Danske Bank

AML/CTF and Sanctions Policy

April 2017

Purpose

This Policy is issued in accordance with the Information Management Policy and sets out the principles and standards for compliance and management of risks associated with financial crime in Danske Bank Group (the Group). The Board of Directors has the overall responsibility for compliance and management of risks associated with financial crime in the Group.

This document is referred to as the Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF) and Sanctions Policy (the "Policy"). The purpose of the Policy is twofold:

1. To prevent the the Group from being used for financial crime so as to comply with all applicable legal requirements; and,
2. To ensure that the most appropriate action is taken by the Group to mitigate the risks associated with financial crime.

This Policy outlines the applicable legal requirements related to financial crime to which the Group must adhere, as well as internal measures which are established by the Group to ensure it complies with these legal requirements. The Policy sets the parameters for the Group in relation to the AML, CTF and sanctions framework.

Scope and application

The Policy applies to all employees, all functions, all units in the Group, and all regulated legal entities once adopted by their Senior Management. In case a Group Policy conflicts with local requirements, Senior Management of the subsidiary can approve a Group Policy with deviations. Any material deviations from the Group Policy must be reported to the Board of Directors of Danske Bank A/S as well as the administrator of the Information Management Policy.

The aim of the Group is not only to comply with relevant legal requirements, but also to mitigate and reduce the potential risk to the Group of our customers using our products, services and delivery channels to launder the proceeds of illegal activity, fund terrorist activity or conduct prohibited financial sanctions activity (these offences denote "financial crime").

Target group

This Policy is relevant to all employees in the Group.

Definitions

Requirements

The Group must comply with the relevant laws and regulations in the Market Areas in which it operates. The Group may exceed the requirements set out in such laws and regulations so as to ensure that the Group is not used to facilitate financial crime. The Group must comply with the requirements set out in the:

1. European Union Directive on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing;
2. Applicable regulations of national governments and multinational bodies in relation to financial sanctions; and
3. Any other national or international law or regulation applicable to the Group's operations.

Money laundering and terrorist financing

Money laundering is the method which criminals use to make illegal economic gains appear legal. The characteristics of money laundering relate to the actions involved in laundering *property* and the knowledge (or suspicion) as to the origin of the property.

Terrorist financing relates to the raising or holding of funds (directly or indirectly) with the intention that those funds should be used to carry out activities defined as acts of terrorism.

The terms "anti-money laundering" and "counter terrorist financing" are generic terms adopted in relation to the predicate financial crimes.

Financial sanctions

Financial sanctions are measures imposed by national governments and multinational bodies which seek to alter the behaviour and decisions of other national governments or non-state actors that may (i) threaten the security of the global community, or (ii) violate international norms of behaviour (e.g. human rights violations).

The Group must comply with the following sanctions measures:

1. The United Nations (UN) Security Council consolidated sanctions list;
2. The EU's consolidated list of persons, groups and entities;
3. The US Department of the Treasury, Office of Foreign Assets Control (OFAC) sanctions lists:
4. The US Department of the Treasury, Financial Crimes Enforcement Network (FinCEN) list;
5. The UK HM Treasury (HMT), Office of Financial Sanctions Implementation, "consolidated list of targets"; and
6. The Group's internal list of natural persons and legal entities.

Risk Based Approach

A "Risk Based Approach" refers to the assessment of financial crime and implementation of measures to reduce or mitigate the risk of financial crime. As a result, the Group will allocate and prioritise resources according to where the most effective risk mitigation is required.

Group measures towards money laundering/terrorist financing and financial sanctions

The Group is undertaking a number of initiatives to strengthen its ability to ensure its compliance with the requirements outlined above. The Group will continually assess its existing IT system and make necessary changes so as to be most effective in accordance with the risk based approach.

Governance

The Board of Directors has instructed the Executive Board to ensure that there is a robust approach within the Group to prevent money laundering, terrorist financing and breaches of financial sanctions. It is the responsibility of the Executive Board to ensure that the Group complies with the measures set forth in this Policy. The Executive Board is responsible for implementing this Policy and may delegate its responsibilities.

The Executive Board shall appoint an "anti-money laundering responsible person" at management level with the responsibility to ensure that the Group complies with the legal requirements.

The Business Units are accountable for the risks related to financial crime. Business Units as well as Senior Management can delegate tasks related to the mitigation of financial crime risks to Group Operations or other first line departments. However, delegating will not change the risk ownership and accountability for Business Units but will merely imply a new responsible unit for conducting the delegated process.

Given the zero tolerance of the Group in relation to financial crime risks, outsourcing to external suppliers may only be executed after close consultation with Group Compliance in accordance with the Outsourcing Policy.

Risk tolerance

The Group does not tolerate any breach of the above requirements. Any material or systemic breaches should be reported to the Audit Committee.

The Group will not accept either natural person or legal entities as customers (both existing and new customers) if they are subject to financial sanctions.

In order to comply with financial sanctions regulations, the Group must be able to verify the identity of its customers. Therefore the Group requires a robust control environment with low error rates for due diligence after applying internal controls.

There are several other legal regulations which impact upon this area in relation to, for example, data and consumer protection. The Group will examine all legal possibilities to satisfy the legal requirements above and, at the same time, comply with data and consumer protection regulations. Should a conflict arise between the requirements within this Policy and any other regulation, Group Compliance should be contacted.

The Group will take all relevant steps to discontinue the provision of products and services to natural persons and/or legal entities where the Group has a reason to suspect that the natural person and/or the legal entity is or will use the Group's products and/or services for financial crime.

Group wide risk assessment on financial crime compliance

The Group operates in several Market Areas with a full range of banking products being offered to multiple customer segments. Accordingly, the Executive Board must establish an overall group wide risk assessment on financial crime describing the inherent financial crime risks of the Group, the control environment to mitigate such risks, and the residual financial crime risk.

The group wide risk assessment on financial crime represents a cornerstone for the Group in meeting the requirements of the risk based approach.

Customer due diligence

The Group's goal of developing its knowledge of its customers so as to improve the value of advice it can offer is closely related to the due diligence obligations of the Group. In parallel to the verification of a customer's identity, the Group applies a risk based approach towards the collection, registration, and monitoring of information in relation to the nature and intent of the customer relationship.

The data gathering which is conducted to meet the above requirements forms the baseline for transaction monitoring and is a foundation in the Group's IT-driven AML, CTF and financial sanctions risk scoring model ("Risk Scoring").

The Group applies a risk based approach towards due diligence through the Risk Scoring with reference to a customer's geographic ties, chosen products and / or services. A Risk Score is applied as low, medium or high. This risk scoring indicates the risk of whether the given customer may use or will use the Group's services and/or products for financial crime.

The Group will decide upon appropriate customer acceptance instructions in order to set clear guidance as to which natural persons and legal entities the Group will see as the strategic customer base with references to AML, CTF and financial sanctions risk. These instructions should also give guidance as to the procedure for terminating a customer relationship due to financial crime concerns.

Given the volume of customers in many Market Areas, the Group requires a robust and effective IT solution to cater for an effective initial registration and ongoing monitoring of the customer base. It is essential that all natural persons and legal entities are registered on the Group's IT systems. Having sufficient identification information, the Group will - within the purpose of the requirements - aggregate all relevant products and services on each customer number.

The Group undertakes significant effort to clarify the ownership and control structure of legal entities. In cases where controls and/or ownership exceeds 25% for a given natural persons, the identity of this beneficial owner must be verified.

Screening of politically exposed persons

In order to ensure that all natural persons defined as politically exposed persons (PEPs) are identified and registered in the Group's system as such, a PEP screening process is conducted when natural persons are on-boarded. Furthermore, the customer database is screened for PEPS on a weekly basis.

Enhanced Due Diligence and On-going Due Diligence

The Group performs enhanced due diligence and on-going due diligence measures proportionate with the Risk Scoring of the customer. High risk customers will therefore be subject to enhanced due diligence and annual on-going due diligence. On-going due diligence processes will be applied to all existing customers within a specific period that will be determined by whether they are scored as *medium* or *low*.

Design
The Group IT solution must be designed to ensure that robust internal controls of customer due diligence is maintained.

This requires strong data quality and, where possible, automatic on-going due diligence between public registries and the Group's IT systems in relation to customer data. Data quality shall be measured and reported as a key performance indicator.

Transaction monitoring

The Group applies a risk based approach to transaction monitoring which includes automated as well as manual processes. Transaction monitoring is conducted in order to evaluate whether the activities of the customer (the use of their products and/or services and/or their general behaviour) is consistent with the stated nature and intent of their relationship. As part of its transaction monitoring, the Group further investigates activities that are deemed to be "unusual" with regard to the stated position of the customer.

The automated transaction monitoring shall on a risk based approach cover all Business Units, all customers, all market areas and all products with appropriate scenarios. The manual transaction monitoring – investigating and reporting of the unusual activity to the Money Laundering Reporting Officers - is achieved through training and awareness campaigns.

Design
The Group performs automated transaction monitoring. Likewise a process has been established where Business Unit employees can file "unusual activity reports" with the Money Laundering Reporting Officers based on information gained from automated and manual transaction monitoring. The Money Laundering Reporting Officers are responsible for assessing whether the described activities in the "unusual activity report" are genuinely suspicious and warrant the filing of a "suspicious activity report" to the local Financial intelligence Unit, if relevant.

Sanctions

In order to comply with sanctions imposed by the UN, EU, US, and any local authorities, relevant control procedures must be in place. Most Market Areas within the Group are EU Member States and, as such, are obligated to follow EU regulation and therefore to comply with EU sanctions.

US sanctions regulations have a major impact on the Group due to the USD transactions that the Group undertakes. The Group has therefore chosen to be compliant with the requirements of the Office of Foreign Asset Control (OFAC) regardless of currency.

The Group has an externally supplied screening solution, which is integrated in the Group's IT systems to ensure that the Group is compliant with AML, CTF and financial sanctions regulations.

The Group establishes a Sanction Board where principal decisions are to be taken regarding Sanctions. The mandate includes decisions on deviations from requirements of the Policy extending the regulatory requirements. If Group Compliance disagrees to the decision of the Sanction Board the decision has to be escalated to the head of the Business Unit.

Transaction Screening
The Group conducts real-time transaction screening on all cross-border payments, swifts and cheques in relation to relevant lists of named terrorist and sanctioned entities.

Customer Screening
The customer screening solution ensures that all natural persons as well as legal entities registered in the Group's IT systems, are screened against the relevant lists of named terrorist and sanctioned entities.

Natural persons and legal entities designated by the UN and EU shall be highlighted and may be subject to asset freezing with subsequent reporting to appropriate authorities. The Group will, to the greatest extent possible by law, terminate or limit the services offered to natural persons and legal entities designated by OFAC as Specially Designated Nationals.

Management information
The Executive Board must determine key performance indicators and develop management information requirements and processes to gain insight into and satisfaction with the effectiveness of the AML framework.

Retention and record keeping
The Group acknowledges that the foundation for a robust internal control environment towards customer due diligence and enhanced due diligence requires electronic retention of the material received for the purposes of customer due diligence, on-going due diligence and/or enhanced due diligence. The archiving must be completed in a manner making it available to all employees having appropriate access to the customer in question (within the Group's existing IT solution). The Group implements measures for other accepted electronic ways of verifying identities.

Documentation must be kept during the lifetime of the customer's relationship with the Group and at least *five* years after termination of the customer relationship.

Training and awareness
The Group requires that all employees possess an adequate awareness levels of the risks of financial crime. Given that financial crime can be identified from various sources, the Group must ensure that all employees have a suitable degree of awareness, i.e. when highly skilled specialist staff (traders, lawyers, managers, staff in back-office, etc.) encounter something unusual relating to a customer's behaviour in their daily work, they must consider whether the unusual behaviour may be as a result of underlying financial crime.

In relation to the training of employees, the Group applies a risk based approach so that the broad range of employees can have their training through yearly e-learning courses targeted towards the job position of the employee. By acknowledging the complexity of this area, the Group supports external certification and face-to-face training for employees working in key positions in this area of the Group.

Reporting
The anti-money laundering responsible person shall report on the Group's AML, CTF measures and on the progress of major mitigating activities and programmes to the Executive Board and Internal Audit on a semi-annual basis as a minimum and on an annual basis to the Board of Directors.

In addition to direct reporting to the Executive Board and the Board of Directors by the anti-money laundering responsible person, relevant money laundering and terrorist financing risks are also part of the on-going operational risk reporting prepared by Group Risk Management.

Review
This Policy must be reviewed by Group Compliance at least annually. Any changes to the Policy must be endorsed by the Executive Board, the Audit Committee and approved by the Board of Directors.