Policy for Measures Against Money Laundering and Terrorist Financing

Company:	Nordnet AB (publ)
Approved by:	Board of Directors
Date of approval:	2024-11-25 (2023-11-23)
Document owner:	Chief Financial Crime Prevention Officer at Nordnet Bank AB
Revised:	Annually or more often if required
Confidentiality class:	Open

Nordnet

Table of content

1 Introduction

This policy applies to Nordnet Bank AB, Nordnet Pensionsförsäkring AB, Nordnet Livsforsikring AS, Nordnet Fonder AB, and, where applicable, all their respective branches and subsidiaries (all companies are hereafter commonly referred to as “Nordnet” or “the Companies”). As a part of its normal operations, Nordnet shall do what it can to prevent money laundering and counteract terrorist financing (ML/TF). This work is critical to ensure that Nordnet complies with the regulatory requirements set on its operations, and necessary so that Nordnet can maintain its good reputation and contribute to the financial system's stability.

The purpose of this policy is to provide a group framework for Nordnet’s work against ML/TF. The policy constitutes a minimum standard. As a principal rule, deviation from the policy may not occur unless the deviation entails more stringent measures or if the national legislation prevents an application of the standards that the policy expresses.

When this policy references ML/TF risks, it also encompasses closely related risks, including but not limited to financial sanctions, fraud, tax evasion, bribery and corruption, market abuse, and insider dealing.

2 Organization and reporting

2.1 Roles and responsibilities

The Companies’ Board of Directors is ultimately responsible for ensuring that there is a well-functioning internal governance and control in the Companies’ operations in accordance with applicable laws and regulations within the ML/TF area. The Companies’ CEO is ultimately responsible for ensuring that risks are managed in accordance with the Board of Directors’ decisions and that operations are conducted appropriately and in accordance with applicable laws and regulations within the ML/TF area.

The Companies shall, where this is considered necessary, or where there are local legal requirements, appoint a Specially Appointed Executive (SAE) and Money Laundering Reporting Officer (MLRO).

To prevent ML/TF in an effective and controlled manner, Nordnet shall apply the three lines of defense according to applicable local regulations regarding governance, risk management, and control.

2.2 Reporting

The Companies’ SAE, or equivalent to SAE, shall, on a regular basis, report to the Board of Directors and the CEO on relevant AML/CFT matters. The report shall, at a minimum, include information on measures, procedures, and other actions decided by Nordnet, how these are implemented, and measures taken to strengthen controls and mitigation measures.

The Companies' MLRO, or equivalent to MLRO, shall, on a regular basis, report to the Board of Directors and CEO on compliance risks within the ML/TF area. The report shall include risks and deficiencies, and if appropriate, proposed measures. The MLRO report may be included in the Compliance department's quarterly report as its own section.

The internal audit shall regularly, at least yearly, report to the Board of Directors on how Nordnet complies with the ML/TF laws. The report shall, at a minimum, include the results of its findings.

The Companies shall also, where required by local rules and regulations, periodically or upon request, submit requested information to the local financial supervisory authorities where applicable.

3 Risk management

3.1 Risk appetite and incident management

Nordnet is committed to identifying and managing the ML/TF risks it is exposed to and taking appropriate measures required to manage these risks across all countries in which it operates. Given the serious consequences that ML/TF can have on Nordnet, the financial system, and society, Nordnet has a low-risk appetite in relation to the overall residual risks of ML/TF. Nordnet's strategy is to mitigate inherent risk across all products/services and work effectively with financial crime prevention and detection by monitoring, controlling, and reporting known and potential risk parameters through a robust and compliant anti-financial crime framework.

Nordnet shall have a process for incident reporting to ensure that incidents are investigated, and that appropriate actions are taken. The incident reporting process shall be further detailed in Risk Control Function's steering documents.

3.2 Risk-based approach

The risk of being used for ML/TF varies depending on customer characteristics, countries, transactions, channels, products, and services, and changes over time. To be able to manage the risks of ML/TF in an effective and structured manner, Nordnet shall apply a risk-based approach. The risk-based approach means that Nordnet needs to identify, assess, and understand the ML/TF risks that Nordnet is exposed to and take appropriate and proportionate mitigation measures in accordance with the level of risk identified, in order to mitigate them efficiently. Situations that entail a higher risk require more extensive mitigating measures than situations that entail a lower risk.

3.3 Business Wide Risk Assessment (BWRA)

As mentioned above, the risk-based approach demands companies to take actions in proportion to the risk they are subject to. In order to enable this, the Companies shall perform a BWRA of its operations. In the BWRA, Nordnet shall assess how the products and services provided could be misused for ML/TF, and how large the risk is that this would occur. The Companies shall, particularly, consider the products/services, customers, distribution channels, and geographical risk factors. The BWRA shall serve as a basis for the Companies' procedures, guidelines, and other

measures to combat ML/TF. The BWRA shall be carried out and documented for each applicable entity and branch in Nordnet.

The BWRA shall be carried out and updated annually, or more frequently if necessary. The BWRA shall also be updated before Nordnet offers new or significantly changed products and services, targets new markets, or makes other relevant changes to the business that may affect the ML/TF risk. In addition, the BWRA shall be updated when prompted by internal or external circumstances.

3.4 Risk classification of the customer

Nordnet shall assess the ML/TF risk associated with customer relationships. As a starting point, the customer's risk shall be based on the risks identified in the BWRA and Nordnet's knowledge about the customer. A new individual risk classification shall be performed if anything changes in the customer's behavior or deviates from what is known during the relationship.

4 Know-Your-Customer (KYC)

The Companies shall obtain the customer knowledge before a business relationship is established, and the information obtained shall be sufficient to manage the risk associated with the customer relationship. The customer knowledge shall also be sufficient for the ongoing due diligence of business relationships and assessing whether a transaction is considered deviant or not. The Companies shall not establish or maintain a business relationship, or carry out a single transaction, if the Company does not have sufficient knowledge about the customer to be able to manage the risk of ML/TF that can be associated with the relationship.

The KYC measures shall be applied in accordance with the risk-based approach. If the risk of ML/TF associated with the customer relationship is classified as low, simplified due diligence measures can be applied. If the risk associated with the customer relationship is classified as high or where required by local rules and regulations, enhanced due diligence measures must be taken.

The Companies shall have procedures that describe the KYC process in detail. The Companies shall also have procedures to terminate a business relationship if the customer due diligence becomes outdated or turns unsatisfactory over time, and sufficient customer due diligence cannot be obtained.

5 Monitoring and reporting

The Companies shall monitor ongoing business relationships and assess individual transactions to discover such that are suspicious or, on reasonable grounds, can be suspected of being part of ML/TF. The focus and scope of the monitoring shall be based on the risks identified in the BWRA, the risk of ML/TF associated with the customer relationship, and other information on the method for ML or TF. The Companies shall, in a separate document, have more detailed guidelines for monitoring and reporting, secrecy and prohibition of disposition.

6 Preservation of documents and information

The Companies shall preserve all KYC information, including potential review and reporting (which is a part of the KYC information) for at least five years after the end of the business relationship. Should national legislation require it, the Companies shall retain documents and information for an extended period, up to the maximum duration permitted by law. The documentation shall be available electronically or in paper format and be easy to access when necessary. Nordnet shall upon expiry of the retention periods, ensure that records are deleted.

7 Processing of personal data

The Companies are subject to the General Data Protection Regulation (GDPR), which applies to all processing of personal data in all countries where Nordnet operates. Sensitive personal data and personal data relating to criminal convictions and offences, may only be processed if necessary to comply with requirements set out by external rules to prevent ML/TF. Information used in monitoring deviant transactions/behavior submitted to the Financial Intelligence Units (FIUs), and such information request from the FIUs, may not be provided to the person registered.

8 Training of employees

All employees, contractors (working more than three months for Nordnet), and others who on similar grounds participate in the work against ML/TF, shall be trained annually in ML/TF issues and financial sanctions. For some parts of the organization, adapted training shall be applied. The program shall be adapted to the department's responsibility and function.

9 Protection of employees, contractors, or others and whistleblowing

The Companies shall have procedures and measures to protect employees, contractors, or others from internal or external threats, retaliation, or other hostile actions in connection to fulfilling their AML/CFT duties. In addition, the Companies shall ensure that reprisals do not strike employees due to reporting ML/TF issues.

The Companies shall have procedures and measures to protect employees, contractors, or others who report irregularities, i.e., whistleblowing possibility. The Companies shall ensure that reprisals do not strike employees because of such reporting.

10 Suitability assessment of employees

The Companies shall have procedures to ensure that all people assigned duties to AML/CFT, have a suitable background and understanding of ML/TF that is commensurate with their duties and

function.

11 Information exchange within the Nordnet group

Nordnet shall have procedures and guidelines for personal data protection and information exchange within the group to ensure that information about suspected ML/TF is shared between them, when necessary.