Rules on measures against Money Laundering and Terrorist Financing

Chapter I: General

1. Purpose and Scope

It is Arion Bank's policy to combat money laundering and terrorist financing and to prevent the Bank's services from being used for these purposes. The Bank is aware that there is an unavoidable risk that the services it offers could be abused in this way. The Bank is also aware that inadequate measures can result in significant damage for the Bank, its shareholders and society as a whole. The Bank takes its responsibilities very seriously and places stringent demands on its employees in this respect.

These rules are based on the Bank's Policy on Combatting Financial Crime, the Anti Money Laundering and Terrorist Financing Act, the Implementation of International Sanctions Act, the Freezing of Funds Act and related regulatory acts, all of which are applicable to every employee of the company, including the board of directors.

Definitions of the terms used can be found towards the end of these regulations.

In addition to the above regulations, the Bank has adopted special Know Your Customer (KYC) Procedures.

2. Main Principles

We know our customers

Employees should know the identity of the customers to whom they provide services and should ensure that the Bank has sufficient information on the customer in question and potential stakeholders. If the customer is a legal entity the employee should try to find out the purpose of the legal entity and who its beneficial owners are. Employees should also try to find out and identify the purpose and nature of the business relationship.

When an employee checks the submitted ID and documents when performing due diligence, they should use their own judgement to make an independent assessment of the reliability of these documents. This means employees must be alert to the possibility of fake ID documents and must check that documents have been properly completed. Employees should also ensure that people representing customers have the proper authority to do so.

Ongoing monitoring

Employees should try to keep information on customers up to date. Information should be updated on a regular basis and employees should update information if they notice it is incorrect or insufficient. Employees should also check the current information, for example when changes are made the business relationship or if the customers asks for additional services.

Employees should endeavour to understand the nature and purpose of the transactions they are responsible for supervising and be alert to changes in trading patterns which may indicate a change in the nature of the business relationship.

Be alert

Employees should always be alert to unusual or suspicious transactions or conduct by customers and notify Compliance of any suspicion they may have that transactions may be linked to actions punishable by law, without letting the customer or a third party know that they have notified the incident.

Approved by CEO 22.07.2020

This is an English translation of the Icelandic original. In the event of any discrepancy, the Icelandic version shall prevail.

Cooperation

Measures against money laundering and terrorist financing are varied as it is necessary to adapt them to a wide range of circumstances. The Bank therefore places a strong emphasis on providing employees with training on the subject and direct access to advice and support from Compliance.

Employees should regularly obtain training on this subject and seek guidance, advice and support from Compliance as necessary. Employees should also not hesitate to inform their supervisors or Compliance of any possible improvements to procedures or risks they become aware of in their work.

Chapter II: Business Relationships

3. Due diligence

It is not permitted to establish a business relationship unless satisfactory due diligence has been performed on the other party in accordance with the KYC Procedures.

Due diligence is performed for multiple reasons. The main purpose is to acquire information so that the Bank is able to assess whether it is allowed to or wishes to have a business relationship with the party in question, with respect to the risk of money laundering or terrorist financing and international trade sanctions. The process involves acquiring certain basic information on the customer which is necessary for the Bank in order to maintain a normal business relationship and to meet its obligations to disclose information to the authorities. Finally, due diligence is designed to ensure that a person is who they say they are and that they are authorized to establish a business relationship.

When performing due diligence it is also necessary to acquire information on stakeholders related to the customer, such as authorized representatives and owners, as applicable.

The scope of due diligence and ongoing monitoring depends on the level of risk of money laundering or terrorist financing represented by the business relationship in question. Risk is assessed by taking a comprehensive look at different factors, such as the type of customer and nature of the business, what goods and services are involved, geographical risk etc. The purpose of the risk assessment is to improve efficiency by focusing attention on the main areas of risk.

Managing directors are responsible for ensuring that customers correspond to the Bank's risk appetite and that due diligence is carried out appropriately in accordance with laws and regulations. The Bank reserves the right to reject all business transactions if the Bank deems the risk to be higher than acceptable.

4. Restrictions on business transactions

The Bank has decided that certain types of business transaction and services shall be prohibited or limited and that the Bank's services will not be made available to certain types of customers.

It is not permitted to commence or continue business transactions:

- if it proves not to be possible to perform adequate due diligence;
- with parties who it is prohibited to do business with according to sanctions imposed by the United Nations, European Union, United Kingdom or United States;
- with parties who would constitute a significant reputational risk for the Bank on account of alleged links to criminal behaviour;
- with parties where there is a strong suspicion that they may misuse the Bank's services for the purpose of money laundering or terrorist financing, or if the party has given a false impression of itself, provided the Bank with forged documents or shown threatening behaviour towards employees;
- with parties who intend to appear under their own name on behalf of a third party;

- with shell banks (i.e. financial institutions which do not have actual operations) and financial institutions which permit shell banks to use their accounts or parties who provide financial services without the required licenses;
- with legal entities which issue shares in the form of bearer shares, without a shareholders' register containing the name of all bearers;
- with parties where for other reasons there is considered an unacceptable risk of money laundering or terrorist financing in respect of the Bank's risk tolerance.

It is also prohibited to act as an intermediary in a transaction if it is clear to the Bank that the transactions are linked to parties who come under the definitions given above. This means, for example, that it is prohibited to act as an intermediary in a transaction if it is clear to the Bank that a customer of the Bank has been tricked into sending money to a counterparty.

It is not permitted to offer customers anonymity in their transactions with the Bank and special care should be taken in the case of new technology or products which encourage anonymity, including product development at the Bank. It is completely prohibited to participate in or encourage transactions where the intention is to conceal beneficial ownership.

It is prohibited to do business with unknown persons, i.e. parties who are not in an ongoing business relationship with the Bank. Individual customers shall be permitted, however, to pay bills and exchange currency, including transactions with foreign currency, for amounts of up to ISK 500,000, and a maximum of the equivalent of €15,000 in total over a period 12 months. Unknown persons are not permitted to perform any money transfers In cases where the Bank does business with unknown persons, a record should always be made the name and ID number of the person as stated in a recognized ID document (or date of birth of person does not have an ID number).

It is prohibited to offer other financial institutions interbank services in the form of payable through accounts.

5. Termination of a business relationship

If a business relationship has already been established which contravenes the restrictions pursuant to Article 4, the business relationship should be terminated.

When deciding how to terminate the business relationship, account should be taken of events and risks at any given time, and the Bank's obligations under the Payment Services Act, in consultation with Compliance. In general the customer should be notified by verifiable means with two months' notice that no further transactions will be possible unless satisfactory information or explanations are provided within a specified time.

The Bank can decide to terminate the business relationship without notice if there is reasonable suspicion that the party in question:

- is subject to international trade sanctions;
- is involved in terrorist financing or organized crime, e.g. illegal arms sales, illegal production and distribution of narcotics, prostitution, human trafficking, illegal pornography or gambling or major embezzlement;
- has misused the Bank's services for the purpose of money laundering, terrorist financing or other criminal acts, has given a false impression of itself or provided the Bank with forged documents or shown threatening behaviour towards employees.

Section III: Regular monitoring and reporting requirements

6. Regular monitoring

The Bank shall conduct regular monitoring of contractual relationships with its customers and check transactions taking place during the contractual relationship to ensure they match the information at hand. In cases where there is considered to be a greater risk, enhanced regular monitoring shall be carried out.

It is the responsibility of each employee to be alert to whether transactions match the information at hand on the customer in question, including with regard to the scope, nature and purpose of the business relationship and the origin of the financial assets.

During regular monitoring it must be ensured that the Bank fulfils its obligations according to the International Sanctions Act No. 93/2008 and related government directives.

7. Transactions requiring special caution

Employees should show special caution with regard to unusual transactions, e.g. under the following circumstances:

- A person is reluctant to provide information, provides unreliable information, or shows an unusually keen interest in the performance of due diligence or monitoring by the Bank;
- A party repeatedly seeks to conduct their business so that the amount involved is below the level which is normally subject to checks;
- A person seeks to do a business transaction with the Bank even though this is highly impractical from a geographical standpoint;
- Transactions involving high amounts paid in cash;
- The transaction does not seem to serve any financial or legitimate purpose;
- The customer or the transaction is connected to high risk countries or regions;
- Transactions are unusual, large or complex in relation to the normal activities or information at hand on the customer, or the conduct of the customer or the transactions are unusual in any other way;
- The transactions, activities, ownership or organization of the legal person are unusual or ambiguous.

In the above circumstances, the employee shall assess whether there are grounds to report a suspicious transaction in accordance with Article 16.

8. Reporting requirements, stopping transactions and confidentiality

All employees are obliged to report any suspicious activities or transactions, if there is any suspicion that they are linked to illegal conduct. This is done through a special intranet form. The report should include a detailed description of the activity considered suspicious. There is no requirement to provide solid evidence or reasoning, and the employee does not need to express an opinion on what kind of criminal offence may lie behind the activity.

Business Compliance shall be informed of incidents where it has not proven possible to verify the reliability of the information at hand or the transactions are rejected for other reasons. Business Compliance evaluates whether the police should be notified under Article 9.

It should be avoided, as far as possible, to carry out transactions if there is any evidence or suspicion that they are connected to illegal conduct. If transactions have not been carried out, this should be mentioned in the report, and the transactions should not be carried out without consulting Business Compliance.

Employees may not under any circumstances inform the customer in question or other third parties that suspicions have been reported or that such report has been sent. An employee who dissuades a

customer from participating in illegal activity is not considered to have violated the ban on reporting information.

The Bank shall take appropriate measures to protect employees who report their suspicions in good faith against threats or other hostile actions which may be traced to such reports. The Bank is also prohibited from punishing an employee in any way for having reported their suspicions.

9. Investigations by Compliance and reports to the police

Business Compliance shall respond to all reports by employees of suspicious activities or transactions as quickly as possible. All reports should be investigated thoroughly as should the background to the transactions and the customer.

Business Compliance shall prepare a written report on each investigation into suspicious or unusual transactions, which should be sufficiently detailed to give a picture of the nature of the transaction and to be useable as evidence in a criminal case.

Business Compliance makes an independent assessment of the reports it receives and decides independently on whether the report should be referred to the police. The report to the police shall contain a detailed description of the conclusions of the investigation and a copy of all necessary information. The report should also specify the deadline for the Bank to carry out the transaction, if it has not been carried out, and it should be decided in consultation with the police whether the transactions should be carried out.

A report to the police should not contain the names or other ways to identify the persons who reported their suspicion and such information should not be divulged unless required to do so by law.

In accordance with a written request from the police investigating cases of money laundering or terrorist financing, Business Compliance should provide all necessary information relating to the report.

The Bank is permitted to share information in accordance with Article 27 (3) of Act No. 140/2018.

10. Freezing funds

It is mandatory to freeze funds and economic resources on the basis of the Freezing of Funds Act No. 64/2019, in accordance with regulations established on the basis of the Implementation of International Sanctions Act No. 93/2008, to prevent any kind of movement of capital, such as the handover of assets, withdrawals, transfers, registration of assets and other transactions, and thereby prevent parties on the list of sanctions from receiving payment or being able to use assets in another way.

When freezing funds, Compliance shall immediately notify the owners, the minister of foreign affairs and the Central Bank's Financial Supervisory Authority of what measures have been taken.

Chapter III: Internal organization

11. Risk assessment

Compliance shall ensure that the Bank performs a risk assessment of its business and its transactions, assessing the risk that its products and services will be misused for the purpose of money laundering or terrorist financing. The assessment shall contain a written analysis and evaluation of risk which shall, among other things, take into account risk factors linked to customers, trading partners or regions, products, services, transactions, technology or distribution channels. The risk assessment shall use as a reference the risk assessment report of the National Commissioner of Police.

The risk assessment shall be updated bi-annually or more often as needed. A risk assessment shall always be performed before new products or services are marketed and when new distribution channels and technology are launched.

12. Procedures

Management is responsible for the implementation of these rules in the relevant division/department, with the appropriate procedures and processes and supervisory measures.

13. Hiring employees

When hiring employees a check should be performed of the applicants' educational and professional backgrounds, their criminal record and other factors relevant to assessing whether the person is in a position which makes it more likely for them to be linked to illegal conduct.

14. Training

Management shall ensure that their employees receive proper and regular training on measures against money laundering and terrorist financing and these rules when they take up their jobs.

Employees engaged in providing financial services, directly or indirectly, should receive sufficient training in accordance with the following:

- New employees should study the Bank's measures against money laundering and terrorist financing as part of new recruit training;
- All employees involved in providing financial services should be sent an online presentation and pass an online test on the subject of these rules annually;
- All frontline employees should go on a special course on measures against money laundering and terrorist financing at least every two years;
- Employees should receive appropriate training when changes to the relevant rules or procedures occur.

This training should ensure that employees know their and the Bank's obligations in respect of measures against money laundering and terrorist financing and the consequences of failing to keep these obligations. Employees should also be informed of the key methods of money laundering and terrorist financing, where the main risks lie, the main clues which may give rise to suspicion and how to respond, and should be kept up-to-date on the main developments in this area.

15. Storing and processing data

The storage and processing of personal data in respect of measures against money laundering and terrorist financing shall accord with the Data Protection Act, see Articles 28 and 29 of Act No. 140/2018.

Information on customers and transactions should be stored securely and in an organized manner to ensure there is an adequate overview of information and that queries from the authorities can be responded to promptly. It should be ensured that there is sufficient information for the authorities to see how due diligence on a customer was performed and how individual transactions were carried out.

Relevant information should be stored for at least five years after the end of the business relationship or occasional transactions occurred. Reports and requests for information from the police in connection with investigations into suspicions of money laundering or terrorist financing, and other dealings with the authorities in connection with investigations into suspicions of money laundering or terrorist financing, shall be kept for at least five years.

It is permitted to share information on customers which was acquired in accordance with these rules within the Bank Group, in accordance with the purpose of these rules and in compliance with the conditions of the Icelandic Data Protection Act. It is also permitted to share information with third parties on the basis of a written agreement.

All employees are permitted to have access to information acquired when performing due diligence. Access to information concerning investigations into suspicious transactions and reports to the police shall be limited to the CEO, employees of Compliance and Internal Audit, unless the law states otherwise.

16. Compliance Officer

The Bank is responsible for ensuring that its employees comply with the Anti Money Laundering and Terrorist Financing Act and these rules. The board of directors shall confirm the appointment of the Compliance Officer as a person responsible pursuant to Act No. 140/2018, and their deputy.

Compliance shall monitor the implementation of these rules and shall ensure that coordinated working methods are adopted which support the implementation of measures against money laundering and terrorist financing in accordance with the law and relevant standards. Compliance shall also be in charge of employee training.

The Compliance Officer shall oversee any activities which are suspected to be linked with financial crime, and ensure that any activities considered reasonably suspicious are reported to the appropriate authorities. The Compliance Officer can recommend that transactions be stopped, that a business relationship is rejected or ended due to the risk of money laundering or terrorist financing. A decision shall be referred to the CEO if the Compliance Officer's recommendation is not followed. The board of directors shall be informed of decisions taken contrary to the opinion of the Compliance Officer.

The Compliance Officer shall ensure that the senior management of the Bank is adequately informed of the risks relating to money laundering and terrorist financing so that it is able to take appropriate measures to reduce and manage such risks.

The Compliance Officer shall provide the board with a report on these rules as often as deemed necessary, but not less than once a year. The board appraises the report and makes recommendations for corrective action, as necessary.

The authority and obligations of Compliance are described in more detail in the Policy on Combatting Financial Crime and the Compliance Officer's Charter.

17. Penalties

Any violation of these rules could result in a warning or the dismissal of the employee, as well as public penalties.

18. Publication, validity and review

These rules are published on the Bank's intranet and come into force when approved by the board.

The rules shall be reviewed as often as necessary, but not less than annually.

19. Definitions

In these rules these terms have the following meanings:

1. Money laundering: Actions by which a natural or legal person accepts or acquires, either for itself or others, proceeds by means of an act punishable by law, see definition in Act No. 140/2018. The person in question does not need to have participated in the initial criminal act, nor does the initial criminal act need to have taken place within Icelandic jurisdiction.
2. Terrorist financing: The collection of funds with the intention or knowledge that they are to be used for the purpose of carrying out a terrorist act, i.e. an offence which is punishable pursuant to Article 100 a.-c. of the General Penal Code.
3. Shell bank: A credit institution or other entity with similar activities founded within a jurisdiction where it has no genuine business activity or management and which is not connected to any financial group subject to supervision.
4. International sanctions: Sanctions in which Iceland is a participant on the basis of the International Sanctions Act No. 93/2008, and other international sanctions specified in the Bank's policy, i.e. sanctions by the EU, the US and UK.