Nordea

AML/CTF Addendum

This addendum supplements the general terms and conditions governing your use of Nordea accounts and services. It outlines our expectations and your responsibilities in ensuring compliance with Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) regulations.
By accepting this addendum, you as Nordea's partner commit to supporting Nordea in its efforts to comply with applicable AML/CTF regulations when using Nordea accounts and services to deliver products and services to third parties.

1. Shared Responsibility and Commitment

Financial crime is a global challenge, and financial institutions play a critical role in detecting and preventing illicit activities. At Nordea, we are committed to ensuring that our services are not misused for illegal purposes. We expect our clients to share this commitment and to operate their accounts in a compliant and responsible manner, supporting Nordea's efforts to protect the financial system from abuse.

Our shared goal is to protect the financial system from abuse and to uphold the highest standards of integrity and transparency.

2. Know Your Customer (KYC) and Information Requests

To fulfill our regulatory obligations, we may request information about your organization, operations, and transactions. These requests may come from our relationship managers, KYC specialists, or compliance teams. You are expected to:

- Provide clear and timely responses to requests related to your customer relationships and activities.
- Share information about transactions on your Nordea accounts and the involved parties to the transactions.
- Report any unusual and suspicious activity on your Nordea accounts.
- Respond to requests for information about your direct customers, and make changes to your account activity if directed by Nordea.
- Notify us of any changes in your business that may affect compliance with applicable to you AML/CTF regulations.

Nordea

3. Licensing and Regulatory Compliance

You must maintain all necessary licenses and registrations required by law in each jurisdiction where you operate. This includes compliance with local regulations related to money transmission, payment services, and other financial activities. Additionally, you must adhere to Nordea's formatting and procedural requirements for payment processing.

You are required to comply with all applicable rules and regulations governing each payment method you utilize as well as any payment formatting requirements stipulated by Nordea.

4. Customer Due Diligence

You are responsible for implementing robust KYC procedures when onboarding and monitoring your customers on an ongoing basis. This includes, but is not limited to, risk-based due diligence, screenings and transaction monitoring to detect and report suspicious activity. Your controls should be proportionate to the size and complexity of your operations.

You must ensure your controls and transaction monitoring is dimensioned to facilitate both effective and efficient monitoring such that suspicious activity can be identified in a timely manner.

5. Information Sharing with Nordea

You must inform Nordea without undue delay of any sanctions, regulatory actions, or suspicious activities related to your customers. Such notifications should be made in writing to your relationship manager and may be followed up by telephone. This obligation is in addition to any legal reporting requirements you may have.

You are required, to the extent legally permissible, to report to Nordea activity in relation to your customers on behalf of whom you have transacted through Nordea Accounts that you have identified as warranting additional review by virtue of it being illegal, unusual, suspicious, or on the basis of any factor that indicates the activity may be outside of the risk tolerance detailed below or otherwise notified to you.

Such information sharing must be directed to your relationship manager in writing, but may be followed up by telephone. Nordea may contact you for additional information. Upon receipt of such notice, Nordea will make a separate assessment of whether the activity constitutes suspicious activity that Nordea must report to the relevant FIU.

Note that this reporting requirement is in addition to any reporting requirements you may be subject to under laws and regulations applicable to you.

Nordea

6. SWIFT Security Requirements

If you use SWIFT for communications, you must safeguard your credentials and infrastructure. Compliance with SWIFT's Customer Security Controls Framework (CSCF) is mandatory. You are responsible for ensuring that your systems are protected against fraud and unauthorized access.

Authenticated payment orders and other instructions will be deemed to be authorized by you as it is your responsibility to ensure that the security procedures and your funds transfer operations and systems are safeguarded and protected from compromise.

7. Prohibited Transactions

Your Nordea accounts must not be used for transactions involving illegal activities or entities lacking proper authorization. Examples of prohibited transactions include, but are not limited to:

- Transactions related to suspected or confirmed Fraud, money laundering, terrorist financing, tax evasion or sanctions violations.
- Transactions without a legitimate business purpose.
- Transactions related to any businesses that are known to be illegal based on applicable laws and regulations
- Payments involving unlicensed and/or unregulated financial service providers or shell banks.
- Transactions with anonymous or bearer share accounts, or gambling related transactions involving entities without proper licensing.
- Payments that would violate, or cause Nordea to violate, economic sanctions, export controls, or currency controls.
- Payments involving unauthorized, unlicensed and/or unregulated banks (direct and/or indirect relationships).
- Payments associated with payable through accounts, or involving third-party payment processors that do not have an adequate AML/CTF and Sanctions program in place.
- Payments involving any anonymous, alias or numbered customer or account (including anonymous passbooks or anonymous safety deposit boxes).
- WTR and Wire Stripping
- Transactions involving Virtual Asset Service Providers (VASPs) that are not registered/licensed as required in a local authority´s register to operate as a VASP
- Transactions involving entities that are considered outside of Nordea's Financial Crime risk appetite, assessed on a case-by-case basis

Nordea reserves the right to reject any such transactions if we have any reason to believe that the transactions pertain to these categories and to take any additional action.

Nordea

8. High-Risk Transactions (Conditional)

Certain transactions are considered high-risk and may only be processed if it is Nordea's view that you have adequate anti financial crime controls in place. These include transactions involving:

- Arms and dual-use goods, battlefield items, or economically critical goods.
- Precious metals from secondary sources.
- Charities, auctions, gambling, and crowdfunding platforms.
- Shipping and trading in free trade zones.
- Used motor vehicle dealers, embassies, consulates, and diplomatic missions.
- Cannabis-related businesses and adult-oriented services (where permitted by law).
- Payments involving transactions designed to achieve a particular tax treatment.
- Industries deemed as controversial and might have an adverse reputational effect on Nordea, assessed on a case-by-case basis

To the extent that your policies and controls are not capable of assuring that payments in these categories will not violate applicable laws and regulations or present an unacceptable level of financial crime or other compliance risk towards Nordea, you must not use your Nordea accounts for such transactions.

9. Transactions Requiring Nordea Approval

If you intend to process transactions involving additional entities in the transaction chain (e.g., downstream processing), you must notify your relationship manager and obtain written approval from Nordea before proceeding. This includes payments involving downstream processing for correspondent banks, Money Service Businesses (MSBs), non-banking financial institutions, VASPs, Payment Service Providers (PSPs) or other money transmitter that are not otherwise prohibited under this addendum.

Payments related to physical cash and other banknote handling that can be seen as cash equivalent including repatriation of funds to the Nordic countries also require prior written approval.

10. Termination and Enforcement

Failure to comply with the requirements outlined in this addendum may result in the rejection of payments or closure of your accounts. Nordea reserves the right to take any necessary action to ensure. We encourage open communication and proactive compliance to avoid such outcomes.

We appreciate your cooperation and commitment to responsible banking. If you have any questions or require clarification, please contact txb.banks.cash@nordea.com