

POLICY ON MEASURES AGAINST FINANCIAL CRIME

adopted by the Central Board on 25 March 2026

Information class: Open

Responsible owner: Handelsbanken Compliance (CQ)

The policy must be applied throughout the Handelsbanken Group, including to subsidiaries, where applicable, unless binding regulations outside Sweden, or relating to subsidiaries, make deviations necessary. Acceptance and backing for such deviations must be gained from the unit responsible at Group level.

1. Introduction

This policy is based on applicable regulations concerning money laundering, terrorist financing, established international sanctions, including regulations on breaches of such sanctions, as well as regulations regarding obligations to combat fraud. Money laundering, terrorist financing, breaches of international sanctions, fraud, tax crimes and corruption are collectively referred to as financial crime.

The work to counter and combat financial crime is of fundamental significance for secure and sound banking operations. Deficiencies in the handling of these matters may affect the Handelsbanken Group's capacity to continue operating, lead to sanctions, other financial losses, and reduced confidence in the business.

2. Risk tolerance

Handelsbanken has a low tolerance for the risk of the exploitation of the Bank in any form of financial crime, and must therefore strive to ensure all risks are assessed as low.

The low risk tolerance implies, among other things, that the Bank must not participate in transactions if its employees do not understand the implications, or in transactions which could be suspected of being linked to criminal activities. This includes, for example, not holding anonymous accounts or issuing anonymous passbooks, or engaging in correspondence with shell banks or institutions that allow their accounts to be used by such banks.

The Chief Executive Officer shall also issue guidelines for further guidance on how the low risk tolerance is to be put into practice in the business operations, including requirements regarding action plans, follow-up and limits.

3. Working methods

3.1 General principles

Applying a risk-based approach, at least annually and otherwise whenever necessary, the business must continuously monitor and analyse how potential criminal activities could conceivably affect the operations, and promptly establish measures to manage any identified risks. Procedures, controls and processes must be adapted to best address the risks.

Particular attention must be paid to the segments, business areas and situations considered high risk according to risk assessments. For example, the Bank may not offer new or changed products or services, carry out reorganisations or operational changes, or contract external suppliers before ensuring that measures are in place to manage identified risks in accordance with the Bank's risk tolerance.

Work must be undertaken with the application of reliable standards and methods to combat financial crime.

3.2 Specific provisions on money laundering and terrorist financing

The work to prevent money laundering and terrorist financing shall be carried out with a risk-based approach whereby the measures are adapted to take into account the risk that the business operations may be used for these purposes. A general risk assessment which must therefore be carried out at least annually in all countries in which the Bank and its subsidiaries to which the regulations apply operate. The assessment must include relevant risk indicators linked to the products and services provided, which customers and distribution channels exist, geographical exposure and other relevant internal and external information in the area. The results of all risk assessments are then aggregated and weighted at Group level.

It is of fundamental importance to have good knowledge of the customer, and an understanding of the customer's business operations, as well as the purpose and nature of the business relationship, and maintaining this knowledge for the full duration of the customer relationship. Customers are to be assigned a risk class on the basis of the general risk assessment and risk-based activities. The Bank must continuously monitor ongoing business relationships and assess individual transactions, as well as ensuring that activities and transactions are in line with the Bank's knowledge of the customer. Suspicious activities must be reported to the relevant competent authority without delay.

3.3 Specific provisions on international sanctions

Handelsbanken must monitor and comply with regulations pertaining to international sanctions in accordance with decisions by the EU, the Swedish Act on Certain International Sanctions and other relevant sanctions programmes. A general sanction risk assessment must be carried out at least annually in all countries in which the Bank and its subsidiaries to which the sanctions regulations apply operate, for the purpose of identifying the risk that the business could violate or otherwise be affected by sanctions regulations. The assessment must include relevant risk indicators linked to the products and services provided, which customers and distribution channels exist, geographical exposure and other relevant internal and external information in the area. The results of all risk assessments are then aggregated and weighted at Group level.

Measures to prevent breaches of international sanctions must be based on the customer's assessed sanctions risk. An assessment is made, on the basis of the information collected, about whether the customer, the customer's business or geographical base are subject to sanctions, as well as through sanction-specific screening of customers and incoming and

outgoing cross-border transactions. The Bank must not enter into a business relationship or execute a transaction if the risk of a sanction breach cannot be adequately assessed and managed.

3.4 Specific provisions on fraud

Fraud against customers covers all illegitimate actions whereby a customer's identity, account information or digital access methods are used illicitly to execute unauthorised transactions. This includes situations where customers have been misled into executing transactions themselves. There are also cases of fraud aimed directly at the Bank's operations.

The Bank shall apply a risk-based approach as regards the prevention, discovery and management of fraud. This entails regular risk assessments, continuous staff training, transaction monitoring and other systematic controls to identify deviations. Any matter that raises suspicion must be investigated promptly. Procedures and controls must be evaluated on an ongoing basis to ensure that fraud protection is effective and robust.

3.5 Other internal procedures to combat financial crime

The work to prevent employees or other contractors from exposing customers or Handelsbanken to fraud, or to prevent employees and contractors from being accessories to customers' crimes in the areas of money laundering, terrorist financing, tax crimes and corruption, shall include training activities, internal control measures, suitability assessments when hiring and at regular intervals during the employment, use of the four-eyes principle in important decision-making processes, and other appropriate measures. Employees and other contractors must have access to a whistleblower function to report irregularities.

4. Organisation

4.1 The Head of HO and specially appointed executive

The Head of Handelsbanken Operations (HO) is the *specially appointed executive* for the parent company. An equivalent executive is also to be appointed for subsidiaries if deemed appropriate or required by external regulations. The specially appointed executive is tasked with ensuring and following up that the Handelsbanken Group works in accordance with external and internal regulations concerning anti-money laundering and terrorist financing. This includes measures to prevent customers from using the Group for money laundering that relates to or derives from, for example, tax crimes, corruption, fraud or other relevant predicate offences.

The Head of HO is also responsible for ensuring and following up that the Handelsbanken Group works in accordance with external and internal regulations concerning compliance with international sanctions. The responsibility includes making decisions to freeze funds as a result of international sanctions.

In addition, the Head of HO is responsible for the Bank's work to tackle fraud, tax crimes and corruption.

Country General Managers must, where deemed necessary, appoint a person with specific responsibility for matters relating to measures designed to prevent money laundering and terrorist financing, including responsibility for implementing the measures required to comply with external and internal rules within the area. The same applies for compliance with international sanctions in the operations.

4.2 Head of CQ, appointed officer for controlling and reporting obligations, and senior officer

The appointed officer for controlling and reporting obligations and the senior officer for compliance with international sanctions, respectively, is the Head of Handelsbanken Compliance (CQ), or the person appointed by the Head of CQ. The Chief Executive Officer may also decide that the responsibilities shall also encompass subsidiaries.

The appointed officer for controlling and reporting obligations and senior officer is tasked with monitoring and regularly verifying that the Handelsbanken Group fulfils its obligations in accordance with external regulations concerning anti-money laundering and terrorist financing, and compliance with international sanctions. This includes developing the Group-wide internal rules specifying measures to be taken in the area and following up the implementation of these rules across the Group, providing advice and support to and informing and training the relevant staff about the rules.

5. Reporting and information to public authorities, etc.

In Sweden, including for Swedish subsidiaries that undertake licensed operations, the appointed officer for controlling and reporting obligations must ensure that information regarding suspected money laundering, terrorist financing or property that might otherwise be derived from criminal activity is submitted promptly to the police authority. Where applicable, the senior officer shall report violations of international sanctions to the relevant authorities.

Branches and subsidiaries outside Sweden must ensure that information regarding suspected money laundering and terrorist financing are submitted to a competent authority, and that decisions made on the freezing of funds as a result of international sanctions are submitted to a competent authority within the country. Reports of suspected cases of money laundering, terrorist financing or other financial crime to a competent authority that are deemed by the local manager to be of particular significance, must be reported to the specially appointed executive for the parent company (Head of HO), provided that this is permitted by the legislation and regulatory requirements of the country concerned.

The appointed officer for controlling and reporting obligations, the senior officer and the Head of CQ must submit a quarterly report to the Chief Executive Officer, the risk committee and the Central Board addressing risks associated with non-compliance as far as these relate to money laundering and terrorist financing, as well as international sanctions.

In addition, the appointed officer for controlling and reporting obligations, the senior officer and the Head of CQ must ensure that the Chief Executive Officer, the risk committee and the Central Board are informed on other occasions when this is deemed appropriate.