Policy on risk management of money laundering and financing of terrorism

SPAREKASSEN SJÆLLAND-FYN

Policy for risk management of money laundering and financing of terrorism

1. Introduction

Pursuant to section 8(1) of the Danish Act on Measures to Prevent Money Laundering and Financing of Terrorism ("the AML Act"), the Board of Directors of Sparekassen Sjælland-Fyn A/S ("Sparekassen") has adopted the following policy on risk management of money laundering and financing of terrorism ("the Policy").

The Policy lays down Sparekassen's focus on the area of money laundering and financing of terrorism for the purpose of effectively preventing, mitigating and managing risks in this area. Sparekassen's risk profile (risk of being misused) is defined in Sparekassen's risk assessment.

The Policy lays down the overall strategic goals for preventing money laundering and financing of terrorism based on the risk assessment of Sparekassen's business model.

To reduce the risk of being misused for money laundering and/or disclosing its current business strategy, Sparekassen has in its external policy, compared to its internal policy, excluded certain types of activities from Sparekassen's risk assessment and its business model. However, the internal policy will always be available to relevant authorities and relevant stakeholders.

2. Risks governed by the Policy

The inherent risk of money laundering and financing of terrorism means the inherent risk of Sparekassen being misused for money laundering and financing of terrorism. This inherent general risk of being misused is based on the national risk assessment as well as the supranational risk assessment.

The Policy is primarily based on the following risk factors related to Sparekassen's business model and to the key elements of Sparekassen's assessment of the inherent risk of being misused for money laundering and financing of terrorism: customers, products, services, transactions, delivery channels, and countries or geographical areas. Other factors affecting the risk of being misused for money laundering or financing of terrorism are assessed as well.

3. Sparekassen's risk profile (inherent risk of being misused) in the area of money laundering and financing of terrorism

Sparekassen is obliged to minimise its risk of being misused for money laundering and financing of terrorism. This is done by complying with the provisions issued under the AML Act, the Regulation of the European Parliament and of the Council on information accompanying transfers of funds, and EU Regulations containing provisions governing financial sanctions.

Based on the risk assessment, Sparekassen's inherent risk of being misused for money laundering or financing of terrorism has been rated as medium/high for money laundering and medium for financing of terrorism.

The sub-assessments of the inherent risk for each risk factor in the risk assessment – customers, products, delivery channels, and geographical areas – serve as a basis for the business process descriptions and procedures prepared and the monitoring scenarios installed in the system designed to monitor customer transactions.

3.1 Customers

Because Sparekassen's portfolio of customers also includes types of customers which from a money laundering and terrorist financing perspective may pose a risk and because Sparekassen has some customers of the type posing an increased risk of money laundering, its customer mix is deemed to involve a high risk of being misused for both money laundering and financing of terrorism.

Sparekassen must therefore have knowledge of its customers, including their identity, and sufficient information about what they want with Sparekassen and what their intentions are (origin of the funds etc), for which reason Sparekassen has considerable focus on Know Your Customer (KYC) activities.

Together with the findings from Sparekassen's KYC activities and considering the customers' transactions, the sub-assessments of the inherent risk for each risk factor in the risk assessment provide a basis for the relevant parameters in Sparekassen's system for regularly monitoring customer activities.

This monitoring (and ongoing follow-up), along with specific opt-outs/delimitation of the business model, ensures that Sparekassen's risk of being misused for money laundering and financing of terrorism is reduced considerably, resulting only in a residual risk that is acceptable.

3.2 Products, services and transactions

Identification and delimitation of risk factors in Sparekassen's products:

Sparekassen's product range consists, for example, of quite traditional deposit products which, combined, are both nationally and supranationally considered to involve a medium risk of being misused for money laundering and financing of terrorism. Also, Sparekassen aims to have long-term full-customer relationships, and this helps reduce the risk of money laundering and financing of terrorism.

However, some standard products and services, such as handling of ATM cash (Sparekassen has no cash service functions at its branches) and Private Banking, are deemed to involve a high risk, yet this risk is mitigated by the parameters installed in the IT-based transaction monitoring system and by the advisers' intensified focus on ensuring that relevant documentation is always sufficient in the day-to-day transactions.

In the national and the supranational risk assessment, the possibility of anonymity – both with respect to what has generated/produced the funds and with respect to what the funds are to be used for – is considered to be a key reason why an increased risk of being misused for money laundering and financing of terrorism exists, and this is therefore a daily focal point for the advisers.

Sparekassen's types of products, services and transactions are therefore rated to involve a medium risk of being misused for money laundering and financing of terrorism.

3.3 Delivery channels
Identification and delimitation of risk factors in Sparekassen's delivery channels:

Sparekassen's risk assessment rates its delivery channels to involve an increased risk of being misused for money laundering and financing of terrorism – especially customers' intensified use of self-service systems is contributory to this rating. However, Sparekassen still has a high level of contact with its customers, and this reduces the risk of delivery channels being misused.

In the national and supranational risk assessment, two delivery channels in particular – "Possibility of Distance Onboarding" and "Possibility of Payment via ATM" – are rated to involve a high risk of being misused.

At Sparekassen, however, it is only possible to use distance onboarding for entirely basic account customers with appropriate proof of identity, but without any kind of products or services except for the legal requirement to have a basic bank account. If business increases, this will require ordinary contact with an adviser. Transactions on the basic bank account will at the same time be monitored immediately by Sparekassen's IT-based transaction monitoring system and, as a standard procedure, all new customers will be monitored more closely in the beginning of a customer relationship.

The "Possibility of Payment via ATM" channel is monitored as all ATMs are under video surveillance, and it goes for them too that transactions are monitored by Sparekassen's IT-based transaction monitoring system with high focus on cash transactions exceeding a certain amount.

The risk assessment rates Sparekassen's delivery channels to involve a medium/high risk of being misused for money laundering and financing of terrorism.

3.4 Geographical areas
Identification and delimitation of risk factors in Sparekassen's geographical areas:

Sparekassen's geographical areas of activity are not by themselves viewed to significantly affect the risk of Sparekassen being misused for money laundering and financing of terrorism.

This view is underpinned by Sparekassen's customers primarily living in Denmark and in the geographical areas that it has branches in. Sparekassen's geographical areas are therefore rated to only involve a low/medium risk of the institute being misused for money laundering and financing of terrorism.

4. Measures to mitigate the risk of being misused for money laundering and financing of terrorism

Using its risk assessment, which is based on both the national and the supranational risk assessment, and own internal experience, Sparekassen has implemented the following measures to minimise the risk of being misused for money laundering and financing of terrorism:

4.1 Rules, guidelines and opt-outs in the business model
Business process descriptions outlining what we do and do not do (based on what increases and reduces the risk of being misused for money laundering and financing of terrorism).

Business process descriptions outlining how we do things – processes, instructions and tools (based on what increases and reduces the risk of being misused for money laundering or financing of terrorism).

Moreover, Sparekassen has opted out of specific industries and is cautious about starting customer relationships in specific industries that must be approved by the Anti-Money Laundering Team.

4.2 Other internal business process descriptions
Sparekassen has also introduced written internal rules on:

- Customer due diligence
- Duty of awareness, screening and recording
- Notification of the Danish Anti-Money Laundering Secretariat
- Retention of recordings
- Internal control
- Risk assessment (serving as a basis for this Policy)
- Risk management (being performed based on this Policy)
- Management control and communication
- Staff training and instruction programmes

These internal rules have been drawn up to support Sparekassen further in reducing/minimising its inherent risk of being misused for money laundering and financing of terrorism (based on the risk assessment prepared by Sparekassen).

4.3 Continuous daily vigilance of staff
The staff's continuous vigilance with respect to customers and their transactions constitutes an important part of Sparekassen's measures to reduce/avoid the risk of being misused for money laundering or financing of terrorism.

It is a duty to be vigilant that all staff must observe in their daily work with respect to all customers – and this duty is supported by continuous and relevant information to and training of the staff.

Information is provided to staff, and they receive training, both individually in connection with feedback on controls (for example, as part of the KYC activities) and at large meetings or

through the issuing of general information (for example, if new learning or insight so requires).

In addition, all staff must regularly complete Sparekassen's IT-based course modules (also an important element in keeping up the staff's skills in this area) which have been updated with current knowledge on how to reduce the risk of being misused for money laundering or financing of terrorism.

4.4 Ongoing monitoring of transactions
Along with staff vigilance, the cornerstone in Sparekassen's dedicated efforts to reduce the risk of being misused for money laundering and financing of terrorism is to regularly monitor customer transactions.

The scenarios installed in the system monitoring customer transactions are based on information from Sparekassen's risk assessment.

However, the basis underlying the scenarios in the monitoring system are deviations from normal behaviour that has been described and is consistent with the customer contract signed, and that is why the KYC process is crucial in the monitoring system timely setting off relevant alarms.

The basic KYC activities have therefore been standardised, optimised and are a constant focus every day – and regularly subjected to control and follow-up.

4.5 Controls
Regular staff have been devoted to controlling and following up on the KYC activities, and any necessary adjustments are reported to the individual adviser and their immediate superior, with regular summarised overviews of performance to the area managers. These overviews of performance serve as a basis for corrective actions, such as a general control of areas not performing adequately.

Any alarm prompted by the monitoring system will result in evaluations and any necessary testing of transactions and/or information. In addition, other relevant controls are performed in key areas that are evident from the individual business process descriptions. Should any new knowledge or the findings from the ongoing monitoring process so dictate, areas will be selected for a thematic review.

The risk-mitigating measures which are described in this Policy (and which are based on Sparekassen's risk assessment) have significantly reduced the inherent risk of Sparekassen being misused for money laundering and financing of terrorism.

5. Residual risk of Sparekassen being misused for money laundering and financing of terrorism

Although the measures described in item 4 above are considered to significantly reduce the risk of Sparekassen being misused for money laundering or financing of terrorism, a residual risk will always exist.

The residual risk must be as little as possible in relation to Sparekassen's business model and also be at an acceptable level for Sparekassen; this risk is assessed annually by the Compliance and Risk Management Function using Sparekassen's internal risk model which incorporates the risk of being misused as well as an estimate of any consequences in the risk assessment.

The residual risk is reported annually to the Executive Board and the Board of Directors. Then it is determined whether the level of this residual risk is acceptable to Sparekassen. If the level is found to be too high, the mitigating measures described above must be re-evaluated or re-thought.

6. Principles for the organisational distribution of responsibilities for the area of anti-money laundering and financing of terrorism

The overall responsibility for preventing and combatting money laundering and financing of terrorism and for complying with financial sanctions rests with the Anti-Money Laundering Team. Sparekassen's Anti-Money Laundering Officer under section 7(2) of the AML Act is Susanne Bouman, who is head of the Anti-Money Laundering Team and responsible to Savings Bank Director Jan Kolbye Jensen.

Jan Kolbye Jensen is responsible to Executive Board member and Chief Executive Officer Lars Petersson, who is also the designated member of the Executive Board responsible for the anti-money laundering area, see section 8(5) of the AML Act.

The Anti-Money Laundering Officer has therefore direct access to the Executive Board, including the designated member of the Executive Board responsible for the anti-money laundering area, and has also access to the Board of Directors.

7. Capabilities of staff

The staff holds a professional competence enabling each employee to do active efforts in a qualified manner to reduce Sparekassen's risk of being misused for money laundering or financing of terrorism in their professional fields.

These qualifications reflect the duties of the specific job function and may arise from education, special industry knowledge or other work experience.

However, this is an area in constant development, and this is why Sparekassen's staff receive regular training in the requirements of the AML Act as well as new relevant knowledge in the area. So, active efforts are made to maintain capabilities to match current threats in this area.

8. Reporting

The Anti-Money Laundering Department reports to the Executive Board, the Board of Directors and the Danish Financial Supervisory Authority at least once a year or when required/relevant if new risks of money laundering, alerts and/or other concerns are identified where the risk of money laundering is considered high.

9.Follow-up and approval

The Anti-Money Laundering Officer reviews the Policy at least once a year and makes the necessary adjustments, after which the Policy is presented to the Executive Board before it is finally approved by the Board of Directors. Adjustments may be made more frequently, if relevant – for example, in the event of significant consequences of changes in the national and supranational risk assessment.

Approved by the Board of Directors

Design : omw.dk · Foto: Ricky John Molloy

For more information, please go to spks.dk

SPAREKASSEN SJÆLLAND-FYN

Sparekassen Sjælland-Fyn A/S | Isefjords Alle 5 | 4300 Holbæk | +45 5948 1111 | info@spks.dk | CVR nr. 36532130