

Policy for Anti-Money Laundering and Financing of Terrorism

1 Summary

SpareBank 1 Nord-Norge (SNN) shall actively work to prevent, uncover and report transactions linked to proceeds of criminal acts or connected with acts of terrorism.

On the basis of the current legislation, expectations from customers and other external stakeholders, business mapping and risk analyses, preventive measures shall be prepared and implemented.

We shall have good knowledge of our customers and monitor transactions in order to identify any suspicious activities. Regular evaluation and learning will help maintain a high level of management and control of this area.

2 Background, Objective and Scope

Financial crime, including money laundering, undermines the integrity of the economic system in any society. The financial industry has a special role in society and our infrastructure can be used as a tool for criminal acts.

Norway is a member of the Financial Action Task Force (FATF). This is an organisation whose mission is to set standards and promote effective implementation of regulatory and operational measures for combating money laundering, terrorism financing, financing of mass destruction weapons and other related threats to the integrity of the international economic system. FATF's standards are implemented through EU Directives and in Norwegian law.

This policy shall help SpareBank 1 Nord-Norge take an active role in combating money laundering and financing of terrorism. The policy complies with the requirements set out in Section 8 of the Money Laundering Act and applies to the SpareBank 1 Nord-Norge Group.

Corruption, bribery and tax evasion inhibit economic growth in a country and deprive people of the right to basic social benefits. Through our anti-money laundering efforts, we also contribute to realising sustainability goal 16 for peace and justice, sub-goal 16.5.

4 Roles and Responsibilities

4.1 Board of Directors

The Board of Directors is responsible for determining the Group's policy on money laundering and financing of terrorism, cf. Section 8 (4) of the Money Laundering Act. The Board of Directors shall be presented with and approve the Group's risk analysis for money laundering and financing of terrorism in connection with the processing of the policy.

4.2 User Responsibility

All managers of SNN have a responsibility to ensure that the business activities are carried out in accordance with applicable laws and regulations and that this can be documented. This also means that managers are responsible for ensuring that employees have adequate knowledge of laws and regulations, that mandatory training is carried out and that the day-to-day business activities reflect this.

All employees of SNN are responsible for ensuring that day-to-day operations are carried out in accordance with the applicable laws and regulations. This means that employees are responsible for complying with laws and regulations, including procedures and guidelines, while performing their duties.

Entities in the relevant company with responsibility for business processes, products and services shall ensure that customer establishment and follow-up of the customer relationship is done in accordance with the regulations and this policy, and that procedures are prepared for this.

Violations of the regulations shall be recorded in the event database as compliance violations.

4.3 Money Laundering Manager

4.3.1 Group Money Laundering Manager

The function of Group Money Laundering Manager has been assigned to the Head of Compliance.

The Group Money Laundering Manager is the premise provider for the Group's compliance with external laws and regulations concerning anti-money laundering and financing of terrorism. This means overall responsibility for competence and advisory services, roles, functions and lines of responsibility.

The Group Money Laundering Manager shall carry out risk analyses for the Group in this area, including preparing general management documents and proposing risk-reducing measures. This person is also the Head of the Group's AML Forum.

The Group Money Laundering Manager shall be presented with all new, or significant changes to products, services, processes and technology for risk assessment. Similarly, the Money Laundering Manager shall be informed of any discrepancies, or changes in roles, functions and responsibilities that affect compliance with this policy.

The Group Money Laundering Manager is responsible for the monitoring of transactions in the bank, including the preparation of guidelines for this and quality follow-up. This also includes responsibility for reporting to the Norwegian National Authority for Investigation and Prosecution of Economic and Environmental Crime (*Norw. Økokrim*) regarding suspicious transactions.

The Group Money Laundering Manager can delegate operational duties which the function has the responsibility for.

4.3.2 Money Laundering Manager Subsidiaries subject to Reporting

The function of Money Laundering Manager of subsidiaries subject to reporting is appointed by the Board of the relevant company. The Board also determines its own instructions for this, in accordance with the responsibility of the regulations and this policy, The Money Laundering Manager is responsible for the company's compliance with external laws and regulations concerning anti-money laundering and financing of terrorism. This means responsibility for competence and advisory services, roles, functions and lines of responsibility.

The Money Laundering Manager shall carry out risk analyses for the company in this area, including preparing general management documents and proposing risk-reducing measures. The Money Laundering Manager is also responsible for reporting in this area internally in the company and to the Group Money Laundering Manager, as well as participation in the Group's AML Forum.

The Money Laundering Manager shall be presented with all new, or significant changes to products, services, processes and technology for risk assessment. Similarly, the Money Laundering Manager shall be informed of any discrepancies, or changes in roles, functions and responsibilities that affect compliance with this policy.

The Money Laundering Manager is responsible for the monitoring of transactions in the company, including the preparation of guidelines for this and quality follow-up. This also includes responsibility for reporting to the Norwegian National Authority for Investigation and Prosecution of Economic and Environmental Crime regarding suspicious transactions.

4.4 Forum for AML

Forum AML is a corporate governing body working with SpareBank 1 Nord-Norge's compliance with anti-money laundering and financing of terrorism regulations, as well as international sanctions.

The forum is an advisory body consisting of money laundering managers in the companies of the Group subject to reporting and others with delegated duties in this area. The forum is headed by the Group Money Laundering Manager.

The mandate for the work in the forum is prepared by the Group Money Laundering Manager.

4.5 Internal Audit

Internal Audit is an independent, objective verification and advisory function that assists the Board and the Group CEO with the fulfilment of their responsibilities related to governance, risk and capital management and internal control. Internal Audit shall evaluate and improve the effectiveness and appropriateness of the Group's governance, risk and capital management and internal control, as well as provide feedback on compliance with applicable laws and regulations, internal guidelines and established control measures in critical areas.

Internal Audit shall carry out regular inspections of the Group's work related to anti-money laundering and financing of terrorism and in particular of the bank's electronic transaction monitoring and the Group's overall management documents.

4.6 HR

HR is responsible for preparing training material, as well as the implementation and documentation of training activities in the subject area.

5 Principles for Governance and Control of Money Laundering and Financing of Terrorism

5.1 Prevention of Money Laundering and Financing of Terrorism

SNN shall comply with the legal requirements and implement measures that are aimed at combating financial crime and acts of terrorism.

SNN shall work actively to prevent, uncover and report transactions related to the proceeds of crime or linked to terrorism.

5.2 Risk-Based Approach

The work on money laundering and financing of terrorism must be based on a risk-based approach. An annual risk assessment shall be prepared both for the Group as a whole and for each company, and this shall be based on a national risk assessment from the Ministry of Justice and Public Security, the Financial Supervisory Authority of Norway's risk assessment and other national and international relevant sources.

The risk assessment shall identify the need for risk-reducing measures, which in turn shall form the basis for the work in this area and the preparation of operational procedures. The risk assessment shall as a minimum include assessments of:

- the scope and nature of the activities, including details of the turnover and the number of customers for the various services and products,
- types of customers, including the purpose and intended nature of the customer relationship, as well as the duration,
- all products with exposure to money laundering and/or financing of terrorism,
- transactions,
- geographical exposure in relation to all of the above areas.

5.3 Know your Customer Principle

SpareBank 1 Nord-Norge shall in its processes seek to counteract anonymity and strive for transparency with the aim of preventing money laundering and financing of terrorism. This shall be done

by:

1. Verifying the customer's identity

The customer's identity shall be verified when any form of customer relationship is established, i.e. even if the customer only uses one service, product or single transaction. The requirements for documented identification shall be determined based on the inherent risk of the service/product/transaction.

2. Knowing the purpose and intended nature of the customer relationship

Before a customer relationship can be established the customer shall answer questions that are intended to uncover the customer's identity and the purpose and intended nature of the customer relationship.

3. Identifying and registering real beneficial owners and politically exposed persons (PEP)

All customers shall answer questions about real beneficial owners and politically exposed persons. In the event of elevated risk and complex ownership structures, further investigations shall be carried out to verify the information obtained, including documenting these.

4. Determining the risk level of the customer

A risk level shall be determined for all customers on the basis of a risk calculation based on information about i.a. the purpose of the customer relationship, the usage pattern for products/services/transactions, the type of customer and owners.

5. Registering and storing information about the customer and the customer relationship

All activities related to customer control shall be documented and be searchable in each company's customer systems.

5.4 Control Mechanisms

5.4.1 Customer Measures

Customer measures shall as a general rule be implemented prior to the establishment of the customer relationship or at the latest before agreements and transactions are adopted / implemented.

Verification of the customer's identity shall as a general rule only be made in person. Special procedures shall be established for customer measures in all companies and for all product and service areas and cannot the customer cannot attend in person, special measures shall be established to confirm the customer's identity.

Both when the customer is a natural person and a legal entity, it shall be determined whether there are real beneficial owners in addition to the customer.

If the customer measures cannot be implemented, no customer relationship shall be established. If continuous customer measures cannot be implemented, the customer relationship shall as a general rule be terminated or blocked in accordance with established guidelines.

5.4.2 Level of Customer Measures and Enhanced Control

The customer measures must be adapted to the business and the information that is available about the customer. Different levels of control shall be implemented based on the customer's risk classification. Special procedures and criteria shall be established for the different risk categories and this shall be based on the at any given time applicable risk assessment.

If the customer is identified as an elevated level of risk, enhanced control shall be put into effect and appropriate measures shall be taken to verify the information presented. This includes the following items, if relevant:

- More details about the nature and purpose of the customer relationship,
- Documentation for the origin of the funds and/or assets,
- Documentation of key figures, including turnover,

- Documentation of business associates
- Documentation that verifies the identity of real beneficial owners,
- Justification for a complex company structure
- Documentation relating to ties with Norway and the need for account conditions, if the customer is not resident here

Customers who are Politically Exposed Persons (PEP) shall always be deemed to have elevated risk levels and shall have enhanced customer measures. The same applies if a PEP has roles or is the Real Beneficial Owner (RBO) of a legal entity.

If an elevated level of risk has been identified for the customer, the establishment of the customer relationship shall be approved by a manager with special authority to do so. The origin of the assets or funds shall always be documented. A specific assessment shall be made of whether the documentation obtained in connection with enhanced customer measures can be deemed to be sufficient and whether the customer can be offered all products/services. This assessment shall be documented.

5.4.3 Continuous Customer Measures

SpareBank 1 Nord-Norge shall implement continuous customer measures for established customer relationships.

Information about customers and customer relationships shall be updated continuously against public sources and be supplemented when necessary in connection with regular customer contacts (updating of customer information and information about the customer relationship).

Information about the customer and the customer relationship shall be collected regularly. When there is an elevated risk level, the customer shall be questioned annually. For other customers, procedures shall be drawn up for regular questioning in accordance with the current risk.

When selling additional products or services in previously established customer relationships, the customer information shall be reassessed and updated, if necessary.

All customers shall be subjected to regular monitoring in order to detect any suspicious transactions, either manually or electronically. Special procedures shall be prepared for electronic monitoring systems and their use shall be evaluated and documented regularly. In the event of interruptions in the automatic controls, measures must be taken to detect suspicious transactions, such as checks against transaction records in the Group's data warehouse.

5.4.4 Customer Measures Distributors and Agents

Even if the customer control is performed by agents/distributors, SpareBank 1 North-Norge is responsible for the control. When this is the case, there shall be an underlying distribution agreement and/or other relevant governing documents that demand quality in the customer control.

5.4.5 Customer Measures Correspondent and Respondent Bank Connections

When entering into correspondent and respondent banking agreements, a specific risk assessment and due diligence investigation shall be carried out. Special procedures shall be established for this.

Such agreements shall not be established with empty banking companies, or with banks in defined high-risk countries, and sufficient investigations shall be carried out to ensure this.

As a general rule, no agreement shall be entered into with an institution from a state outside the EEA as a respondent institution. If this is done, the following requirements must be met:

- Sufficient information about the respondent institution shall be collected to understand the nature and reputation of the business and the quality of the supervision
- The respondent institution's measures against anti-money laundering and financing of terrorism shall be assessed
- Approval must be obtained from the CFO before establishment
- When establishing settlement accounts, we shall ensure that the respondent institution has verified the identity of and conducts ongoing follow-up of customers who have direct access to accounts with the correspondent institution and on request can provide relevant information from the customer measures and the continuous follow-up to the correspondent institution.

5.4.6 Screening against Sanctions Lists, Orders to Freeze Assets and Earmarking

SpareBank 1 Nord-Norge shall comply with orders to freeze assets and earmarking from national and international authorities. Customers and transactions should be screened on an ongoing basis against sanctions lists. The responsibility for the freezing of funds and reporting belongs to the Group Money Laundering Manager or those authorised by him/her.

5.5 Rejection of Customers, Blocking and Discontinuation of Customer Relationships

If the customer does not contribute to the implementation of customer measures, including any required enhanced customer measures, the customer relationship shall not be established. Similarly, the customer relationship shall as a general rule be discontinued or blocked if the customer does not contribute to the implementation of customer measures in an ongoing customer relationship.

5.6 Investigation and Reporting

If circumstances are uncovered that may indicate that funds are associated with money laundering or financing of terrorism, investigations shall be conducted. Investigations shall always be conducted if circumstances are uncovered that differ from our knowledge of the customer and the purpose and intended nature of the customer relationship.

The following circumstances and transactions shall also always be investigated:

- The transaction seems to lack a legitimate purpose.
- The transaction is exceptionally large or complex.
- The transaction is unusual based on the customer's known commercial or personal patterns of transactions.
- The transaction is made to or from a person in a country or region that does not have satisfactory anti-money laundering and financing of terrorism measures.
- A transaction that otherwise has an unusual character.

If the investigations do not disprove the suspicion, the matter shall be reported to the Norwegian National Authority for Investigation and Prosecution of Economic and Environmental Crime without undue delay.

As a general rule, the transaction shall not be made before the Norwegian National Authority for Investigation and Prosecution of Economic and Environmental Crime has been notified. If it is impossible to stop the transaction, or if stopping the transaction can complicate investigations of a person who may benefit from a suspicious transaction, the Norwegian National Authority for Investigation and Prosecution of Economic and Environmental Crime shall be notified immediately after the transaction has been completed.

6 Competence and Training

The Board of Directors, the management and all employees of the Group shall as a minimum every two years complete e-learning with certification in this area. If special circumstances indicate that the knowledge should be updated more frequently, additional training must be undertaken.

The subject area shall also be part of the curriculum in all authorisation schemes for specific professional positions. All new employees must complete an individual training programme and e-learning with certification.

The training requirements also apply to temporary manpower (substitutes, student teachers, etc.).

7 Reporting

Status and development in the area of money laundering and financing of terrorism shall be reported quarterly to the management and the board of directors of the separate companies subject to reporting in the Group. The reporting at the Group level shall be included in the compliance reporting, and include the status of all companies.

At the end of each quarter, the Money Laundering Manager of the subsidiaries and the Operational Money Laundering Manager shall report the status of controls and any discrepancies to the Group Money Laundering Manager.

Annually as a minimum, the management and the board of directors shall receive a summary report in this area in connection with the updating of the money laundering and financing of terrorism risk analyses, the money laundering and financing of terrorism annual cycle and/or a revision of other governing documents in this area.

Operational interruptions or errors resulting in a significant reduction in functionality of the bank's and the finance company's electronic monitoring system, shall be reported to the Financial Supervisory Authority of Norway without undue delay.

8 Disclosure of Group Information

The compliance department is the Group's centralised function for information sharing, cf. Section 6-5 of the Money Laundering Regulations.