

Document owner:	Approved by:	Version:	Date of approval:
GMLRO - GLENN SÆTHER	MANAGEMENT AND BOARD	1.0	30.11.2017

# SpareBank 1 SR-Bank ASA Anti Money Laundering (AML/CTF) and Sanctions Policy

## Revision history:

Date	Version	Description of content	Author	Approved
14/11/2017	1.0	Version for approval by Management and Board	Inglen Haugland	Management and Board

This Policy is updated based on findings from risk analysis conducted during spring 2017 and is valid from the date of approval.

## 1. GROUP AML POLICY STATEMENT

The term policy refers to a governing document that describes the overall principles and guidelines, including authority, roles and responsibilities associated with the area in which the policy applies.

### 1.1 Statement

It is the policy of SpareBank 1 SR-Bank to prohibit, and actively prevent and detect money laundering and any activity that facilitates money laundering or the funding of terrorists or criminal activity. The Group has developed internal routines to detect and prevent any attempt of such financial crime and has established procedures for customer due diligence, reporting, internal control and record keeping.

All employees shall respond to suspicious transactions and suspicious circumstances, which may involve money laundering or terrorist financing.

### 1.2 Regulator

SpareBank 1 SR-Bank is regulated by the Financial Supervisory Authority of Norway, Finanstilsynet. ([www.finanstilsynet.no](http://www.finanstilsynet.no)).

### 1.3 Self Assessment

A completed Wolfsberg Group AML Questionnaire is available at <https://www.sparebank1.no/content/dam/SB1/bank/sr-bank/om-oss/Investor/virksomhetsstyring/annet/Wolfsberg%2025.04.2017.pdf>

## 2. PURPOSE

The purpose of SpareBank 1 SR-Bank's policy on anti-money laundering and terrorist financing is to provide guidelines and principles for establishing, implementing, improving and monitoring compliance,

Document owner:	Approved by:	Version:	Date of approval:
GMLRO - GLENN SÆTHER	MANAGEMENT AND BOARD	1.0	30.11.2017

as well as to clarify the roles and responsibilities associated with this work, both in terms of automated and manual routines.

This document provides an overall description of the Group's measures, including guidelines and principles that apply to the company's management and control environment, as well as how the business is organized to comply with legal requirements.

## 2.1 Scope

This policy is company-wide, meaning that it applies to all business areas and organizational units, as well as all employees and managers in SpareBank 1 SR-Bank.

## 3. DEFINITIONS

### 3.1 Roles

**Group Money Laundering Reporting Officer (GMLRO)** is the Group's Chief of AML and holds the formal responsibility for AML, CTF and Sanctions within the Group. The GMLRO is the owner of the Group's AML policy and is responsible for updating it according to the AML regulations, and implementing the policy within the organization.

**Money Laundering Reporting Officer (MLRO)** is delegated the operational and the strategic responsibility for AML from the GMLRO. The MLRO is the official responsible for monitoring and reporting suspicions related to money laundering.

### 3.2 Other definitions

**Know Your Customer (KYC)** is the process of a business identifying and verifying the identity of its clients.

**Money Laundering** is the process of transforming the profits of crime and corruption into ostensibly "legitimate" assets.

**Counter-Terrorist Financing (CTF)** refers to activities that provides financing or financial support to individual terrorists or terrorist groups.

**Beneficial owner** refers to anyone who enjoys the benefits of ownership of a security or property, and yet does not nominally own the asset itself.

**Politically Exposed Person (PEP)** is a term describing someone who has been entrusted with a prominent public function. A PEP generally presents a higher risk for potential involvement in bribery and corruption by virtue of their position and the influence that they may hold.

**Customer** means any individual or entity who seeks to enter or has already entered into a business relationship, or conducts a one-off transaction with the Company as principal or as a client agent.

Document owner:	Approved by:	Version:	Date of approval:
GMLRO - GLENN SÆTHER	MANAGEMENT AND BOARD	1.0	30.11.2017

**Employee** means an individual working at any level and grade within Companies, including (but not limited to) the board of directors, senior managers, officers and other employees (whether permanent, fixed-term or temporary).

**Money Services Business (MSB)** is a legal term used to describe businesses that transmit or convert money.

**Off-the-Shelf Company** is a company which has already been registered by an accountant or lawyer, and which is ready for sale to someone who wants to set up a new company quickly.

**Shell Company** is a non-trading company used as a vehicle for various financial maneuvers or kept dormant for future use in some other capacity.

#### 4. LEGAL AND REGULATORY FRAMEWORK

SpareBank 1 SR-Bank's AML controls are based on legal and regulatory requirements from:

- Norwegian regulations are based on the recommendations of FATF and Directive 2005/60/EC of The European Parliament and of The Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing.
- FATF Recommendations – adopted February 2012
- Norwegian laws and other directives provided by the Norwegian authorities:
  - Act no. 11 of 6 March 2009 (Money Laundering Act)
  - Regulation No. 302 of 13 March 2009 (Money Laundering Regulation)
  - Circular no. 24/2016 “Guide to new anti-money laundering legislation and combating financing of terrorism”
- Sanctions from the Norwegian Ministry of Foreign Affairs
- Guidelines issued by The Basel Committee on Banking Supervision:
  - “Sound management of risks related to money laundering and financing of terrorism”, January 2014
- Official Norwegian Report (Norges Offentlige Utredingar) NOU 2016: 27
- US Patriot Act

#### 5. SPAREBANK 1 SR-BANK'S FRAMEWORK FOR PREVENTING MONEY LAUNDERING & INTERNAL COMMUNICATIONS AND CONTROL ROUTINES

SpareBank 1 SR-Bank has developed a clear set of policies and procedures outlining its general AML and Counter-Terrorist Financing (CTF) standards and principles, which are integrated into its business processes. SpareBank 1 SR-Bank applies a risk-based approach towards assessing and managing money laundering and terrorist financing risks. All policies and policy-related documents are published internally

Document owner:	Approved by:	Version:	Date of approval:
GMLRO - GLENN SÆTHER	MANAGEMENT AND BOARD	1.0	30.11.2017

and are available to internal staff at all times. Policies and procedures are subject to an annual review cycle to ensure their conformity with AML regulations and changes in the risk landscape/analysis.

The group has established an internal whistle blowing system for circumstances related to possible failure to comply with the money laundering rules.

## 5.1 AML Roles and Responsibilities

The following roles and responsibilities are defined for employees at SpareBank 1 SR-Bank:

### 5.1.1 The Board

The board has overall responsibility for the management and organization of the AML area in the Group and to ensure accordance with applicable laws and regulations.

### 5.1.2 CEO

The CEO has overall responsibility for the AML area and reports directly to the board.

### 5.1.3 Group Money Laundering Reporting Officer (GMLRO)

Executive Vice President of Business support and development (FSU) is the Group's Chief of AML and holds the formal responsibility for AML within the organization, delegated by the board. GMLRO is the owner of the bank's AML policy and is responsible for updating it according to the AML regulations, and implementing the policy within the organization.

### 5.1.4 Money Laundering Reporting Officer (MLRO)

Executive Vice President of Business support and development (FSU) has delegated the strategic and operational responsibility for AML to the MLRO and the AML unit. The MLRO is the official responsible for monitoring and reporting suspicions related to money laundering, AML training to ensure competence as part of the group's risk culture, as well as responsibility for revising AML processes and improvement of electronic surveillance systems.

GMLRO and MLRO sets the strategic direction of the AML work within the group.

### 5.1.5 First line of defence

All managers at SpareBank 1 SR-Bank are responsible to adapt and implement the Group's AML processes. The implementation will take a risk-based approach to materiality and the effectiveness of the process shall be documented. All employees are required to adhere to the bank's internal control policies and communication routines.

### 5.1.6 Second line of defence

Compliance together with GMLRO, representing the second line of defense, evaluate, monitor, provide advice, configures, quality controls, quantifies and aggregate risk. Second line will help ensure that all relevant legal requirements are fulfilled, calibrate frameworks and processes, as well as contribute to the necessary competence building and risk culture.

Document owner:	Approved by:	Version:	Date of approval:
GMLRO - GLENN SÆTHER	MANAGEMENT AND BOARD	1.0	30.11.2017

### 5.1.7 Third line of defence

The Group's Internal Audit function, representing the third line of defense, provides independent advice and confirmation on risk management, internal audit and corporate governance, with regards to the Group's compliance to AML regulations.

## 5.2 Risk Based Approach

The AML risk analysis is subject to annual review. As part of the annual review process, the Group's will:

- 1) Identify risks
- 2) Identify risk mitigation measures
- 3) Implement risk mitigation measures
- 4) Provide adequate training
- 5) Monitor the effectiveness of risk mitigation measures preventing money laundering and terror financing.

## 5.3 Customer Due Diligence

SpareBank 1 SR-Bank will not enter into, or maintain, a business relationship with a client, unless the identity of the client and/or the Beneficial Owner is known, and the nature of business or formal requirements concerning the identification of the client and/or Beneficial Owners are fulfilled.

SpareBank 1 SR-Bank applies a risk based approach to customer due diligence and Know Your Customer (KYC) procedures, both before establishing the customer relationship, and ongoing through the client relationship, and applies enhanced due diligence for customers deemed to represent higher risk such as Politically Exposed Persons (PEPs).

The Bank applies a risk-based approach to monitoring of its transactions, customers, senders, beneficiaries, and correspondent banking relationships against the FATF list, OFAC list, and Sanctions from the Norwegian Ministry of Foreign Affairs. The Bank will request information to document the purpose of its customer's relationships and transactions, and to document the origin of its customer's funds.

## 5.4 Transaction Monitoring

All customer transactions are monitored on a daily basis. The Bank's monitoring system is designed to identify suspicious transactions based on a set of criteria defined through our risk assessment process. All customers are screened against sanctions lists (EU, OFAC, UN) on a daily basis. PEPs are screened when onboarding a customer and on a yearly basis.

Transactions and suspicious circumstances that will be prioritized in terms of investigation and reporting to local FIU (Økokrim) are:

- Transactions related to newly established customers.
- Transactions related to customers identified as high risk.
- Transactions related to terrorist financing.
- Transactions to or from tax havens.

Document owner:	Approved by:	Version:	Date of approval:
GMLRO - GLENN SÆTHER	MANAGEMENT AND BOARD	1.0	30.11.2017

- Money in transit through SpareBank 1 SR-Bank.

## 5.5 Prohibited Activities

SpareBank 1 SR-Bank will not:

- Accept assets that are known or suspected to be the proceeds of criminal activity.
- Enter into/maintain business relationships with individuals or entities known or suspected to be associated with terrorist activity, criminal organization's or members of such, or on sanction lists.
- Establish customer relations to shell banks, or customers with established customer relations to shell banks.
- Establishing customer relationships or conducting transactions with shell companies or persons or entities established with customer relationships in such.
- Enter into relationships with clients from sanctioned countries or;
- Enter into relationships with clients operating in the following industries:
  - Dealers involved in the illegal distribution of Arms and Munitions.
  - Pornography.
  - Illegal gambling.
  - Cryptocurrency.
  - Money Services Businesses (MSBs) unless partly- or fully owned by the Group.
- Process payments to its own suppliers established with trust, complicated ownership structures or in tax havens.
- Maintain business relationships with individuals or entities known or suspected to be associated with tax evasion.
- Establish customer relationships with or conduct transactions that do not support the UN Global Compact's principles (<https://www.unglobalcompact.org/what-is-gc/mission/principles>).

## 5.6 Reporting Procedures

Employees reports any suspicious transactions to the Bank's AML Officer, organized in the AML unit. Suspicious transactions are reported to Financial Investigations Unit (FIU) – The Norwegian National Authority for Investigation and Prosecution of Economic and Environmental Crime (Økokrim – [www.okokrim.no](http://www.okokrim.no)).

## 5.7 Record Keeping

All investigated and reported customer relationships and transactions are kept for a period of up to 6 years, calculated from the time of transaction execution, or from the end of the business relationship.

## 5.8 Confidentiality

Personal data is considered confidential and will not be shared with external third parties unless stipulated by applicable laws.

Document owner:	Approved by:	Version:	Date of approval:
GMLRO - GLENN SÆTHER	MANAGEMENT AND BOARD	1.0	30.11.2017

### **5.9 Training**

The Bank provides AML training programs to all staff within the organization. The training is risk based, and is adapted based on roles and responsibilities. The Group makes sure the AML training material and AML updates are available to all employees at all times.