Policy on Anti Money Laundering and Countering Terrorist Financing

Adopted by	The Board of Directors of Swedbank AB (publ.)
Date of adoption	19 June 2019 (replaces 25 May, 2018)
Applies for	the Bank and all Subsidiaries
Group Framework Owner	The Head of the Anti-Financial Crime Unit as the Specially Appointed Executive
Distribution	Group Regulation section on the intranet
Language version	English
Information class	External
Basis	- Regulation (EU) 2015/847 of the European Parliament and of the Council on information accompanying transfers of funds. - Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and applicable national law. - Swedish Act (2017:630) on Measures against Money Laundering and Terrorist Financing. - Swedish Act (2017:631) on the registration of beneficial owners. - Swedish FSA's regulation 2017:11.

1. Purpose

Swedbank AB (publ.) ("The Bank") and its subsidiaries (together referred to as "the Group" or "Swedbank") is one of the largest financial services group in the Nordic and Baltic region, providing a wide range of products and services. The size of the operations makes the Group systemically significant and it plays an important role in the local communities where the Group serves.

Money Laundering ("ML") and Terrorist Financing ("TF") activities are threats to the integrity and the stability of the international financial system. Swedbank has a responsibility to its customers, shareholders and regulators to prevent the Group from being used to facilitate the movement of criminal proceeds or transfer of funds destined to finance terrorism. The Group is committed to identifying and managing the ML/TF risks that it is exposed to and to take proportionate measures required to manage these risks across all jurisdictions in which it operates.

Therefore, the Group will apply robust and consistent Anti-Money Laundering and Counter Terrorist Financing ("AML/CTF") standards and procedures to prevent use of the services, products or channels for purposes of ML/TF in the jurisdictions in which it operates.

The Bank has established this policy on AML/CTF (the "Policy") to ensure compliance with the Group's regulatory obligations, support the broader customer strategy, maintain its good reputation and to contribute to the stability of the financial system. It provides a uniform set of high-level risk management principles and minimum requirements which must be established, maintained and operated throughout the Group to prevent, detect and take proper action against ML/TF.

Defined terms used herein shall have the meaning set out in this Policy. Other terms and definitions not provided herein shall have the meaning set out in the List of Group Common Definitions.

2. Scope and application

This Policy applies to the Group. Regulated Subsidiaries shall adopt the principles and minimum requirements as set out in this Policy. Wherever local regulations are stricter than the requirements set out in this Policy, the stricter standard shall be applied.

If any applicable regulations are in conflict with this Policy, Subsidiaries may adopt the Policy with deviations, after consulting the Specially Appointed Executive, Chief Legal Officer or Head of Group AML.. Any material deviations from the Group Policy must be reported to the Board of Directors of the Bank as well as the Group Framework Owner. This policy must be read in conjunction with any associated frameworks, including but not limited to the Group Instruction on AML/CTF and the Policy on Financial Sanctions, where more detailed requirements are outlined.

3. Roles and Responsibilities

Effective AML/CTF risk management requires proper governance and the establishment of clearly defined accountabilities and responsibilities across Swedbank's three lines of defence and senior management. The unit or person with ultimate ownership and authority for the task, making the final decision, is accountable. There can only be one unit or person accountable. The unit or person assigned to perform the activity is responsible. There can be multiple responsibilities, if the task is performed in several business areas or functions. Accountabilities and responsibilities for AML/CTF risk management must be clearly defined and documented in mandates or role/job descriptions and assigned appropriately.

3.1. Board of Directors

The Board of Directors of the Bank ("the Board") is ultimately accountable for defining and overseeing the overall implementation of the Group's principles, strategies and objectives, including appropriate control and risk management systems, to prevent ML/TF ("the Group AML/CTF Framework"). The Board must satisfy itself that the Group is and continues to be equipped with the necessary and sufficient resources (in terms of personnel and technology) to effectively manage risks identified in the Group's risk assessments and must establish a clear and consistent risk appetite across the Group. Corresponding accountability applies to the relevant[1] Board of each Subsidiary.

[1] In countries where two-tier corporate governance systems apply.

3.2. CEO

In line with the Governance Instruction, the CEO of the Bank and the CEO of each Subsidiary is accountable for the day-to-day management of the respective legal entity in accordance with the strategic directions and objectives set forth by the Board. The CEO of the Bank shall in the capacity of President of the Group also adopt accompanying group instructions and the group wide AML/CTF organisation, to mitigate and manage effectively the risks of ML and TF. The CEO of the Bank and the CEO of each Subsidiary may delegate responsibilities and tasks.

The CEO of the Bank and the CEO of each Subsidiary shall ensure that there are adequate resources in place, including personnel and technology, to secure compliance with this Policy and the accompanying framework.

3.3. Specially Appointed Executive

The CEO of the Bank and, when deemed necessary, each Subsidiary shall ensure that a Specially Appointed Executive ("SAE") at executive management level is appointed.

The Group SAE is accountable for the development and maintenance of the Group AML/CTF Framework, including risk management practices, controls and performance of ML/TF risk assessments, and for ensuring that the framework is implemented consistently throughout the Group. The Group AML/CTF Framework must be effective and continuously adapted to new and changed ML/TF risks.

Each SAE is responsible for establishing governing and decision-making fora and committees with documented charters and senior level representation from the first and second line of defence, such as e.g. a Group AML/CTF committee or other adequate AML/CTF committees. The purpose of an AML/CTF committee shall be to ensure effective and adequate handling of ML/TF risks.

Each SAE shall report to the relevant Board, CEO and Group SAE. The Group SAE is responsible for the group level reporting on AML/CTF matters. The SAE may delegate responsibilities and tasks, in accordance with applicable regulations, to subordinate employees with adequate competence, knowledge and suitability.

3.4. Business Management

The Business Management (BA/PA/GF Head), as the first line of defence, is accountable for the risks related to ML/TF within their respective areas of responsibility. The Business Management may delegate tasks related to AML/CTF. However, delegating will not change the risk ownership and accountability for the business relationships and transactions, as well as the accountability to comply with applicable laws and regulations.

3.5. Appointed Officer for Controlling and Reporting

The CEO of the Bank and each Subsidiary shall ensure that a Compliance Officer at executive management level is appointed in the Bank and each relevant Subsidiary, as Appointed Officer for Controlling and Reporting ("OCR"). An appointed OCR could, if appropriate, be appointed for several or all entities within the Group.

The OCR is accountable for the design, maintenance and performance of effective ongoing second line of defence compliance controls, including the reporting to the Financial Intelligence Unit (FIU). It is responsible for the ongoing oversight of AML/CTF related system and control requirements across the Group. The OCR shall report to the Board and CEO. The OCR may delegate responsibilities and tasks, in accordance with applicable regulations, to subordinate employees with adequate competence, knowledge and suitability.

3.6. Internal Audit

Internal Audit, as the third line of defence, is the independent control function and shall test and evaluate the Group's internal policies, controls, IT-systems, models, risk management and procedures regarding AML/CTF.

4. Risk management

The Group is committed to and has processes and procedures in place to identify and manage the risks that it is exposed to and take proportionate measures adequate to manage these risks across all jurisdictions in which it operates – i.e. applying a risk-based approach.

4.1. Risk-Based approach

The risk of being exposed to ML/TF depends on multiple risk factors, such as different customers, countries/geographic areas, products, services, distribution channels and transaction flows, and thus changes over time. It is also recognised that the ML/TF risks may vary across the Group depending on the activities carried out. To adequately and effectively manage and mitigate the ML/TF risks a risk-based approach shall be applied.

The purpose of the risk-based approach is to take appropriate, proportionate and adequate measures to mitigate identified risks. This means that more actions should be taken where the risks are deemed higher. Processes, systems and controls need to be developed and continuously adapted to the nature and extent of the identified risks. Also, resources and qualified personnel need to be allocated accordingly.

4.2. Risk assessment and classification

Each legal entity within the Group, where deemed relevant, shall perform risk assessments that identify, assess and classify the inherent risks of ML/TF. The risk assessments shall take into account relevant risk factors including those relating to customers, countries or geographic areas, products, services, transactions or distribution channels. The risk assessments shall clearly present an overview of the nature and type of risks for ML/TF faced by each legal entity, as well as assessing and describing the levels of those risks. In addition, the mitigating measures in place shall be mapped and evaluated to assess the residual risks in view of the exposure to inherent risks.

The further details and requirements concerning the group risk assessment process and risk classification model shall be outlined in the Group AML/CTF Instruction and accompanying Group Directives.

4.3. Risk appetite for ML and TF risks

The Board is accountable for determining the Group's ML/TF risk appetite and overseeing adequate and effective internal controls for the management of risks. The group risk assessments aim to provide a view of the assessed ML/TF risks, including inherent risks and the residual risks that remain following the application of mitigating measures, given the profile, geographic presence and the activities carried out in the Group. The risk appetite for ML and TF risks is defined in the Policy on Enterprise Risk Management and shall be measured and monitored by key risk indicators.

4.4. Prohibited relationships

The Group will not establish or maintain a business relationship with customers or other parties, nor offer products or services:

- Where such relationships are prohibited under applicable AML/CTF laws and regulations (as defined in the accompanying CEO instruction on AML/CTF) or applicable Financial Sanctions laws or regulations (as defined in the Policy on Financial Sanctions);
- Where the customer or third party's business activities are known to be illegal based on applicable laws and regulations governing this relationship; or
- When the understanding about the prospective customer and its intentions is unclear, the customer or third party is attempting to hide its true identity or place of operations by e.g. refusing to provide appropriate documentation or providing false or misleading information.

5. Know Your Customer ("KYC")

The Group is committed to ensuring that it performs consistent and documented KYC measures that are aligned to and based on the ML/TF risks assessed to determine the risk level of the customer prior to establishing a business relationship or carrying out an occasional transaction. The KYC process shall also aim to support the broader customer strategy, by adding value to the services offered to the customers by the Group.

The Group shall perform KYC measures with respect to its customers, authorised representatives and beneficial owners in line with a risk-based approach. KYC measures include the initial assessment of ML/TF risks associated with the customer relationship, customer due diligence, enhanced customer due diligence where required, simplified customer due diligence where permitted and the on-going customer due diligence to keep KYC information up-to-date and to follow up the ML/TF risk associated with the customer relationship.

The application of risk sensitive customer due diligence measures aims to establish that the prospective customer is who it claims to be and identifies whether it is acting on behalf of another party. The customer due diligence process also aims to establish whether there are any legal or risk appetite barriers to entering into a business

relationship with the prospective customer and to understand the purpose and nature of the relationship.

The process enables the Group on an on-going basis to ensure that the risks associated with the customer relationships are sufficiently mitigated and managed to be in line with the risk appetite of the Group. The Group may determine to exit a relationship, cease or limit the provision of certain products and services if said customer relationship falls outside of the risk appetite or fulfils any of the criteria of being a prohibited customer relationship.

The Group is committed to ensuring that there are robust IT-solutions and strong data quality to enable management reporting of the KYC process based on key performance indicators and key risk indicators.

6. Transactions monitoring

The Group shall perform risk-based transactions monitoring of its customer relationships, including scrutiny of transactions undertaken throughout the course of the business relationship and occasional transactions, to ensure that transactions are consistent with the Group's knowledge of the customer, the purpose and nature of the relationship and the customer's business activities and risk profile. The transactions monitoring aims to identify suspicious and deviating behaviour. The Group is committed to ensuring that it has in place a robust and effective IT system for ongoing monitoring of business relationships and transactions. This also requires strong data quality and technical support.

7. Internal reporting of unusual activity

The Group is committed to ensuring that all employees remain vigilant to the risks of ML/TF and are aware of their personal obligations to file an internal report where they have suspicion, knowledge or reason to believe that a customer or other party may be involved in ML or TF. Processes and procedures for reporting must be implemented and information provided as part of the training provided to employees (see further in section 12 below).

8. Investigations and external reporting

All alerts generated by the transactions monitoring and reports of unusual activities filed internally must be reviewed and investigated by the Group, and if required, escalated to further investigation and possible external reporting to the local Financial Intelligence Unit ("FIU"). Sufficient and adequate KYC information must be obtained, and the KYC information held on the customer must be updated if needed to review and investigate the alerts to determine whether the alert needs to be escalated. Evidence and documentation of all investigations and escalations must be retained to confirm the activities undertaken and the decision rationale.

9. Corporation with authorities

The Group may receive request for information from competent authorities or law enforcement in connection with ML/TF investigations. The Group is fully committed to cooperating with such requests in an effective, prompt and expedient way.

10. Record keeping

Records of relevant KYC information must be retained for a period of five years (following the termination of a customer relationship or performance of transactions) unless local requirements require a longer retention period or data protection regulation limits data from being held for such a period. There shall be adequate processes and routines for the retention of data, documentation and archiving, including but not limited to the traceability and availability without undue delay of customer due diligence measures, transaction monitoring and FIU reporting measures and the supporting evidence and records of transactions, including transactions undertaken throughout the course of a business relationship and occasional transactions.

11. Personal data and information sharing

Adequate routines shall be established for the processing of personal data and information sharing within the Group in accordance with GDPR, applicable local legislation and/or applicable Group Regulation. When information sharing within the Group is needed, there shall be Group common processes and routines for at least concerning customer due diligence, account and transaction details and other relevant information in order to prevent ML/TF.

12. Model risk management

Where models are used for risk assessments, risk classifications and/or monitoring, or other procedures there shall be routines for model risk management. The purpose of the routines for the model risk management is to evaluate and ensure the quality of the used models.

13. Training

There shall be adequate processes and routines to ensure ongoing training programs for all relevant employees and other relevant individuals depending on specific needs and in accordance with applicable Group Regulation. The training programmes shall help employees and other relevant individuals to recognise activities which may be related to ML/TF and how to proceed in such cases. The processes and routines shall include development, implementation and follow-up of training programmes, including documentation of performed training, within the Group.

14. AML Suitability assessment

Routines shall be established to ensure that employees and other relevant persons involved in tasks to prevent the Group from being used for ML or TF, have a level of understanding that are commensurate with their duties and functions, in accordance with applicable Group Regulation.

15. Protection of staff

Procedures shall be established to safeguard employees and other relevant individuals in case of threats or other similar actions as a consequence of fulfilling any obligation under the AML/CFT framework, including but not limited to the KYC process, investigations and documentation of incidents.

Procedures shall also be established to ensure that employees and other relevant individuals are not subject to reprisals because he or she has reported suspected ML or TF internally or externally to the local FIU.

16. Internal reporting (raise your concern)

There shall be adequate processes to ensure internal reporting to internal stakeholders, including but not limited to the CEO and the Board. Furthermore, there shall be routines in place to ensure that systematic shortcomings or incidents are reported in accordance with routines for internal reporting.