VONBAN SWISS AG

TRANSPARENCY AND AML POLICY

Date of Issuance: February 2025

VONBAN

Contents

INTRODUCTION

The purpose of this policy is to establish controls for VONBAN SWISS AG (hereinafter referred to as the "Company" or "VONBAN") against Anti-Money Laundering and Counter-Terrorist Financing. It aims to introduce measures that mitigate the risks of money laundering and/or terrorist financing threats, which VONBAN may encounter as a result of its business activities.

CLIENTS ARE REQUESTED TO READ, UNDERSTAND AND ACCEPT THE CONTENTS OF THIS POLICY PRIOR TO ENTERING INTO A RELATIONSHIP WITH VONBAN.

VONBAN fully acknowledges that its products and services might be at risk from individuals seeking to launder criminal proceeds or facilitate funds designated for the financing of terrorism. As such, the Company is committed to fostering and promoting a compliance culture throughout the firm which underpins the importance of preventing Money Laundering and Terrorist Financing.

The Company maintains systems and controls to prevent financial crime that align with the risks inherent in its business and products. Consequently, the Company has developed this AML Program. As part this program, VONBAN is obligated to adhere the following:

- Anti-Money Laundering Act (AMLA) and related ordinances;
- Swiss Criminal Code (SCC);
- Federal Act on the Suppression of Terrorism (Terrorismusgesetz) and other relevant Swiss legislation;
- Federal Act on Combating Money Laundering and Terrorist Financing in the Financial Sector (Geldwäschereigesetz, GwG);
- Relevant FINMA regulations, guidelines, and circulars.

The Company takes into account the guidance, provisions, and findings contained within:

- Financial Market Supervisory Authority (FINMA) guidelines and circulars;
- Financial Market Supervisory Authority (FINMA) Anti-Money Laundering (AML) Circulars;
- Federal Department of Finance (FDF) regulations and guidance on combating money laundering and terrorist financing;
- Relevant guidance and reports issued by the Financial Action Task Force (FATF) and other international organizations.

1. KEY DEFINITIONS

Money laundering ("ML") is defined as the process of concealing, disguising, converting, transferring, or removing the proceeds of criminal activity to make them appear legitimate. It involves handling funds or property that are the product of criminal conduct, with the intention of disguising the illicit origins of those funds or property. The primary purpose of money laundering is to enable criminals to enjoy the benefits of their illegal activities without

drawing attention to the true source of their funds. Money laundering is a criminal offense under the Anti-Money Laundering Act (AMLA).

Terrorist financing ("TF") refers to the provision, collection, or receipt of funds or other financial resources, with the intention or knowledge that they will be used for the purposes of terrorism. The definition encompasses various activities, including:

- Directly or indirectly providing funds or financial assistance to individuals, groups, or organizations involved in terrorist activities.
- Fundraising, collecting, or soliciting money with the knowledge or suspicion that it will be used to support terrorist acts.
- Possessing, managing, or using money or property with the intent to facilitate acts of terrorism.

Client/Client – a person (whether legal entity or natural person) who seeks to form a business relationship, or with whom a business relationship is formed.

Senior management – Company officers or employees with sufficient seniority, possessing sufficient knowledge of the Company's ML/TF risk exposure, and responsible for taking decisions affecting its risk exposure such as the Board Members.

Financial Crime refers to a variety of illegal activities involving the abuse of financial systems and institutions for criminal purposes. It includes various offenses such as money laundering, fraud, bribery, corruption, terrorist financing, insider trading, tax evasion, and other illicit financial activities.

Financial sanctions are measures imposed by national governments and multinational bodies aimed at influencing the behavior and decisions of other national governments or non-state actors that may pose a threat to global security or violate international norms.

VONBAN complies with the following sanctions measures:

- The Swiss State Secretariat for Economic Affairs (SECO) sanctions lists;
- The United Nations (UN) Security Council consolidated sanctions list;
- The European Union'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 distinct three key stages of Money Laundering:

- Placement: This involves the physical or financial placement of proceeds from criminal activities or illegally obtained funds into financial institutions.
- Layering: This stage entails separating these proceeds from their original source by creating layers of transactions intended to conceal the ultimate source and transfer of the

funds. For example, illegally obtained funds may be divided into multiple transactions to hide their origin and obscure the connection to the initial entry point.

- Integration: Integration involves giving the appearance of legitimacy to the proceeds from criminal activities. Integration schemes reintroduce the illegally obtained funds into the economy as seemingly legitimate funds.

Money Laundering Offence: Pursuant to article 305bis of the Swiss Criminal Code (SCC), the following actions constitute money laundering offence and are subject to criminal proceedings:

- Taking steps to obstruct the identification, tracing, or forfeiture of assets that one knows or should assume originate from a felony or qualified tax offense;
- Committing a predicate offense, felony, or qualified tax offense;
- Intentionally committing an act aimed at forfeiting such assets;
- Knowing that the assets originate from a predicate offense;
- Predicate offenses include crimes against property such as misappropriation, fraud, robbery, criminal mismanagement, handling stolen goods, bankruptcy offenses, drug dealing, bribery, and evasion of indirect taxes, including stamp duties, withholding tax, VAT, customs duties;
- Engaging in or participating in an arrangement that the client knows or suspects facilitates the acquisition, retention, use, or control of criminal property by or on behalf of another person (section 328); or
- Acquiring, using, or possessing criminal property (section 329);
- Participating in an arrangement that facilitates the concealment, removal from the jurisdiction, transfer to nominees, or any other retention or control of terrorist property (section 18, Terrorism Act 2000).

Swiss Regulatory Authorities

- “FINMA”: The Swiss Financial Market Supervisory Authority, responsible for ensuring the proper functioning of Switzerland’s financial markets and compliance with anti-money laundering (AML) regulations.
- “MROS”: The Money Laundering Reporting Office Switzerland, the central authority for receiving and analyzing suspicious activity reports (SARs).
- “GwG”: The Federal Act on Combating Money Laundering and Terrorist Financing in the Financial Sector (AMLA) governs measures to prevent and detect money laundering in Switzerland.

2. SCOPE AND OBJECTIVE

The policy outlines how VONBAN will manage the risks associated with money laundering and ensure consistency across the Company.

This policy provides comprehensive guidance to employees of the company on addressing anti-money laundering issues.

All employees, directors, officers, and affiliated introducers are required to adhere to this policy. Failure to comply may result in disciplinary and/or legal consequences.

This AML policy, along with other existing AML controls, aims to achieve the following:

- Define the Due Diligence processes that the Company's Compliance Team must follow for proper client onboarding.
- Identify ML and TF risks inherent to the company's business through established client risk assessment procedures.
- Define the Company's risk appetite statement for each member to adhere to in their respective duties.
- Implement procedures for screening clients.
- Identify suspicious transactions and define appropriate actions for reporting them.
- Appoint a MLRO responsible for AML Compliance.
- Provide AML&CTF training to employees.
- Implement internal record-keeping requirements.

The Company ensures that its internal controls and procedures effectively identify, assess, and manage ML/TF risks.

The AML policy undergoes review at least annually and whenever there are changes in legislative requirements, modifications in the Company's activities, or significant events.

The MLRO is responsible for monitoring compliance with this AML policy.

All employees of the Company are obliged to read the policy and confirm their understanding in writing.

Additionally, new employees must complete AML and Sanctions training before starting work, and existing employees must undergo AML training annually.

3. THE MONEY LAUNDERING REPORTING OFFICER (MLRO)

VONBAN clearly outlines the roles and responsibilities of all individuals overseeing the Company's AML/CTF strategy and ensuring compliance with all AML/CTF requirements.

The policy is communicated to all staff during their onboarding process. Updates are communicated via email from the MLRO.

In relation to training requirements, administrative staffs who do not handle financial transactions or sensitive client information may not require AML training. Similarly, software developers based abroad who are not directly involved in financial operations or client interactions, unless working on systems related to AML compliance, may also be exempt from AML training.

The Company's Money Laundering Reporting Officer (MLRO) is responsible for the following:

- Ensuring that the firm's AML/CTF policies, procedures, and controls are appropriately designed and implemented to mitigate the firm's exposure to Money Laundering and Terrorist Financing.
- Participating in the decision-making process regarding the firm's AML/CTF strategy and taking ownership of the risk-based approach.
- Involvement in the development of the firm's policies, procedures, and controls, as well as approving them.
- Understanding the level of Money Laundering and Terrorist Financing risk to which the firm is exposed.
- Ensuring that the firm fulfills its obligations under the Anti-Money Laundering Act, Federal Act on the Suppression of Terrorism, and other relevant Swiss regulations.
- Implementing Business Risk Assessment for each activity undertaken by the company,
- Incorporating legal and regulatory requirements into company policies and procedures,
- Establishing a monitoring system for suspicious transactions to enable reporting investigation, documentation, and handing off to the authorities,
- Carrying out regular risk assessments and advise on actions to be taken,
- Promoting a compliance culture across Golden Suisse,
- Serving as the company's liaison with the regulator.
- Handling communication between the Company and relevant authorities.
- Receiving, analyzing, and submitting internal suspicious activity reports.
- Approving Politically Exposed Persons (PEPs).
- Approving higher-risk clients.
- Delivering training sessions.

All other compliance matters are communicated to the MLRO upon triggered events and upon operational requirements.

All employees of VONBAN undergo screening and vetting and are being vigilant about the possibility of any of its managers, internal or external staff (employees) engaging in ML/TF activities or assisting individuals outside the company in such activities.

To prevent and detect any potential misconduct by an employee, the Company policy includes rigorous processes for recruiting new staff and monitoring all relevant staff activities.

VONBAN assesses the risk of money laundering or terrorism financing associated with individual positions within the company and conducts appropriate due diligence and screening of employees in each case. Employees undergo screening upon onboarding and at regular intervals during their employment with the company.

Employee screening involves evaluating the skills, knowledge and expertise necessary for the effective performance of their duties, including the behavior and integrity of the individual.

All employees receive training to recognize and report suspicious activities. They also undergo regular training on the laws pertaining to Anti-Money Laundering and Counter Terrorist Financing.

Employees with access to AML systems undergo enhanced background checks, including financial and criminal records. Annual AML training is mandatory for all staff, covering updates in Swiss regulations, international sanctions, and emerging money laundering typologies. Completion is documented in employee records.

4. RISK BASED APPROACH CULTURE

VONBAN implements a comprehensive risk-based approach and conducts a thorough analysis of its exposure to ML/TF risks.

Accordingly, senior management of VONBAN recognize the importance of conducting a firm-wide risk assessment to identify and evaluate ML/TF risks relevant to the business.

This assessment ensures that ML/TF risks are adequately identified and continually monitored, allowing the company to implement proportionate measures to effectively manage these risks.

The Business-Wide Risk Assessment (BWRA) must consider risks arising from the following categories:

- Jurisdictional Risk.
- Client Risk.
- Product/Service Risk.
- Transaction Volume Risk.
- Delivery Channel Risk

The Company conducts a Business-Wide Risk Assessment (BWRA) considering the inherent risks of the business and their potential impact and likelihood. Subsequently, the Company evaluates appropriate controls to mitigate these risks and establishes an acceptable risk level or risk appetite.

This process helps to clearly identify acceptable relationships and those considered risky, where identified risks cannot be sufficiently mitigated through existing controls. As a result, relationships deemed unacceptable to the Company are promptly identified. This comprehensive approach ensures effective mitigation of any remaining risk after the risk assessment.

All inherent risks in the business are identified and mitigated accordingly. An overall residual risk to the firm’s business is developed, and controls and resources allocated where most needed to mitigate ML/TF risks. More resources and risk-mitigating measures are allocated to areas with the highest identified risks.

The Board of the Company is informed about the results of the firm-wide risk assessment. The Compliance and Risk team records the number of High-Risk clients, the number of clients using high-risk products, the number of high-risk transactions, the number of transactions performed to and from high-risk countries, and the number of clients in different risk groups (low, medium, high).

The BWRA is reviewed annually or more frequently if triggered by an event.

This approach aims to identify the most cost-effective and proportionate way to manage and mitigate the risks posed to the Company.

The rationale behind the Company's application of the risk-based approach is not to deviate from the due diligence measures where the risk of ML/TF is low, but rather to provide flexibility to vary the extent of the application of the due diligence measures depending on the level of identified risks.

The risk-based approach enables senior management to customize systems and controls to specific business needs, thereby focusing resources more effectively where needed.

A risk-based approach requires VONBAN to undertake the following steps:

- Identify ML/TF risks relevant to the Company.
- Assess the risks presented, particularly regarding:
  - Clients and any underlying beneficial owners
  - Products or services
  - Acquisition channels (inbound vs. outbound)
  - Geographical areas of operation
- Design and implement controls to manage and mitigate these assessed risks, considering the company's risk appetite.
- Monitor and enhance the effective operation of these controls and appropriately document the actions taken and the reasons behind them.

The Company regularly undertakes appropriate measures, proportionate to the nature and size of its operations, to identify and evaluate the risks of money laundering and terrorist financing arising from its activities or business. This includes considering risk factors such as client profiles, geographical locations, delivery channels, and any national or supranational risk assessments related to money laundering and terrorist financing risks.

During the onboarding process of a business relationship, as well as on an ongoing basis, a risk assessment of the applicant's business, including beneficial ownership, will be conducted based on the following risk criteria:

- Client Risk
- Product Risk
- Geographical/Country Risk
- Channel Risk

The resulting risk category will determine:

- Acceptance or rejection of the business relationship
- Type of due diligence conducted
- Frequency of ongoing monitoring

VONBAN assesses AML/CTF risks by implementing a risk-based approach and considering national and supranational risk assessments, as well as recommendations and guidelines from organizations such as the Financial Action Task Force (FATF), European Banking Authority (EBA), and other relevant international and local laws and regulations.

In compliance with Swiss regulations, the Company conducts regular risk assessments to evaluate all Money Laundering and Terrorist Financing risks associated with its business operations.

The Company has developed a Client Risk Assessment (CRA) framework to assess inherent risks across its consumer clients. This includes internal procedures and processes to conduct individual ML/TF risk assessments and categorize clients into specific risk categories based on factors such as client type, activity frequency, relationship history, country of residence, and offered products.

Areas assessed to determine the company's AML vulnerabilities include risks posed by clients, products and services offered, geographical areas of operation, transaction volume and complexity, and delivery channels used.

Appropriate due diligence is conducted before establishing a business relationship with a client, with the level of due diligence determined by the client's inherent risk rating and ongoing monitoring requirements.

Clients undergo a Client Risk Assessment (CRA) during onboarding and at regular intervals thereafter. Risk levels (Low, Medium, or High) are assigned based on various factors, with different review frequencies applied accordingly.

Changes in a client's circumstances or risk factors may lead to a reassessment of their risk level, with due diligence re-requested for verification purposes.

Any significant changes in risk types during the client relationship, such as adverse media discoveries, ownership structure changes, or unusual behavior, trigger a re-review of the client's inherent risk assessment.

In cases of suspicious behavior, an Unusual Activity Report is completed and submitted to the MLRO with a Suspicious Activity Report (SAR) sent to the Swiss Financial Market Supervisory Authority (FINMA) if suspicions are justified.

5. VONBAN's RISK APPETITE

VONBAN is dedicated to combatting financial crime and ensuring that its products are not utilized for the purposes of money laundering, terrorist financing, or fraudulent activities. The company upholds strict and transparent standards and continually enhances its internal processes to ensure compliance with relevant laws and regulations.

The risk appetite applies to all employees, clients, products, and activities of the Company. The Company adheres to the Risk Appetite Statement in cases where concerns or issues arise regarding VONBAN's conduct, its clients, products, or countries of operation.

The company has zero tolerance for:

- Establishing or maintaining business relationships with clients from sanctioned countries or activities.
- Maintaining business relationships with clients attempting to initiate or receive transactions from prohibited jurisdictions.

The Company does not accept clients who are residents from the below listed jurisdictions:

1. Afghanistan
2. Belarus
3. Bosnia and Herzegovina
4. Burundi
5. Central African Republic
6. Crimea and Sevastopol
7. Cuba
8. Darfur
9. Ghana
10. Guam
11. Guatemala
12. Iran
13. Iraq
14. Laos
15. Libya
16. Myanmar/Burma
17. North Korea
18. Russia (excluding Crimea and Sevastopol)
19. Somalia
20. South Sudan
21. Syria
22. Venezuela
23. Yemen

The Company maintains a strict policy of zero tolerance towards any violations of financial crime laws and regulations within its business operations.

Moreover, the Company strictly prohibits engaging with any individuals who are subject to international sanctions or embargoes. It is essential for the Company to fully comply with all sanction requirements.

6. CLIENT DUE DILIGENCE

One of the key requirements for preventing money laundering is the implementation of client-related due diligence or Know Your Client (KYC) processes. These obligations include identifying the client and any persons acting on their behalf, determining the beneficial owner, gathering information on the purpose and intended nature of the business

relationship, assessing any politically exposed person (PEP) status, and continuously monitoring the business relationship.

The existing Client Due Diligence Procedures enable the Company to identify its clients and understand the purpose and intended nature of the business relationships.

The Company conducts thorough and rigorous due diligence on each client to evaluate their status, identity, and suitability for the product/service in question.

The Client Due Diligence (CDD) measures implemented include:

- Identifying the client and verifying their identity using documents or information from a reliable and independent source.
- Identifying the beneficial owner(s) and verifying their identity, understanding the ownership and control structure of the client.
- Assessing the purpose and intended nature of the business relationship (business profile).
- Conducting ongoing monitoring of the business relationship and transactions to ensure consistency with the company's understanding of the client, business, risk profile, and source of funds.

The Company applies CDD measures in the following situations:

- Before establishing a business relationship and providing any services to the client.
- Prior to conducting an occasional transaction.
- In case of suspicion of Money Laundering or Terrorist Financing.

If the Company is unable to apply CDD measures to a client, it will:

- Refrain from executing any transaction for the client.
- Avoid establishing a business relationship with the client.
- Terminate an existing business relationship with the client if necessary.

The Company may also in some instances consider submitting a suspicious activity report.

In addition to verifying the identity of the client, VONBAN shall also gather information on the purpose and intended nature of the business relationship, including knowledge of the following elements:

- Information on the projected turnover and scope of the business that the client intends to conduct with the Company.
- Details regarding the anticipated destination of payments.
- Information about the business, its products, and services.
- Details concerning the anticipated utilization of the services provided by VONBAN
- Expected amounts of monthly and yearly monetary transactions and the countries involved in the initiation or receipt of monetary transactions.

Certain types of clients are considered higher risk. Consequently, such clients may undergo additional due diligence checks. If there is limited publicly available information or if the risk is deemed unacceptable, these clients will be prohibited from conducting business with VONBAN.

Type of physical persons are currently recognized by VONBAN during Client Due Diligence.

Permitted Natural Persons:

- Persons above the age of 18
- Persons requesting settlement accounts where each incoming amount is intended to settle main transaction, or for forwarding purposes
- Persons requesting settlement accounts for rapid circulation, where incoming funds are forwarded within sixty (60) days
- Persons who are deemed institutional
- Persons who are acting as professional treasurers
- Persons legally residing in Switzerland
- Persons legally residing in the EEA
- Persons legally residing in countries deemed acceptable under FATF:

Argentina	Japan
Australia	Republic of Korea
Austria	Luxembourg
Belgium	Malaysia
Brazil	Mexico
Canada	Netherlands
China	New Zealand
Denmark	Norway
Finland	Portugal
France	Saudi Arabia
Germany	Singapore
Greece	South Africa
Hong Kong (China)	Spain
Iceland	Sweden
India	Switzerland
Ireland	Turkey
Israel	United Kingdom
Italy	United States

Restricted Persons:

- Self-employed persons
- Persons above the age of 65
- Politically Exposed Persons from Restricted Countries

- Persons with no employment or commercial holding history
- Persons with no tax residency certificates
- Persons having business interests of over 50% in restricted countries
- Persons receiving or generating active or passive income from restricted countries

Prohibited Persons:

- Persons opening accounts solely for deposit purposes or interest generation purposes
- Persons requesting settlement accounts not intended for rapid circulation, where incoming funds are forwarded within sixty (60) days
- Persons under the age of 18
- Incapacitated persons
- PEPs from prohibited countries
- Persons residing in prohibited countries
- Persons having business interests in prohibited countries
- Persons with Felonies as per the Swiss Criminal Code

The type of legal entities currently recognized by VONBAN during Client Due Diligence.

Permitted Legal Entities:

- Eligible Companies with professional treasury operations
- Eligible Companies requiring to maintain necessary liquidity for processing customer business
- Eligible Companies requesting settlement accounts where each incoming amount is intended to settle main transaction, or for forwarding purposes
- Eligible Companies requesting settlement accounts for rapid circulation, where incoming funds are forwarded within sixty (60) days
- Limited Company
- Public Limited Companies
- General Partnerships
- Joint Ventures with clearly defined shareholder agreements and charters

Restricted Legal Entities

Clients are restricted and enhanced due diligence is conducted where the legal form of the contracting entity is:

- Private Partnerships
- Limited Partnerships without General Partners
- Limited Partnerships in Tax neutral Jurisdictions
- Registered Charity or Foundation
- Sole Proprietor/Trader
- A trust
- Société de Gestion de Patrimoine Familial – SPF

- Funds/ Variable capital investment companies/Special purpose vehicles/Sovereign wealth funds
- Micro Enterprises
- Companies pending incorporation or legal registration
- Newly Redomiciled Companies

Prohibited Legal Entities:

Clients cannot be accepted where the legal form of the contracting entity is:

- A company which does not have professional treasury operations
- A company which intends to keep received funds for more than 60 days
- A company which does not intend to collect funds to be subsequently forwarded for the settlement between them, and for example, vendors, service providers and suppliers
- A company without an identified UBO as a physical person
- A holding company without commercial holdings
- A holding company in tax neutral jurisdictions
- A holding company for a private individual without commercial subsidiaries
- Unregistered charity or foundation
- A company with bearer shares
- Shell companies
- Companies from prohibited countries
- Subsidiaries of companies from prohibited countries
- Any company deemed to be used for tax evasion purposes

Below are the outline of sectors industries and types of businesses that are not recognized by VONBAN during due diligence.

Prohibited Business Sectors

VONBAN does not provide any type of services to businesses offering the following activities/services:

Business Sector	**Activity/Service**
Adult/Dating	Escort/Prostitution Agencies Pornography featuring children, rape, humiliation, or bestiality Any other form of pornography depicting sexual intercourse
Animals & Plants	Unlicensed Animal trades. Unlicensed Animal feed trades.

	Import and Export of souvenirs derived from protected animal and plant species under the Swiss Federal Laws
Bail Bondsman	Bail Bondsmen related activities
Cash/Foreign Currencies/Securities	Physical Cash trading activities of any kind. Physical foreign exchange activities of any kind. Physical securities transfer activities of any kind
CBD	Marijuana dispensaries
CFD Trading/Spread betting	Unregulated CFD/FX traders Binary Options traders CFD Brokers licensed in the following jurisdictions: ▪ Marshall Islands ▪ Cayman Islands ▪ Vanuatu ▪ United Arab Emirates (UAE) – where regulatory regime is part of Sharia Law ▪ Belize
Cryptocurrency/Blockchain	ICOs/IEOs/IDOs ATMs Unregulated cryptocurrency exchanges (or any other related services) where licensing or registration for AML/CFT purposes is a legal requirement Cryptocurrency businesses with insufficient KYC & CDD practices
Cultural Property	Any activities related to transfers of cultural and/or archaeological assets/properties of any kind unless explicitly licensed by a public authority
Financial Services	Unregulated or inadequately licensed financial institutions/money service businesses Lending, including Pay-day lenders Unregulated account aggregators
Fireworks (Pyrotechnic)	Trading activities related to pyrotechnic/fireworks and hazardous substances related to the fireworks sector.
Fortune Tellers	Any fortune telling activities, including but not limited to tarot cards, horoscope readers and psychics

Gambling	Unlicensed gambling activities Skins/loot box trading Unlicensed game of chance activities
Get-rich-quick Schemes	Any schemes marketed as get-rich-quick Pyramid Schemes Multi-level marketing
Narcotics & Drugs	Any activities related to narcotics, drugs, and abusive substances as per the definitions set by the Swiss Agency for Therapeutic Products (Swiss medic) website.
Pharmaceuticals	Drug related paraphernalia, e.g., selling bongs, hookah Illegal/synthetic drugs or prescription drugs without a prescription
Regulated Services	Non-licensed counselling centres Unlicensed lawyers or legal services Unlicensed Auditing Services
Speciality Retail	Counterfeit goods Human body parts Offensive goods related to crime, e.g. photographs memorabilia Tobacco & electronic cigarettes Pyrotechnic devices and hazardous materials, e.g. fireworks, explosives, toxic/flammable goods Animals and Livestock Interference transmitter (jammers) Stolen Property Police-related items Army and National Security Services related items Mailing lists and personal information Government documents and IDs Lock picking devices Embargoed goods from prohibited countries
Streaming	Illicit streaming of copyright media and software

Telecommunications	Illegal telecommunications devices Illegal telecommunication interceptor devices
Timeshare	Any type of timeshare service/product
Weapons	Activities of any kind related to firearm weapons, weapon components, ammunition and ammunition parts

7. ENCHANCED DUE DILIGENCE

The Company conducts inherent client risk assessments before onboarding a client. If a client risk assessment results in High Inherent Risk, Enhanced Due Diligence (EDD) measures are implemented to mitigate identified risks.

EDD is typically applied in the following circumstances:

- When a Politically Exposed Person (PEP) is identified;
- When financial crime-related adverse media is discovered;
- When establishing a business relationship with a Client residing or incorporated in a high-risk country;
- When the beneficial owner of a client resides in a high-risk country;
- When the client's mother company is incorporated in a high-risk country;
- When declared or expected transactions are conducted to or from a high-risk third country;
- When the natural person or persons related to a client fall in the restricted persons list;
- When the client belongs to or transacts with a restricted sector as indicated in the due diligence section.

EDD measures are applied for each high-risk case, in addition to regular Client Due Diligence (CDD) measures.

The VONBAN Compliance Team considers the following situations as high risk:

- Client inherent risk assessment results in high risk;
- The client or a potential client is a PEP, if the client is a close associate of a PEP or if a family member is a PEP or associated with a PEP;
- The client is involved in a business activity connected to a high-risk country;
- The client resides, operates, or is incorporated in a high-risk country;
- The client is from a high-risk industry;
- The client conducts businesses or produces products that may present a higher risk of Money Laundering and Terrorist Financing (ML&TF);
- Relevant adverse media is discovered;
- In any case where a transaction is complex and unusually large, or there is an unusual pattern of transactions;

- In any case where a transaction or transactions have no apparent economic or legal purpose;
- Transactions performed to/from high-risk countries;
- In case of an opaque ownership structure of a legal entity client;
- Any client or business activity falling within the restricted list noted in the client Due Diligence Section.

EDD measures applied by the Company include:

- Obtaining senior management approval to start or continue the business relationship;
- Increased identification and verification of documents relating to the client, directors, controllers, and/or beneficial owners;
- Detailed inquiries to understand and validate the purpose and nature of the business relationship, including the client's source of wealth and/or source of funds, directors, controllers, and/or beneficial owners;
- Obtaining additional information on the client's occupation, volume of assets, information available through public databases;
- Confirmation of expected activity to be transacted by the client;
- Scrutiny of transactions utilizing automated/manual transaction monitoring systems;
- Enhanced monitoring of the client’s transactions;
- Obtaining information on the reasons for intended or performed transactions;

Conducting enhanced monitoring of the business relationship by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination.

The below is a non-exhaustive list of documents and information which may be requested from the client as a part of EDD.

- A certified company structure;
- Annual audited accounts;
- A credit reference (from a reputable credit reference agency);
- Financial statements and banking references;
- Business Plan;
- Source of funds or source of wealth information in relation to a director, shareholder, the ultimate beneficial owner, or an end user;
- Proof of employment of a shareholder, the ultimate beneficial owner, or an end-user;
- A copy of the most recent independent financial crime audit;

As part of EDD, the following Source of Funds and Source of Wealth may be requested:

- Identity proof and proof of address of all the directors and shareholders owning 10% of shares or more;
- Current Management Accounts;

- Bank statements showing income not older than 3 months;
- Documents confirming Source of Funds and Source of Wealth of the shareholders or/and beneficial owners;
- Letter of secured or unsecured loan;
- Wage slip or contract letter from employer;
- Annual Income (confirmation from employer or tax filing);
- Financial returns & audited accounts.

For high-risk clients, Vonban will:

- Require independent verification of source-of-funds documentation, including confirmation by a regulated financial institution.
- Conduct site visits or interviews where necessary.
- Utilize third-party data providers to validate wealth origins and confirm legitimacy.

8. SANCTIONS SCREENING

International sanctions are political and economic measures imposed by countries or international organizations to influence the behaviour of other states or entities. These sanctions are typically used to protect national security interests, uphold international law and maintain or restore international peace and security.

They serve as a legitimate foreign policy tool, wherein one or more countries impose penalties and restrictive measures against states, individuals, or entities that engage in actions such as human rights violations, contributing to territorial or religious conflicts, supporting terrorism, or violating fundamental norms recognized by the international community.

VONBAN complies with and screens against international sanctions, including, but not limited to the following lists:

- Swiss State Secretariat for Economic Affairs (SECO) consolidated sanctions lists;
- The European Union Consolidated Financial Sanctions List;
- The United Nations (UN) Security Council consolidated sanctions list;
- 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;
- UK's Office of Financial Sanctions Implementation (OFSI)-HM Treasury Consolidated Financial Sanctions List

The screening is conducted against the above-mentioned lists with the following frequency:

- Prior to entering into a business relationship;
- During the onboarding process;
- Monthly, throughout the course of ongoing business relationships.

Each potential match undergoes verification and investigation. A match will be considered false if it involves a different name, date of birth, gender, or place of incorporation (in the case of a legal entity client). The evaluation process of a match is documented, and the person in charge records the reasons for a particular decision made.

A positive sanction hit is reported to the MLRO immediately. The MLRO may there onwards inform SECO and the relevant authorities about the suspension of accounts of persons or entities subjected to sanctions. The company is prohibited from engaging in activities that are prohibited by international financial sanctions.

9. POLITICALLY EXPOSED PERSON (PEP) SCREENING

A politically exposed person ("PEP") refers to any natural person who currently holds or has previously held a prominent public function in Switzerland or in another country, or is an immediate family member of such an individual, or an individual known to be closely associated with them.

Politically exposed persons specifically include:

- Heads of State, Heads of Government, Ministers, Deputy Ministers, and Secretaries of State.
- Members of parliament and equivalent legislative bodies.
- Members of the governing bodies of political parties.
- Members of supreme courts, constitutional courts, or other high courts whose decisions typically have no further recourse.
- Members of the governing bodies of audit institutions.
- Members of the governing bodies of central banks.
- Ambassadors, chargés d'affaires, and defense attachés.
- Members of the administrative, management, and supervisory bodies of state-owned enterprises.
- Directors, Deputy Directors, members of the governing body, or other leaders with comparable roles in intergovernmental international or supranational organizations.

Close associate – a natural person who shares membership with a PEP in the same legal entity or non-legal entity body, or maintains another business relationship with the PEP, or is the sole Beneficial Owner of a legal entity or non-legal entity body established or operating de facto to acquire property or personal benefits for the PEP.

Close family members – the spouse, the person with whom the partnership is registered (cohabitant), parents, brothers, sisters, children, children’s spouses, and children’s cohabitants.

Known Close Associate – means a known close associate of a PEP as being either an individual known to have joint beneficial ownership of a legal entity, legal arrangement or any other close business relationship with a PEP. Also, an individual who has sole beneficial ownership

of a legal entity, or a legal arrangement, which is known to have been set up for the benefit of a PEP.

The status as a Politically Exposed Person (PEP) typically ceases one year after the individual concludes their qualifying activity. If the Client, who is a PEP, no longer holds significant public functions, the Company must, within 12 months, reassess the remaining risks associated with the Client and implement appropriate measures based on the risk level.

These measures persist until it is confirmed that the risks commonly linked with PEPs no longer apply to the client.

Any declassification of a PEP can only take place with approval from MLRO. All declassified PEPs are documented. Additionally, risk-sensitive ongoing monitoring is continued until the former PEP is determined to no longer pose any specific PEP-related risks to the Company's business.

Due to the higher risk of money laundering posed by high-profile political figures, Enhanced Due Diligence (EDD) is applied to all PEPs. Application of EDD enables the Company to understand sources of wealth and source of funds relating to a PEP and to build a transactional and client profile to monitor transactions and PEP Client behavior.

The screening is performed against the details obtained in the identification documents which were collected during the client due diligence process. Re-screening occurs each month. Re-screening occurs each time relevant Sanctions or PEP lists change.

Every potential match is verified and investigated. A match can be considered as false in case it is based on a different name, a different date of birth, a different gender, a different place of incorporation (in case of a legal entity client).

VONBAN utilizes automated transaction monitoring tools to track PEP-related transactions in near real-time. Any flagged activity is escalated for manual review by the MLRO. Declassification of a PEP is subject to MLRO approval, documented in the client file, and communicated to relevant authorities as required.

10. ADVERSE MEDIA SCREENING AND SPECIAL INTEREST PERSONS (SIP) SCREENING

As part of Due Diligence verifications, the Company conducts adverse media searches. The Company is obliged to understand the reputation of its clients and must be aware whether they were previously investigated for any criminal offense committed or if any penalties were applied to them.

Every potential match must be verified and investigated. If the relevant member of the staff is not able to discount a match, it will be referred to the MLRO of the Company who will decide what further action is required.

11. TRANSACTION MONITORING

VONBAN conducts ongoing monitoring to all of its client relationships.

Throughout the duration of a client's account relationship, the Company will observe the activity within the account and scrutinize transactions to ensure they align with the Company's understanding of the client, their business, and risk profile, as well as the source of funds when applicable.

The Company will give particular attention to any complex, unusually large, or suspicious transaction patterns that lack an apparent economic or legal purpose.

For ongoing monitoring purposes, the Company has implemented adequate systems and processes tailored to the size and complexity of the company. This includes monitoring the account relationship with the client, ensuring compliance with the Company's requirements, and detecting and reporting suspicious or unusual transaction patterns.

Whenever possible, the Company will inquire about the background and purpose of such transactions and document its findings for potential disclosure to relevant authorities if necessary. If unusual patterns are identified, enhanced due diligence will be conducted, which may involve establishing the source and destination of funds, obtaining more information about the client's business, and monitoring the business relationship and subsequent transactions more closely.

Any suspicious activity will be reported to the MLRO for further investigation or reporting to the relevant authorities.

VONBAN adopts a risk-based approach to continuously monitor its clients for signs of money laundering, with a focus on transaction monitoring and client reviews. The company will apply varying levels of monitoring based on the risk rating assigned to each client.

As part of ongoing monitoring, the company will ensure that client documents, data, and information are updated at appropriate intervals.

The Company conducts periodic reviews of its clients, with the frequency of these reviews depending on the risk level posed by each client. The specific time frames for reviewing the accuracy of client data are as follows:

- Low-Risk Clients – reviewed once every two calendar years. This interval is based on the low risk of money laundering determined by the Client Risk Assessment (CRA) conducted by the Company.
- Medium-Risk Clients – reviewed once every 18 calendar months. If the CRA results in a medium risk of money laundering, the review of client data accuracy is conducted within the 18-calendar month’s period.
- High-Risk Clients – reviewed every 12 calendar months. For clients identified as posing a high risk based on the CRA results, data updates are performed on an annual basis.

The client risk assessments conducted on the existing client base are reviewed to capture any changes that may have occurred.

Whenever a triggering event occurs, such as anomalies detected during continuous monitoring, identification of a Politically Exposed Person (PEP), discovery of financial crime-related adverse media, or a previously unidentified match with sanctions, the client undergoes a thorough review.

In the event of changes in a client's circumstances, such as changes in corporate structure, ownership and control, client base, required products, jurisdictional scope of operations, transaction types, etc., a reassessment must be conducted.

Enhanced ongoing monitoring is applied to all clients that were assigned a high risk. It is also applied to all PEP relationships.

12. SUSPICIOUS ACTIVITY REPORTING

The Company defines suspicious activity as any activity that deviates from normal or usual practice. Furthermore, the Company acknowledges that its business activities may potentially attract clients with suspicious activity.

The purpose of reporting suspicious activity is to report any known or suspected violations of the law or suspicious activities observed by the Company's internal teams. The Company ensures that all its staff members can identify potential signs of fraud, money laundering, and terrorist financing.

The following behaviors are considered suspicious:

- The client fails to provide the required data and is unresponsive.
- The client submits incomplete or incorrect data.
- The client or its representative avoids providing the necessary data to establish its identity, conceals the identity of the beneficial owner, or avoids providing information necessary to establish the identity of the beneficial owner.
- It is not possible to determine whether the Client operates on its own behalf or is controlled by someone else.
- It is not possible to understand the ownership and control structure and the nature of the client's business (in the case of a legal entity client).
- It is not possible to obtain information about the purpose and intended nature of the client’s business relationship.
- It is not possible to verify the identity of the client and the beneficial owner according to documents, data, or information obtained from a reliable and independent source.
- An address provided by the client to identify an individual's residency or company's operational placement appears vague, unusual, or cannot be found on online databases and generally acceptable online maps.

If an individual is suspected, the report includes the individual's full name, date of birth, gender, identity number, country where the identity number was issued, occupation, address, contact details. The same details for any other associated parties suspected are also included in the report.

The onboarding or ongoing activity of such a reported client is stopped.

The MLRO analyzes such reports and determines whether the suspicions are justified. If the suspicion is validated, the MLRO proceeds with submitting a suspicious activity report to the relevant authority.

Suspicious Activity Reporting (SAR) Process

1. Internal Escalation: Employees must report suspicious activities to the MLRO within 24 hours of identification.
2. MLRO Analysis: The MLRO assesses the report, ensures supporting documentation is complete, and validates suspicion within 72 hours.
3. MROS Submission: Validated SARs are submitted to MROS within the statutory timeframe, ensuring compliance with AMLA Article 9.
4. Post-Reporting: Document SAR submissions, monitor the client's activity, and maintain ongoing dialogue with MROS as required.

12. ANNUAL POLICY REVIEW

This policy is reviewed annually by the MLRO in consultation with senior management. Updates incorporate changes in Swiss regulations, FATF guidance, and internal risk assessments. All updates are documented and communicated to employees.

13. POLICY DISCLOSURES

The reader of this Policy acknowledges and agrees that VONBAN may validly provide certain information, such as for example information about VONBAN, as well as amendments to this Policy, and other notices and policies exclusively via the VONBAN website.

All stakeholders are urged to undertake to consult the VONBAN website regularly at www.vonban.ch