Policy on anti-money laundering and counter-terrorism financing

January 2025

This policy is published in Swedish and English. In the event of any differences between the English version and the Swedish original, the Swedish version shall prevail.

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 consolidated 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, strong costumer protection and a reduced risk of negative impact on Avanza's brand.

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 implementation

The CEO of each company shall inform every employee in a managerial position of the provisions of this policy and is responsible for its incorporation into the operations.

Definitions

Money laundering refers to actions concerning money or other property derived from crime or a criminal activity that;

- can conceal the property's connection to crime or criminal activity,
- can promote the ability for someone to benefit from the property or its value,

- can promote the ability for someone to evade legal consequences, or
- involves someone acquiring, possessing, claiming a right to or using the property.

Actions that typically are intended to conceal that someone intends to enrich themselves or another through future criminal acts are also included in the concept.

Terrorism financing refers to the collection, provision or receipt of money or other property intended to be used, or with knowledge that it is intended to be used, to commit particularly serious crimes or to be used by a person or group of people who commit particularly serious crimes or are found guilty of attempts, preparations, conspiracy or complicity in such crimes. Collecting, providing or receiving money or other property with intent intended to be used or with knowledge that it is intended to be used for so-called terrorist trip is also terrorism financing.

Sanctions refer to limits on the freedom to act for a state, a group or a 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, among other things, freezing of 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 and appropriate measures tailored to Avanza's identified risks, in order to prevent Avanza from being used for money laundering and terrorism financing purposes. The Board of Directors of each Company shall for this purpose establish a strategic plan that is reviewed and updated annually or as necessary.

Internal control

The Board of Directors and the CEO are ultimately responsible for ensuring that the business takes necessary measures against 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 in the business.

Independent audit function

An independent audit function (IAF) is included in the internal audit function. The IAF is responsible for reviewing and regularly evaluating the Companies' internal policies, controls and procedures aimed at ensuring that the Companies fulfill their obligations under the Money Laundering Act and regulations. The IAF shall further review and regularly evaluate other control functions and submit and follow up on recommendations made to the operations.

Central Function Responsible

The Board of Directors has appointed the Chief Compliance Officer (CCO) as the Group's appointed officer for controlling and reporting obligations (CFA). CFA is responsible for monitoring and continuously controlling that the Companies comply with the requirements set out in the money laundering regulations. CFA shall also check and assess whether the Companies' internal and common procedures and guidelines are effective and appropriate. In the event of observations, CFA shall provide recommendations for remediation to

the business. Furthermore, CFA is also responsible for monitoring developments in the money laundering regulations and providing advice and support to employees and informing and educating relevant persons about rules concerning money laundering and terrorist financing. Additionally, the CFA is responsible for reporting to the Financial Police regarding deviating transactions and activities.

Specially appointed executive

Each Company shall assess whether it should appoint a specially appointed executive (SAE). If a decision is made not to appoint a SAE, a thorough justification for the decision must be prepared and documented. The decision shall be reviewed annually or upon change in the business. The responsibilities, authorities and tasks 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, authorities and tasks that otherwise would be the responsibility by the SAE.

The Board of Directors assigns the SAE the responsibility for conducting and updating a general risk assessment of how the Company's products and services can be used for money laundering or terrorism financing purposes and the likelihood of it occurring. The SAE is also assigned the responsibility to establish and update a Group policy, procedures and guidelines, and assure that the Company as a whole implements the measures and controls (first line) outlined in this policy. Moreover, the SAE shall compile periodic reporting for the SFSA. The SAE shall report at least anually to the Board of Directors and the CEO.

General risk assessment

Each Company shall have a process for establishing a business-adapted general risk assessment of the risk of the Company being used for money laundering or terrorism financing purposes. There shall be procedures for establishing, evaluating and updating the general risk assessment.

The Company's SAE, or if one has not been appointed the Company's CEO, is responsible for conducting a general risk assessment at least annually or more frequently upon changes in the business. The general risk assessment shall be designed to form the basis for the Company's procedures, guidelines and other measures against money laundering and terrorism financing.

Internal procedures

Each Company's board of directors shall annually establish guidelines and each Company's CEO shall establish an instruction that complement this policy.

Moreover, each Company shall develop procedures with scope and content 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 changed risks for money laundering and terrorist financing. The procedures shall cover the following areas:

- Implementation, evaluation and follow-up of the general risk assessment
- Implementation of initial and ongoing Know-Your-Customer (KYC) monitoring and risk assessment
- Monitoring of transactions that can be assumed to be part of money laundering or terrorism financing
- Reporting to the Swedish Police Authority
- Handling of financial sanctions including freezing and reporting accounts and amounts to the Swedish FSA.

- Retention of documents or actions taken for KYC purposes and which have been taken during the review of suspicious transactions
- Training of employees in matters concerning money laundering and terrorism financing
- Suitability assessment of employees
- Protection for employees from threats, retaliation or other hostile actions and reprisals
- If the Companies use models for risk assessment, risk classification, monitoring or other procedures, there shall be procedures in place for model risk management.
- In cases where the company has outsourced measures against money laundering or terrorist financing, there shall be procedures for outsourcing operations.

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 previously already adopted a Group-wide *Instruction on Whistleblowing (Sw Instruktion om visselblåsning)* and a *Code of Conduct (Sw Uppförandekod)*. Furthermore, the Companies have adopted Guidelines on *Conflict of interests* (Sw *Riktlinjer om intressekonflikter*) as well as Guideline on *Customer complaint handling (Sw Riktlinjer om kundklagomålshantering)*, which shall also apply to the application of money laundering regulations.

Risk assessment of customers

Each Company shall assess 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 based on the general risk assessment and the Company's knowledge of the customer. The customer's risk profile shall be followed up and changed when there is reason to do so. The customer's risk should form the basis for the controls and follow-up to be conducted on the customer and how often the follow-up should be concluded.

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 the customer is assessed as posing a high risk or very high risk of money laundering or terrorism financing, enhanced KYC measures shall be taken. These measures shall be more extensive than those normally taken and aims to mitigate the increased risk.

Each Company shall continuously and as needed follow up ongoing customer relationships to ensure that KYC is up-to-date and sufficient to manage the assessed 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 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 Authority.

Training

Each Company shall have a training plan for all employees and contractors in regards to AML/CTF training. The training shall at least 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 participate in the business on a similar basis if they perform tasks of significance to prevent the business from being used for money laundering or terrorism financing.

Information sharing within the Group and message ban

In certain cases there is a need to share information 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 Money Laundering Act, information on suspected money laundering and terrorism financing can be shared with affected Companies.

Information on reported natural and legal persons is subject to the laws on bank secrecy. This rule, that information about reported customers may not be shared with unauthorized persons, is called prohibition of disclosure and violations of this prohibition can lead to personal criminal liability. Companies are allowed to break the prohibition of disclosure obligation when exchanging information about these customers. If a Company needs additional information about a report and its contents, only a limited number of roles should be able to request access to the information. The specific roles authorised to do so should be outlined in each company's guidelines.

Information to be shared

Information that a natural or legal person has been reported to the Financial Police shall be shared by the Companies. The information shall indicate which natural or legal person has been reported and the Company that reported it. When the records for a report are deleted, i.e. erased, according to current regulations, the Information that a person has been reported shall no longer be shared between the Companies.

Complementary information

In certain cases, the Company may also need to share information about why a natural or legal person has been reported to the Financial Police. This may include information about a suspected transaction or activity

in order to determine whether a natural or legal person who has been reported by a Company should still be allowed to establish a customer relationship with another Company.

Processing of personal data

Each Company has adopted a Group-wide *Personal data processing policy (Sw Policy om behandling av personuppgifter)* as well as a company-specific *Instruction on the processing of personal data (Sw Instruktion för behandling av personuppgifter)*. These policy documents shall cover at a minimum the processing of personal data, rules for information sharing within the Group with respect to suspected money laundering and terrorism financing, for how long data may be stored and other relevant information.

Retention of documentation

The Companies shall have procedures for retaining documents concerning actions taken to obtain 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.

Prohibition of shell companies, mailbox banks, and anonymous services

No company may establish or maintain relationships with shell companies or mailbox banks and must ensure that such relationships are not established or maintained by other credit institutions with which the Companies collaborate. This must be verified when entering into the agreement within each Company. There is also a prohibition against anonymous accounts, passbooks, or safe deposit boxes.

Reporting

Each Company shall at least annually inform its Board of Directors about the risks of being used for money laundering and terrorism financing purposes identified in the business and the measures taken to reduce the risks. This means that the CFA shall report at least annually to the Company's Board of Directors and the CEO and that the SAE shall report at least annually 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 managerial position are responsible for ensuring that this governing document is followed. The CEO is ultimately responsible for ensuring that the Company has self-assessments and procedures in the business that ensure good internal control. Employees, contractors and others who for similar reasons participate in the business and perform tasks of significance to prevent the business from being used for money laundering or terrorism financing shall be made aware of the content of this policy and comply with it.