Policy on anti-money laundering and counter-terrorism financing

December 2023

Introduction

Background and purpose

Avanza Bank Holding AB (publ) is the parent company of a group ("Avanza") whose companies are subject to the rules in the Act on Measures against Money Laundering and Terrorist Financing (2017:630) ("the Money Laundering Act") and the Swedish Financial Supervisory Authority's regulations (FFFS 2017:11) regarding Measures against Money Laundering and Terrorist Financing ("the regulations"). Avanza Bank Holding AB (publ) is not subject to the regulations, but in its capacity as parent company to companies that are subject to the regulations the Board of Directors of Avanza Bank Holding AB (publ) shall establish a single policy for the Group.

The purpose of the policy is to ensure that the companies in the Group share the same compliance guidelines and procedures and that they work effectively and with a risk-based approach to prevent the company from being exploited for money laundering and terrorism financing purposes. This also contributes to sound business practices and protects customers while reducing the risk that Avanza's brand will be adversely impacted.

Scope and entry into force

In addition to Avanza Bank Holding AB (publ), this policy covers Avanza Bank AB (publ), Avanza Fonder AB and Försäkringsaktiebolaget Avanza Pension ("the Companies") and all employees, contractors and others who for similar reasons participate in the activities of the Companies.

The policy is effective as of the date it is approved by the Board of Directors of Avanza Bank Holding AB (publ).

Communication and introduction

The CEO of each company shall inform every employee in a management position of the provisions of this policy and is responsible for its assimilation.

Definitions

Money laundering refers to measures with respect to money or other property generated from a criminal act that:

- can disguise the connection between the property and the criminal act,
- can enable the persons involved to avail themselves of the property or its value,
- can enable the persons involved to circumvent legal consequences, or
- mean that someone acquires, holds, claims the right to or utilises the property.

Measures that typically are intended to disguise that a person intends to enrich themselves or others through future criminal acts are also covered by the term.

Terrorism financing refers to collecting, supplying or receiving money or other property so that the property can be used, or in the knowledge that it is intended to be used, to commit a crime or used by a person or group of persons who commit a serious crime or are guilty of attempting, preparing, conspiring to or participating in such crimes. Collecting, providing or accepting money or other assets to be used, or in the knowledge that it is intended to be used, for terrorist purposes are also terrorism financing.

Sanctions refer to limits on the freedom to act for a state, a group or person through a collective decision by other states. Sanctions are enacted by the international community to try to influence the actions of states, groups or individuals through various financial and political means. Financial sanctions include freezing assets and other financial resources, restrictions on financial transactions and investment restrictions.

Strategic plan

Each Company shall have a documented strategy for anti-money laundering and counter-terrorism financing. The primary goal for Avanza is to implement effective, targeted measures based on Avanza's identified risks, in order to prevent Avanza from being exploited for money laundering and terrorism financing purposes. The Board of Directors of each Company shall for this purpose prepare and establish a strategic plan that is reviewed and updated annually or as needed.

Internal control

The Board of Directors and the CEO are ultimately responsible for ensuring that the necessary measures are taken to combat money laundering and terrorism financing, that internal rules are consistent with external laws and regulations, and that these rules are appropriate, implemented and complied with.

Independent audit function

An independent audit function (IAF) is included in the internal audit function. The responsibilities and tasks of the IAF are defined in each Company's guidelines within the area.

Appointed officer for controlling and reporting obligations

The Board of Directors appoints the Chief Compliance Officer (CCO) as the Group's appointed officer for controlling and reporting obligations (CFA). The responsibilities and tasks of the CFA are defined in each Company's guidelines within the area.

Specially appointed executive

Each Company shall determine whether the Company shall appoint a specially appointed executive (SAE). A decision not to appoint a SAE shall be motivated and documented in detail. Decisions shall be re-evaluated annually or when the business changes. The responsibilities and powers of, and information provided to, the SAE or equivalent officer if a SAE is not appointed shall be defined in each Company's guidelines within the area. If the Company does not appoint a SAE, the CEO is responsible for the areas of responsibility, powers and information that otherwise would been borne by the SAE.

The Board of Directors assigns the SAE the responsibility to implement and update a general risk assessment of how the Company's products and services can be exploited for money laundering or terrorism financing purposes and how large the risk is that it could occur, the preparation and updating of a Group policy, procedures and guidelines, and that the Company as a whole implements the measures and

controls (first line) stated in this policy. Moreover, the SAE shall compile periodic reporting for the SFSA. The SAE shall report at least once a year to the Board of Directors and the CEO.

General risk assessment

Each Company shall have a process for preparing a general assessment of the risk inherent in its business that it will be exploited for money laundering or terrorism financing purposes. Procedures must be in place to prepare, evaluate and update the general risk assessment.

The Company's SAE, or if one has not been appointed the Company's CEO, is responsible for ensuring that a general risk assessment is conducted at least once a year or when the business changes. The general risk assessment shall be designed to serve as the basis of the Company's procedures, guidelines and other measures to prevent money laundering and terrorism financing.

Internal procedures

Each Company's CEO or board of directors shall annually set out guidelines and instructions to complement this policy.

Moreover, each Company shall set out procedures whose scope and content are determined by the size, nature and risks of money laundering and terrorism financing which have been identified in the general risk assessment, and adapted to new and revised risks of money laundering and terrorism financing. The procedures cover the following areas:

- Implementation, evaluation and follow-up of the general risk assessment
- Implementation of Know-Your-Customer (KYC) and risk assessment of customers as well as continuous KYC monitoring
- Monitoring of suspicious transactions and activities as well as transactions and activities that while not unusual can be assumed to be part of money laundering or terrorism financing
- Reporting to the Swedish Police
- Responses to financial sanctions including freezing and reporting accounts and amounts
- Retention of documents or actions which have been taken for KYC purposes and which have been taken in reviewing suspicious transactions
- Training for employees on money laundering and terrorism financing
- Suitability assessments of employees
- Protection for employees from threats, revenge or other hostile actions and reprisals
- In cases where the Companies use models for risk assessment, risk classification, oversight or other routines, procedures shall be in place for model risk management.

Each Company shall maintain an appropriate reporting system for employees and contractors who want to report suspected non-compliance with the provisions of the Anti-Money Laundering Act or regulations – a whistleblower system. The Companies have previously adopted a Group-wide *Instruction on Whistleblowing* and a *Code of Conduct*.

Risk assessment of customers

Each Company shall determine the risk of money laundering and terrorism financing associated with the customer relationship (the customer's risk profile). The customer's risk profile shall be determined on the basis of the general risk assessment and the Company's knowledge of the customer. The customer's risk profile is monitored and revised as needed.

Know Your Customer (KYC)

The Companies shall not establish or maintain a business relationship or execute an individual transaction unless they have an effective KYC process to manage the risk of money laundering and terrorism financing as well as to monitor and assess the customer's activities and transactions.

If a customer is considered a high risk or very high risk of money laundering or terrorism financing, more stringent KYC measures shall be taken. These measures shall be more extensive than those normally taken and designed to mitigate the elevated risk.

Each Company shall monitor on an ongoing basis and as needed current customer relationships to ensure that KYC is up-to-date and sufficient to manage and assess the risk of money laundering or terrorism financing associated with the customer. This process is risk-based and conducted on an ongoing basis and when the risk associated with the business relationship changes, e.g. when the customer expands their product engagement.

Authorised decision-maker

Each Company shall appoint an authorised decision-maker for customers established in high-risk third countries, correspondent banking relationships and politically exposed persons. The authorised decision-maker shall be appointed from among the members of the Board of Directors, the CEO or other decision-makers with sufficient knowledge of the Company's risk exposure to money laundering and terrorism financing and with sufficient authority to make decisions that impact the risk exposure.

Monitoring and reporting

Each Company shall monitor ongoing business relationships and assess individual transactions in order to detect activities and transactions that deviate from what the Company has reason to expect based on the risks identified in the general risk assessment and what the Company knows about its customers, products and services. The Company shall also monitor in order to detect activities and transactions that while not unusual can be assumed to be part of money laundering or terrorism financing. If there is still a suspicion that an activity or a transaction may constitute money laundering or terrorism financing after a review, it must be reported to the Swedish Police.

Training

Each Company shall have a training plan for all employees and contractors who receive AML/CTF training on an ongoing basis. The training shall at a minimum cover the relevant aspects of current regulations, the general risk assessment, procedures and guidelines.

Suitability assessment

Each Company shall ensure the suitability of employees, contractors and others who for similar reasons participate in the business and perform tasks of importance to preventing money laundering or terrorism financing.

Information sharing within the Group

In certain cases information has to be shared between the Companies. The information that can be shared must be important to the particular Company and its ability to detect, mitigate or prevent money laundering and terrorism financing. According to the Anti-Money Laundering Act, information on suspected money laundering and terrorism financing can be shared with affected companies.

Shared information

Information on a natural or legal person that has been reported to the Swedish Police shall be shared by the Companies. The information shall include which natural or legal person has been reported and the Company that reported it. When the documentation used in a report is destroyed, i.e. deleted, the information that a person has been reported may according to current rules no longer shared by the Companies.

Complementary information

In certain cases, the Company may also need information on why a natural or legal person has been reported to the Swedish Police. This includes information on a suspected transaction or activity in order to determine whether a natural or legal person who has been reported by a Company may still establish a customer relationship with another Company.

Information on reported natural and legal persons is subject to the laws on bank secrecy. According to the Anti-Money Laundering Act, companies within a group are violating these bank secrecy laws when they share reported information. The information may not be disclosed more than necessary. If a Company needs complementary information on a report and its content, only a limited number of persons may request it. These roles are defined in each Company's guidelines.

Processing of personal data

Each Company has adopted a Group-wide *Personal data processing policy* as well as a company-specific *Instruction on the processing of personal data*. These policy documents shall cover at a minimum the processing of personal data and information sharing within the Group with respect to suspected money laundering and terrorism financing and other relevant information.

Retention of documentation

The Companies shall have procedures for retaining documentation on measures that have been taken to gather KYC, review unusual or suspicious activities or transactions, and comply with current regulations. The Companies shall also ensure that the documentation and information are easy to access and identify.

Reporting

Each Company shall inform its Board of Directors at least once a year which risks of being exploited for money laundering and terrorism financing purposes have been identified and what measures have been taken to reduce the risks. This means that the CFA shall report at least once a year to the Company's Board of Directors and the CEO and that the SAE shall report at least once a year to the Company's Board of Directors and the CEO. Moreover, the Companies shall periodically report to the SFSA.

Compliance

The CEO and every employee in a management position is responsible for complying with this policy document. The CEO is ultimately responsible for ensuring that the Company has self-assessments and procedures that guarantee good internal control. Employees, contractors and others who for similar reasons participate in the business and perform tasks of importance to preventing money laundering or terrorism financing shall be made aware of the content of the policy and comply with it.