Extract from
Instruction
for procedures against
Money Laundering
and
Terrorist Financing
for the SEB Group

derived from the Instruction for the President and Chief Executive Officer

adopted by the President and Chief Executive Officer of
Skandinaviska Enskilda Banken AB (publ)
on 20 November 2017

1. General

The SEB Group shall, as part of its normal business conduct, combat Money Laundering and Terrorist Financing. This is of utmost importance in order to meet regulatory obligations, to maintain the SEB Group ´s good reputation, and to contribute to the stability of the financial system. The SEB Group shall also apply high ethical standards and assume social and environmental responsibility.

2. The SEB Group's AML Governance Model

The SEB Group's AML Governance Model shall be based on a three-line of defense approach: First line responsibility rests within divisions, business areas and business units, subsidiaries, branches and affiliated companies. The first line is responsible for the implementation of AML/CFT procedures and controls, as well as for a comprehensive ML/TF Risk Assessment and risk management. Second line responsibility rests with Group Compliance in line with the Instruction for Compliance in the SEB Group. Third line responsibility rests with Group Internal Audit being responsible for independent control and evaluation.

The SEB Group's AML Governance Model includes the following roles;

1. Group AML Senior Manager (first line on group level);
2. Group AML Risk Committee (first line on group level);
3. Group AML Coordinator (first line on group level);
4. AML Business Responsible(s) (first line);
5. AML Operative Responsible(s) (first line);
6. Group Compliance (second line); and
7. Group Internal Audit (third line).

The Group AML Senior Manager:

- is responsible for conducting and updating the SEB Group´s ML/TF Risk Assessment;
- is the owner of the ML/TF Risk Assessment process and responsible for the methodology of conducting the assessment, including relevant areas to be evaluated when assessing ML and TF risks within SEB;
- shall compile the business units´ respective risk assessments to a consolidated SEB Group ML/TF Risk Assessment;
- shall ensure that the SEB Group adopts instructions, procedures and controls regarding AML and CFT measures which at any time fulfil internal and external AML and CFT requirements;
- is responsible for following up on that routines and procedures to counter ML and TF risks are implemented in the SEB Group, including relevant KYC processes;
- shall, on an ongoing basis, report to the CEO on the risks of the SEB Group being exposed to ML and TF as well as the management and mitigation of ML/TF risks;

- is responsible for the AML risk scoring model routines including documentation of the model and changes to it; and
- shall delegate decision making power to each Customer Adoption Committee and approve of the committees´ work instructions.

3. Management of ML/TF Risks

In order to manage ML/TF risks in a structured and efficient way, a risk assessment process shall be implemented. Its main components are to:

1. identify and assess threats and vulnerabilities and level of risk exposure (impact and probability) with the aim to point out inherent risks;
2. manage and mitigate identified risks;
3. assess and follow-up the residual risk; and
4. report internally.

The risk assessment process shall provide the foundation to an ongoing understanding and effective management of the ML/TF risks in relation to:

1. SEB's Customer base;
2. the products and services SEB offers;
3. the geographies involved;
4. the delivery channels employed by SEB; and
5. other relevant, including possible emerging, risk factors.

4. Know Your Customer

A sound KYC program is the best method of preventing ML and TF, the basis of a professional relationship with Customers, and an important tool to apply an appropriate level of customer due diligence measures.

The Client Executives have the full responsibility for knowing their Customers and understanding their business relationship with SEB. Thus the KYC process, including the initial and ongoing due diligence measures, shall be carried out in the business unit responsible for each Customer although certain tasks maybe delegated and/or centralized.

The main components in the KYC process and applying customer due diligence measures are:

1. identity check and verification of identity and check of PEP status;
2. check of ownership- and control structure and identification/verification of Beneficial Owner and check of PEP status;
3. assessing and, as appropriate, obtaining information on the purpose and intended nature of the business relationship (1-3 jointly referred to as Basic KYC information);
4. checking against sanction lists etc.;
5. performing risk scoring measures;
6. assigning relevant due diligence level;

7. applying enhanced due diligence measures (when applicable);
8. obtaining Customer Adoption Committee´s approval (when applicable); and
9. ongoing Customer due diligence (monitoring of the business relationship and transactions).

5. Monitoring and reporting

Customer activities and transactions shall, based on a risk based approach, be monitored manually by the Client Executive within ongoing customer due diligence and electronically by specially designated employees in order to identify suspicious activity.

The assessment of what constitutes suspicion shall be based on the information about the Customer obtained by the employee handling the matter, and the scope of the Customer´s business relationship, along with SEB´s general knowledge of deviating or suspicious transaction patterns.

Should the review give rise to an actual or potential suspicion related to ML/TF, the Client Executive shall immediately report the issue to Compliance, which shall initiate an investigation and decide whether to report the issue to the FIU in the form of an SAR. Matters of a more serious nature where a SAR has been made shall be reported to the relevant AML Business Responsible or AML Senior Manager and Head of Division/Subsidiary or Head of Site.

The obligation to report is also applicable in situations where the business relationship has been declined, or the transaction has not been processed due to suspicious circumstances.

.

SEB shall have a transaction monitoring system for detecting suspicious activities and support the monitoring of significant changes in Customers´ behaviour or business profile and unusual transactions. The transaction monitoring system shall be developed to include relevant information for risk scoring measures in the KYC process.

6. Recordkeeping

All KYC information shall be kept for a period of at least five years after the business relationship with the Customer has ended or, in the case of one-off transactions, after the execution of the transaction, unless a longer retention period is required under applicable local law.

All KYC information shall be stored electronically so that it is available immediately on demand by the Client executive, and by Group Compliance.

7. Training

The following training strategy shall be the basis for the training programs that shall be set up within the divisions and business units.

Once every third year: All employees shall pass the SEB AML/CFT e-learning program. The program shall be a part of the introduction for all new employees.

Annually: All employees dealing with customer-related matters or, who, due to the nature of their position, have special needs of AML/CFT knowledge, shall, as a complement to the SEB AML/CFT e-learning program, be trained, updated and/or informed regarding important and relevant AML/CFT regulations and relevant internal procedures as appropriate.

Ongoing: For employees operating in areas which may represent high risk, e.g. Correspondent Relationship, international private banking and non-resident Customers, the need for tailor made training or information shall continuously be assessed by the business with the support of Group Compliance and when a need is identified, action shall be taken.