



Policy on Combating Financial Crime for Arion bank

It is Arion Bank's policy to combat financial crime¹ and to prevent the misuse of the Bank's services and operations for such purposes. The Bank implements and upholds both domestic and internationally recognized standards in this regard, including those relating to international sanctions.

The objective of this Policy is to set out the approach the Bank takes to meeting its legal obligations according to Act No. 140/2018 on measures against money laundering and terrorist financing and Act No. 68/2023 on the execution of international sanctions and the freezing of funds. The Policy is implemented with more detailed rules and procedures.

The exploitation of the financial system for financial crime poses a clear risk to the integrity, proper functioning, reputation and stability of the Bank and the financial system as a whole. In order to reasonably prevent such misuse, the Bank takes the following measures.

- it regularly assesses financial crime risk, and takes appropriate measures to mitigate such risk;
- it maintains effective internal controls and independent compliance monitoring, and ensures the development of coordinated practices to support the sound implementation of this Policy, including through the implementation of a 'three lines of defense' model;
- it performs risk-based customer due diligence, including identifying and verifying customers and their beneficial ownership structures, and understanding the nature and purpose of business relationships, and assesses the financial crime risk posed by all customers;
- it performs Enhanced Due Diligence ("EDD") and enhanced monitoring on high-risk customers, and screens all customers and connected parties (e.g., beneficial owners) against lists of Politically Exposed Persons ("PEP");
- it maintains risk-based procedures for securing approval from the relevant Managing Director and consultation from the Compliance function regarding high risk customers;
- it screens customers and connected parties (e.g., beneficial owners) and international transactions against international sanctions lists, issued by the UN, EU, OFAC (USA), and HMT (UK), and if sanctioned persons are identified, the Bank rejects the business and freezes funds and economic resources in accordance with law;
- it maintains an efficient and safe framework for internal and external reporting of suspicions, including protection of involved employees, and manages communications with authorities in an efficient manner;
- it ensures that management is fully briefed on financial crime risks, that relevant employees regularly receive adequate training, and that they have ready access to advice and support;
- it strictly prohibits the falsification of books and records;
- it ensures payment transparency.

¹ Financial crime is any crime involving money, including but not limited to, money laundering, terrorist financing and the financing of weapons of mass destruction (proliferation), and financial sanctions.



Risk tolerance

The Bank intends to conduct business only with reputable customers who use its products, services, and related accounts for legitimate purposes, and whose identities can be determined and verified, and are responsive when concerns are identified in relation to financial crime related issues.

The Bank will not knowingly offer products or services to, or establish or maintain a relationship with:

- a party who engages in money laundering, the financing of terrorism or proliferation or is subject to international sanctions, as designated by the UN, EU, US OFAC, or UK OSFI, or who is otherwise considered to pose a high risk of using the Bank's products and services for illicit activities due to the person's real or perceived association with illicit activities;
- a party where the Bank is unable to determine or verify applicable information necessary to provide it with sufficient clarity to assess the financial crime risk presented by the relationship;
- a party who is an issuer of bearer shares or similar instruments, a shell bank or an unlicensed financial undertaking, or who provides services to such persons;
- a party that for other reasons pose an unacceptable risk of money laundering or financing of terrorism or proliferation.

The Bank shall not offer the following services:

- Anonymous or fictitious name accounts or transactions;
- Payable through accounts for correspondent banking.

The Bank reserves the right to reject any customer, payment or business that is not consistent with its risk appetite, including the right to reject facilitating payments to/from non-account holders where the Bank has strong reason to believe is linked to illicit activity.

Implementation

Based on this policy, the Bank has:

- Procedures for appointing a first line Managing Director responsible for AML/CFT²;
- Procedures for appointing a second line independent AML/CFT Compliance officer³;
- Procedures for assessing and mitigating the Bank's financial crime risk exposure;
- Procedures for customer due diligence, customer risk assessment and appropriate record keeping;
- Rules and procedures for the implementation and use of remote customer onboarding solutions;
- A policy and procedures on anti-bribery and corruption;
- Procedures, systems and controls for ongoing monitoring of business relationships, sanction screening, and the reporting of suspicious transactions;
- Appropriate employee screening, and initial and regular training for relevant employees;
- Supervision and the monitoring of compliance with the policy by an independent Compliance function.

Responsibility and reporting

The CEO ensures that applicable rules and procedures are implemented. Furthermore, the CEO ensures that management is committed to taking appropriate measures to detect and mitigate financial crime risk; including through the regular review of the Bank's financial crime risk assessment.

It is the responsibility of the Managing Director of each business unit to ensure that an adequate due diligence on their respective customers is performed and maintained, and to decide whether to accept

² AML/CFT is the abbreviation of Anti-Money Laundering and Combating the Financing of Terrorism and Proliferation.

The Managing director responsible for AML/CFT is the responsible person according to the Act 140/2018 paragraph 2 of article 34.

³ AML/CFT Compliance Officer according to the Act 140/2018 paragraph 3 of article 34 and EBA/GL/2022/05.



customers who are considered to pose higher risk with regards to this policy. The AML/CFT Compliance Officer shall be consulted regarding high-risk customers, where applicable, before decision is made.

The Managing Director of each business unit is also accountable for the accurate completion of the financial crime risk assessment, and for ensuring that identified risks are effectively managed on an ongoing basis. Moreover, it is the responsibility of Managing Directors to ensure that rules on anti-bribery and corruption are adhered to in their respective division, and to assess what gifts and gratuity is appropriate, in line with the Bank's anti-bribery and corruption policy. It is the responsibility of every employee to report any suspicious activities, and to keep such reports confidential.

The AML/CFT Compliance Officer is authorized to veto the execution of individual transactions not consistent with this Policy. Furthermore, the AML/CFT Compliance Officer can direct a Managing Director to reject or terminate relationships not consistent with this Policy. Such decision can be appealed to the CEO.

Managing Director responsible for AML/CFT

It is the responsibility of the Managing Director responsible for AML/CFT to ensure that measures and procedures and internal control measures put in place are adequate and proportionate, and that risks are managed effectively.

The Managing Director responsible for AML/CFT shall secure that the Executive Committee are provided with sufficient information to fulfil their responsibilities regarding this policy. The Managing Director responsible for AML/CFT shall report to the Executive Committee on any significant issues or breaches regarding ML/TF and provide recommendations on how to remediate them.

The Managing Director responsible for AML/CFT shall report at least annually to the Board's Risk Committee and at least annually to the Board of Directors.

AML/CFT Compliance Officer

It is the responsibility of the AML/CFT Compliance Officer to ensure the development of coordinated practices to support the sound implementation of this policy, by monitoring and regularly assessing the adequacy and effectiveness of the measures and procedures put in place.

It is also the responsibility of the AML/CFT Compliance Officer to oversee any activities which are suspected to be linked with financial crime, and to ensure reporting to the appropriate authorities any activities considered reasonably suspicious.

The AML/CFT Compliance Officer shall submit a report on financial crime risk at least semi-annually to the Board's Risk Committee and at least annually to the Board of Directors, as part of the regular Compliance reporting. The AML/CFT Compliance Officer shall inform the Board of Directors of the results of the financial crime risk assessment.

The policy comes into effect once published and shall be made available on the Bank's website.