation — will trigger a reassessment of the risk profile and an update to the form.

This structured approach ensures that increased risk is neither assumed lightly nor overlooked. It is grounded in verifiable data, responsive to change, and aligned with the Company's obligation to prevent abuse of its services for illicit purposes.

Approval and Ongoing Control Mechanisms

No business relationship that has been classified as increased risk may be accepted without formal approval by the AMLA Officer. Where residual risks remain or the profile requires further evaluation, the case is escalated to the Compliance Committee for final review. This two-tier approval mechanism ensures both operational scrutiny and strategic oversight, and guarantees that all risk-based decisions are made in a manner consistent with the Company's governance and legal obligations.

Once an increased risk relationship is approved, it becomes subject to enhanced due diligence and intensified monitoring, as outlined in the previous chapter. The customer's documentation and risk profile are reviewed at least annually, and more frequently when risk triggers or red flags appear. The AMLA Officer is responsible for ensuring that all enhanced measures remain active and effective throughout the duration of the relationship.

Every approval decision, supporting justification, and monitoring outcome is fully documented in the AMLA file, forming part of the audit trail required by the VQF and FINMA. Where an increased risk relationship no longer meets the Company's standards, or if further clarifications fail to mitigate open concerns, the Compliance Committee may decide to terminate the relationship and, where appropriate, notify the authorities in accordance with AMLA.

In accordance with the VQF SRO Regulations, the Company, having more than 20 permanent business relationships, will define and apply its own criteria for identifying increased risk business relationships.

These criteria may be applied uniformly across the organization and described directly in this Directive, or determined on a case-by-case basis by means of a documented risk profile. The Company uses the VQF standard risk profile form (Doc. No. 902.4) or an internal equivalent to assess the Customer's risk level.

6. BUSINESS POLICY REGARDING POLITICALLY EXPOSED PERSONS (PEPs)

The Company recognises the Increased risk presented by business relationships involving politically exposed persons (PEPs) and implements strict procedures to identify, assess, approve, and monitor such relationships in accordance with Article 58 of the VQF SRO Regulations. These procedures ensure that potential abuse of the financial system by individuals in positions of public trust is proactively identified and mitigated.

In line with regulatory requirements, the Company treats all business relationships with foreign PEPs as increased risk by default. Relationships with domestic PEPs or PEPs of international organisations are also treated as increased risk when other relevant risk factors are present, such as exposure to high-risk jurisdictions, involvement in complex structures, or lack of transparency regarding source of wealth.

Classification and Risk Assessment

Every customer relationship is screened for PEP status during the onboarding process and on a continuous basis thereafter. The Company uses reputable compliance databases and watchlist providers to identify PEPs, their close associates, and family members.

Where a customer is identified as a PEP, the classification is recorded in the customer's VQF Risk Profile (Form 902.4) and reflected throughout the AMLA file. The assessment includes

not only confirmation of PEP status but also an evaluation of related risk indicators such as jurisdiction, political function, ownership structure, and transactional behavior.

Foreign PEPs are always classified as increased risk. Domestic PEPs or individuals affiliated with international organisations are classified as increased risk if one or more additional risk criteria are met. The determination is made by the AMLA Officer, who is also responsible for ensuring that the classification is accurately documented and kept up to date in the event of changes in the individual's political role or risk profile.

Internal Policy on Acceptance of PEPs

The Company does not maintain a blanket ban on onboarding politically exposed persons. Instead, it has adopted a controlled acceptance policy, under which PEPs may be accepted only following enhanced review and multi-level internal approval.

All PEP relationships are subject to enhanced due diligence, including verification of the source of wealth, assessment of political exposure, and background screening of associated individuals or entities. If the results of these checks support a possible onboarding, the AMLA Officer prepares a detailed acceptance recommendation.

The decision to accept a PEP customer must be approved by the Compliance Committee. This committee, composed of the AMLA Officer and the Board of Directors, reviews the full file and determines whether the risk level is compatible with the Company's internal standards and regulatory obligations.

If the risk exposure is unusually high — for example, involving senior political office, ongoing media controversy, or cross-border corruption concerns — the Company may decide not to accept the relationship, even if the technical documentation is in order. In such cases, the rationale for rejection is recorded and preserved in the AMLA file.

Where approval is granted, the relationship enters an increased risk category and is subject to the controls set out in this chapter.

Documentation and Monitoring of PEP Relationships

PEP relationships, once approved, are placed under continuous monitoring, with controls that go beyond those applied to standard increased risk customers. These controls are designed to ensure both the legitimacy of the relationship and the Company's readiness to detect and respond to any changes in political status, public exposure, or transactional behavior.

Each PEP file must include:

- A written justification for the decision to accept the relationship, including references to the source of wealth, risk classification, and control measures
- Verification and plausibility checks confirming the legitimacy of the declared assets and income
- Screening results against sanctions lists, PEP watchlists, and adverse media databases, covering the individual, their close associates, and relevant family members

A clear entry in the Company's register of increased risk customers, with a PEP flag

The customer's risk profile is reassessed at least once per year. If a PEP's circumstances change materially — for example, resignation from political office, involvement in legal proceedings, or emergence of new risk indicators — the AMLA Officer immediately initiates a new review, and if needed, an escalation to the Compliance Committee.

Training, Detection, and Escalation

All employees involved in onboarding or managing customer relationships are trained to understand what constitutes a PEP, how to detect potential PEP indicators, and when to escalate concerns. This training includes real-world scenarios and is refreshed regularly as part of the Company's AML and compliance training program.

If a customer is later discovered to be a PEP after the business relationship has already been established, the AMLA Officer will immediately reclassify the relationship as increased risk and initiate the required enhanced due diligence and approval process. If the PEP status was not disclosed at onboarding, the Company may take disciplinary or remedial measures, depending on the nature of the omission and the individual's responsibility.

This escalation process ensures that the Company remains compliant not only with the VQF SRO Regulations but also with its internal expectations for transparency, integrity, and prudence in managing politically sensitive customers.

7. INCREASED RISK TRANSACTIONS

Principles and Criteria for Identification

The Company maintains clear internal regulations for identifying transactions that present increased risk. In accordance with Article 59 of the VQF SRO Regulations, at least one transaction-related risk indicator is assigned to every business relationship, and further indicators may be defined in the Risk Profile (VQF Form 902.4).

The identification of such transactions is an essential part of our risk-based approach and ensures that deviations from expected behavior are recognized early. In practice, increased risk transactions are those which, by their nature or context, differ significantly from what is plausible or previously declared by the customer. To this end, the following aspects are considered:

The amount of incoming or outgoing assets in relation to the customer's expected activity

The type, frequency, or structure of transactions, particularly where they differ from declared use or from similar customer profiles

Unusual counterparties, jurisdictions, or instruments that were not anticipated during onboarding

Any payment involving high-risk or non-cooperative countries as listed by the FATF

These criteria may apply across customer segments or be defined case-by-case within the customer's documented profile. Where thresholds are introduced (e.g., volume or frequency

limits), these are tailored based on the customer's risk classification, financial background, and intended business purpose.

Transactions are flagged for increased risk both through real-time detection (automated rules) and periodic assessments by the AMLA Officer and Compliance Team.

Monitoring and Internal Escalation Process

All transactions are monitored continuously through a hybrid framework of automated monitoring tools and manual control mechanisms. The Company employs external providers—such as Sumsub, Crystal Blockchain, or equivalent vendors—to support monitoring through:

- Automated detection of anomalies
- Pattern recognition and typology-based alerting
- Jurisdictional and counterparty screening

When a transaction triggers an alert—whether for exceeding a defined limit or deviating from the expected pattern—the AMLA Officer undertakes a formal review. This includes consulting the customer's risk profile, transaction history, and previously provided documentation.

If the transaction cannot be plausibly justified, the customer is contacted for clarification. Depending on the nature of the deviation, the Company may request documentary proof such as invoices, contracts, or bank statements.

Should concerns persist or if red flags are confirmed, the case is escalated to the Compliance Committee, which evaluates whether continued relationship or reporting to MROS is warranted. All decisions, communications, and conclusions are documented in the customer's AML file.

Adaptation and Continuous Review

The transaction monitoring thresholds, rules, and typologies are not static. They are regularly reviewed by the Compliance Department in collaboration with the AMLA Officer, based on:

- Internal audits and findings from actual case reviews
- Typologies or warnings issued by FINMA, FATF, or law enforcement
- Reassessments of individual customer profiles due to business or geographic changes

The aim of these reviews is to maintain a monitoring system that remains effective and proportionate as criminal behavior and regulatory expectations evolve.

Linkage to Overall Monitoring Framework

This chapter on increased risk transactions integrates fully with the broader transaction monitoring regime described in Chapter 8, where both proactive detection and reactive investigation mechanisms are detailed.

Through the combined use of VQF forms, digital tools, staff training, and documented escalation paths, the Company ensures that increased risk transactions are not only detected

and reviewed but formally recorded, reassessed, and responded to in line with VQF requirements.

In accordance with Article 58 paragraph 3 and Article 59 paragraph 2 of the SRO Regulations, the Company will identify and assess increased risk transactions for each business relationship. In addition to the mandatory risk indicators, the Company has defined a set of internal criteria for determining whether a transaction deviates significantly from the expected behavior and therefore qualifies as increased risk.

These criteria may be defined generically within this Directive or assigned on a case-by-case basis using the VQF standard risk profile (Doc. No. 902.4) or an equivalent internal form.

The Company applies at least one of the following transaction-based criteria to each business relationship:

- The amount of individual incoming or outgoing transactions;
- The type, amount, or frequency of transactions compared to the customer's stated activity and profile;
- The type, amount, or frequency of transactions compared to typical patterns for similar business relationships;
- Deviation from any transaction behavior previously declared or expected by the customer;
- Where thresholds are used (e.g., transaction limits), these are defined proportionally to the Customer's risk profile, source of wealth, and expected transaction volume.

8. Principles of transaction monitoring

The Company maintains a robust and risk-sensitive transaction monitoring framework that enables it to detect unusual or suspicious activities across all business relationships. This framework is built in accordance with Article 55 of the VQF SRO Regulations, which requires financial intermediaries to ensure that all transactions are reviewed for consistency with the customer's profile, risk classification, and declared purpose of the relationship.

The aim of transaction monitoring is to identify behaviors or transaction patterns that deviate from what is reasonably expected, and to respond to such deviations with appropriate internal controls, clarifications, or escalation. The monitoring process applies equally to fiat and crypto transactions and is designed to function both in real time and retrospectively.

Monitoring and Internal Escalation Process

The Company applies a hybrid monitoring model that combines automated surveillance systems with manual review procedures to ensure continuous oversight of all financial activity conducted through its platform. Transaction data is analyzed in real time by third-party monitoring tools such as Sumsub, Crystal Blockchain, or other compliant providers. These tools are configured to detect indicators such as:

- Transactions exceeding predefined thresholds
- Patterns inconsistent with the customer's risk classification or transaction history
- Transfers involving high-risk jurisdictions, counterparties, or instruments

- Structuring behaviors, rapid movement of funds, or unknown sources

When a transaction triggers an alert, the system flags it for investigation. The alert is automatically routed to the AMLA Officer, who conducts a first-level assessment. This includes reviewing the customer's current risk profile, the specific transaction in question, and any related history. The AMLA Officer may also consult supporting documentation previously submitted by the customer.

If the transaction appears to lack economic or legal plausibility, or raises new concerns not covered in the original risk assessment, the customer is contacted and asked to provide clarification or documentation. This may include invoices, contracts, explanations of business purpose, or proof of source of funds.

If the clarification provided is incomplete, unsatisfactory, or introduces new red flags, the case is formally escalated to the Compliance Committee. This committee reviews the full case file and determines whether the transaction should be reported to the Money Laundering Reporting Office Switzerland (MROS), whether the relationship should be restricted or terminated, or whether monitoring should be increased. All findings, interactions, and final decisions are recorded in the customer's AMLA file for audit and supervisory purposes.

System Review and Continuous Improvement

The transaction monitoring system is subject to ongoing evaluation to ensure that it remains effective, relevant, and proportionate to the Company's evolving risk landscape. In accordance with Article 61 of the VQF SRO Regulations, the Company regularly reassesses both individual customer risk profiles and the overall configuration of its monitoring framework.

The Compliance Department, in coordination with the AMLA Officer, reviews and updates the monitoring rules, thresholds, and alert-handling procedures based on:

- New typologies or regulatory notices issued by FINMA, FATF, or law enforcement authorities
- Internal case reviews or lessons learned from suspicious activity reports (SARs)
- Changes in the services offered, the types of customers served, or the jurisdictions involved
- Findings from internal audits or external supervisory inspections

System updates are tested, documented, and logged to ensure transparency. When thresholds are updated or new risk factors introduced into the monitoring logic, these changes are recorded and integrated into staff training and procedural documentation.

All monitoring system configurations, rule changes, and reviews are retained in accordance with the Company's document retention obligations, and are made available for regulatory review upon request.

The Company maintains clear internal regulations for identifying transactions that present increased risk. In accordance with Article 59 of the VQF SRO Regulations, at least one transaction-related risk indicator is assigned to every business relationship, and further indicators may be defined in the Risk Profile (VQF Form 902.4).

The identification of such transactions is an essential part of our risk-based approach and ensures that deviations from expected behavior are recognized early. In practice, increased risk transactions are those which, by their nature or context, differ significantly from what is plausible or previously declared by the customer. To this end, the following aspects are considered:

The amount of incoming or outgoing assets in relation to the customer's expected activity

The type, frequency, or structure of transactions, particularly where they differ from declared use or from similar customer profiles

Unusual counterparties, jurisdictions, or instruments that were not anticipated during onboarding

Any payment involving high-risk or non-cooperative countries as listed by the FATF

These criteria may apply across customer segments or be defined case-by-case within the customer's documented profile. Where thresholds are introduced (e.g., volume or frequency limits), these are tailored based on the customer's risk classification, financial background, and intended business purpose.

Transactions are flagged for increased risk both through real-time detection (automated rules) and periodic assessments by the AMLA Officer and Compliance Team.

9. BASIC AND ADVANCED TRAINING OF THE PERSONS WORKING IN THE AMLA SECTOR

The Company recognises that the competence and awareness of its personnel are fundamental to ensuring an effective and legally compliant anti-money laundering framework. In accordance with Article 84 of the VQF SRO Regulations, and in line with the VQF Training Concept (Doc. No. 610.1), the Company has implemented a structured training regime for all individuals whose duties are relevant to the application of the Anti-Money Laundering Act (AMLA).

This training framework applies to all staff whose activities directly or indirectly involve customer onboarding, monitoring, due diligence, transaction analysis, or escalation. It includes members of the Board of Directors, the AMLA Officer, the Compliance Committee, central file administrators, account managers, and external service providers who are engaged in AML-related activities on behalf of the Company.

Training is not treated as a one-time formality but as an ongoing professional obligation that evolves alongside regulatory expectations and the Company's own risk landscape.

Initial Training and Familiarisation

Every individual assuming responsibilities within the AMLA framework is required to complete an initial training program before undertaking any operational tasks. This training ensures that each staff member understands the legal and regulatory obligations applicable to their role, and is able to identify and respond appropriately to potential signs of money laundering or terrorist financing.

The content of this training includes a comprehensive overview of the AMLA and VQF SRO obligations, an introduction to the Company's internal procedures for customer identification and acceptance, and an explanation of the risk-based approach applied to customer due diligence. Particular emphasis is placed on recognising transaction anomalies, understanding the escalation process, and correctly applying controls for increased risk customers and politically exposed persons.

This initial training may be delivered in person or via internal digital platforms, and is overseen and documented by the AMLA Officer.

Ongoing and Refresher Training

To ensure that all relevant individuals remain current with evolving legal and operational standards, the Company provides periodic refresher training. This training is conducted at least once per calendar year and is mandatory for all personnel with AMLA duties.

Refresher sessions are tailored to address current developments, including regulatory changes issued by FINMA or VQF, internal updates to procedures or systems, and emerging financial crime typologies or case patterns. These sessions also reinforce key principles of due diligence, transaction monitoring, and risk escalation, ensuring that staff remain attentive and competent in the execution of their duties.

Training is adapted to the functional level of the participants. For example, account managers receive scenario-based training on identifying abnormal customer behavior or inconsistencies in source of funds, while compliance and monitoring staff receive more detailed updates on procedural and legal obligations.

Advanced Training for AMLA Officer and Key Compliance Roles

The AMLA Officer and other employees entrusted with elevated compliance functions are required to complete more comprehensive and specialised training programs. This includes in-depth modules on enhanced due diligence, the management of PEP relationships, cross-border risk assessment, and the proper handling of suspicious transaction escalations.

Advanced training is acquired through participation in VQF-approved seminars, external certification programs, and relevant workshops or webinars. The Company encourages such personnel to remain engaged with sector-specific learning opportunities, and maintains a record of certifications and course completions as part of its internal competence documentation.

This ensures that the individuals at the core of the Company’s AML framework possess the necessary depth of knowledge and judgement to lead, advise, and make determinations in complex or sensitive cases.

Documentation and Oversight

All training activities—whether initial, refresher, or advanced—are recorded and retained in a central training register maintained by the AMLA Officer. This register includes the date and content of the training, the method of delivery, and the names and roles of the participants.

The AMLA Officer is responsible for ensuring that training records are accurate, complete, and readily available for audit by VQF or any supervisory authority.

The Company's training policy is reviewed annually to ensure it remains aligned with statutory obligations, internal requirements, and the dynamic nature of financial crime risks. This review includes evaluation of training effectiveness, as measured by internal audit feedback, post-training assessments, and observed performance in the handling of AML matters.

By embedding a culture of continuous learning and professional discipline, the Company ensures that all individuals engaged in AMLA responsibilities are well-equipped to contribute to the integrity of the financial system and to uphold the trust placed in the Company by regulators, clients, and counterparties.

The Company ensures that all individuals whose roles involve AMLA-relevant duties—including members of the Board of Directors, Compliance Officers, Central File staff, Account Managers, and any third-party service providers involved in onboarding or monitoring—receive appropriate AML training.

This training aims to ensure that all personnel are adequately prepared to recognize, assess, and respond to money laundering and terrorist financing risks in accordance with AMLA and VQF SRO Regulations.

10. RESPONSIBILITIES

The Company maintains a well-defined structure of responsibilities and authority in all matters related to anti-money laundering and the implementation of the AMLA. This structure ensures that all roles involved in due diligence, risk evaluation, transaction monitoring, and reporting are clearly assigned, consistently executed, and traceable across operational and governance levels.

Responsibility within the AMLA framework is distributed in accordance with the Company's internal control system and the requirements of the VQF SRO Regulations, particularly Articles 61, 81, and 82, which govern the principles of delegation, oversight, and internal accountability. The allocation of duties supports not only regulatory compliance but also the efficient and risk-conscious operation of the Company.

Overview of Responsibilities and Governance

The Company operates under a tiered governance structure that separates strategic oversight, operational execution, and independent control.

The Board of Directors, acting as the Company's senior executive body, retains overall responsibility for AML governance. It approves key directives and policies, ensures that the AMLA Officer (AMLA Department) are sufficiently resourced, and monitors the general effectiveness of the internal control system. The Board of Directors is informed regularly of compliance issues, material risk exposures, and any reports submitted to MROS.

AMLA Officer under the authority of the Board of Directors, is responsible for the implementation of the AML strategy in day-to-day operations. This includes ensuring compliance with operational obligations, supervising the onboarding process, supporting the

AMLA Officer in enforcing internal regulations, and approving escalated decisions such as the acceptance of increased risk customers.

The AMLA Department, acting independently from the operational business units, is responsible for overseeing the full implementation of the Company's AML measures. It evaluates customer and transaction risks, reviews alerts, monitors ongoing compliance with due diligence obligations, and ensures that all procedures remain aligned with the Company's internal policies and the VQF regulatory framework.

Assignment of Specific Duties

The Company ensures that individual AML-related responsibilities are allocated with precision, and that all personnel involved in these processes are appropriately trained and supported.

Customer identification and onboarding are carried out by trained Account Managers. They are responsible for obtaining all relevant KYC documents, ensuring completeness, and verifying customer identity in accordance with internal procedures. Document verification must be completed prior to activating the business relationship.

The completion of risk profiles and documentation, including the VQF Risk Profile (Doc. No. 902.4) and the Customer Profile (Doc. No. 902.5), is performed by onboarding staff under the supervision of the AMLA Officer. The information gathered forms the basis of the customer's risk classification and transaction monitoring thresholds.

Assessment of the origin of funds and wealth is performed jointly by the Account Managers and the AMLA Department. Where inconsistencies arise or red flags are detected, the AMLA Officer may request additional documents or clarifications from the customer. EDD is initiated if necessary.

Transaction monitoring is conducted via automated surveillance tools, with alerts reviewed by the AMLA Department. Where anomalies are detected, AMLA Officers perform Directive reviews and customer clarifications in accordance with internal procedures.

Approval of increased risk customers and transactions is subject to a two-step control. First-level review is carried out by the AMLA Officer, with final approval granted by the Compliance Committee, composed of the AMLA Officer and the Board of Directors. No increased risk customer is accepted without this approval. For PEP or profiles of exceptional sensitivity, the AMLA Officer may also consult Compliance Committee.

Reporting of suspicious activity to MROS is the responsibility of AMLA Officer. AMLA Officer ensures that all reporting obligations are fulfilled independently and without undue delay.

Escalation and Internal Reporting

Escalation procedures are embedded within the Company's AMLA framework to ensure timely intervention in cases of uncertainty, increased risk, or suspected abuse.

All red flags, unresolved anomalies, or confirmed risk events must be promptly escalated to the AMLA Officer. If further escalation is required, the case is referred to the Compliance Committee for decision. This escalation path is clearly defined and documented.

The AMLA Officer prepares regular compliance reports for both the Board of Directors. These reports cover the overall status of AML controls, training activities, customer risk profiles, monitoring trends, and any reports filed with external authorities. Reports are issued at least annually or more frequently if material risks or incidents arise.

Oversight and Accountability

All AMLA-related activities within the Company are performed under the principle of segregation of duties and the four-eyes principle, ensuring that no individual is solely responsible for critical decision-making in increased-risk or sensitive areas.

Responsibilities are formally communicated through job descriptions, onboarding briefings, and internal compliance memos. Each individual engaged in AMLA functions is made aware of their obligations and the scope of their decision-making authority.

The AMLA Officer is accountable for maintaining up-to-date documentation of responsibilities and ensuring that staff operate within the defined control structure. The Company regularly reviews its internal delegation and escalation framework as part of its compliance risk assessment and internal audit processes.

This structure ensures that AML responsibilities are executed efficiently, transparently, and in full compliance with applicable law, while maintaining appropriate checks and balances across all levels of the Company’s governance and operations.

11. RESPONSIBILITY FOR REPORTING TO MROS

The Company defines clear internal procedures for the identification, evaluation, and reporting of suspected money laundering or terrorist financing activities, in line with the obligations set forth in Articles 66 to 72 of the VQF SRO Regulations and Articles 9 and 10 of the Anti-Money Laundering Act (AMLA).

Responsibility for fulfilling these obligations lies with the AMLA Officer, who is entrusted with the authority to assess suspicious activity, take immediate protective measures, and report to the Money Laundering Reporting Office Switzerland (MROS) where legally required. There is no separate MLRO function within the Company; all duties typically assigned to such a role are integrated into the mandate of the AMLA Officer.

When the AMLA Officer identifies a transaction, behavior, or customer profile that may indicate a criminal origin of assets, the financing of terrorism, or participation in a criminal organization, they conduct a prompt internal analysis to verify whether the suspicion meets the reporting threshold defined in Article 9 AMLA. This review includes examination of transaction data, correspondence, the customer’s risk profile, and any clarifications already obtained.

If the suspicion cannot be dispelled and the conditions for reporting are met, the AMLA Officer independently prepares and submits a suspicious activity report (SAR) to MROS without

delay. While the AMLA Officer may consult with the Compliance Committee in complex or reputationally sensitive cases, the decision to submit the report remains their sole legal and operational responsibility.

Simultaneously, the AMLA Officer ensures that any assets related to the suspected activity are immediately frozen, as required under Article 10 AMLA, and that no further transactions are processed until either MROS provides clearance or the legally mandated waiting period expires.

The AMLA Officer is also responsible for enforcing the ban on informing third parties, commonly referred to as the “tipping-off ban.” Under no circumstances is the customer, their representative, or any other third party informed of the report, the freeze, or the internal investigation. Disclosure is strictly limited to those Company employees directly involved in the reporting process and bound by internal confidentiality obligations.

All decisions, analyses, communications with MROS, and related documentation are securely retained in the customer’s AMLA file. These records are made available only to competent supervisory authorities or upon legal request, and are managed in line with the Company’s retention and audit obligations.

By concentrating the reporting function within the role of the AMLA Officer, and supporting it with clearly defined procedures, the Company ensures legal compliance, rapid internal action, and the integrity of the reporting process.

12. ENGAGEMENT OF EXTERNAL AUXILIARY PERSONS

The Company does not engage any external auxiliary persons or third-party service providers for the fulfillment of due diligence obligations under AMLA. All responsibilities—ranging from customer identification to transaction monitoring and reporting—are conducted exclusively by internal personnel under the supervision of the AMLA Special Department.

Internal processes are designed to ensure that staff have the required knowledge, systems, and training to fulfill all due diligence obligations independently and in accordance with the VQF SRO Regulations.