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 rules are based on the Bank's policy on measures against money laundering and terrorist financing and the Measures against Money Laundering and Terrorist Financing Act No. 64/2006 and related government regulations.

The obligations stipulated in these rules apply to all employees and board directors of the Bank.

2. Definitions

For the purpose of these rules the following definitions shall apply:

- Money laundering: Actions by which a natural or legal person accepts or acquires, either for itself or others, proceeds by means of a violation punishable by law, see definition in Act No. 64/2006. The person in question does not need to have participated in the initial violation, nor does the initial violation need to have taken place within Icelandic jurisdiction.
- Terrorist financing: The collection of funds with the intention that they should be used or in the knowledge that they are to be used for the purpose of carrying out an act of terrorism, i.e. an offence which is punishable pursuant to Article 100 a.-c. of the General Penal Code.
- Approved identification documents: Identification documents with a photo issued or approved by the government and which are valid when shown, including passports, driving licenses, identity papers issued by the National Register and electronic authentication documents containing qualified electronic certificates. A certified copy of an approved identification document confirmed by a notary public or qualified public authority has the equivalent value of the original of the identification document.
- Beneficial owner: A natural person (one or more) who ultimately owns or controls the customer, directly or indirectly, e.g. a party which has a shareholding or voting rights of 25% or more in the legal person.
- Distance selling: When a business relationship is established without the customer providing identification in person, i.e. if establishing the business relationship by mail, telephone or the internet.
- Exposed persons: Natural persons subject to international sanctions or natural persons resident outside Iceland and who have been entrusted with prominent public functions, as well as their immediate family members and close associates. Prominent public functions in this context refer, for example, to influential politicians, judges, people in senior administrative positions and high-ranking persons in state-owned enterprises, cf. further definition in Regulation No. 811/2008.
- Correspondent banking business: When a foreign bank is provided with banking services which enable it to provide its customers with goods and services which it could otherwise not provide, with Arion Bank acting as intermediary.

- 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.

3. Main principles

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.

Employees should ensure that people representing customers have the proper authority to do so.

Employees responsible for supervising business relationships with a legal person should endeavour to understand the purpose and ownership structure of the legal person and to get to know the individuals who actually manage the legal person.

Employees should make an effort 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.

Employees should always be alert to unusual transactions or unusual conduct by customers and notify Compliance of any suspicion they may have that transactions may be linked to actions punishable by law.

CHAPTER II: DUE DILIGENCE

4. General information on due diligence

Due diligence refers to the obtaining of information on a customer and the independent verification of this information, in order to ensure that the customer is the person they say they are and that the Bank understands the nature of the business relationship.

The managing director shall ensure that due diligence is performed on the customers of the relevant division in accordance with these rules and that further information is obtained as warranted.

It is not permitted to establish a permanent business relationship unless due diligence has been performed which meets the requirements of these rules.

It is not permitted to carry out transactions with persons who are not in a permanent business relationship with the Bank, if the transaction is the equivalent of €15,000 or more, or the equivalent of €1,000 or more in the case of a transaction with foreign currency, or transferring financial assets, in the case of single transactions, whether this involves the transfer of assets domestically or cross-border, amounting to ISK 150,000 or more based on the officially posted exchange rate at any time, unless due diligence has been performed which meets the requirements of these rules.

If a person is already in a permanent business relationship when these rules come into effect, no changes should be made to the business relationship unless the available information meets the conditions of these rules. Changes to the business relationship include all types of loan, opening new accounts and issuing payment cards.

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 during product development at the Bank.

It is permitted to pass on information on customers which must be kept in accordance with these rules within the Group, in keeping with the purpose of these rules and compliance with the conditions of the Icelandic Data Protection Act.

5. Cases where due diligence shall be performed

Due diligence must be performed in the following cases:

- At the beginning of a permanent business relationship with a specific department at the Bank;
- If the available information is insufficient or there is doubt as to whether it is correct or reliable;
- If the person who is not in a permanent relationship with the Bank intends to carry out a transaction equivalent to €15,000 or more, or the equivalent of €1,000 or more in the case of a transaction with foreign currency, whether the transaction is carried out in a single operation or in several operations which appear to be linked;
- When transferring financial assets, in the case of occasional transactions, whether this involves transfers of financial assets domestically or cross-border, amounting to ISK 150,000 or more based on the officially posted exchange rate at any time.
- If there as any suspicion of illegal conduct, regardless of any exemptions or restrictions.

If there is reason to suspect that the proposed transaction is for the benefit of a person other than the customer, information must be obtained on who that person is and due diligence must be performed on the person in question before the transaction is carried out. However, it is permitted to open a fiduciary account for attorneys and brokers of real estate, companies and shipping vessels even if it is not divulged on whose behalf the account is opened, provided that the account is specifically identified as such an account.

A person is permitted to open a gift account for a third party without due diligence having been performed on the third party, provided that payments cannot be made from the account before due diligence has been completed. The name and ID-No. of the person opening the account on behalf of the customer must always be recorded, or a due diligence performed, depending on the size of the transaction.

The start of a permanent relationship on the basis of an agreement on private pension savings or additional insurance coverage shall be considered to be the date of the first payment from the Bank. Due diligence shall then be performed on the recipient.

6. Due diligence of natural persons

6.1. Acquiring information

When performing due diligence the correct name, ID-No. and address of the person shall be recorded, if the Bank does not already have this information on record.

No further information, or verification of the information, is requested in the case of issuing gift cards, currency cards or other non-refillable digital currency, where the total amount is below €250.

In other cases, it must be checked whether the Bank has a record of the correct information on the person’s nationality, job, phone number and e-mail address, if applicable, sample of handwriting and information on the purpose of the transaction.

6.2. Verifying information

A natural person shall prove their identity by showing approved identification documents, of which a copy should be taken, or sufficient electronic identification, if this has not already been done. The address provided should also be verified by looking it up in the National Registry.

- If the address is not listed in the National Registry, the person concerned shall provide material confirming the address, such as a bill from a reliable source which is issued to the name and address of the person concerned.
- If the person is not resident in Iceland it should be established whether that person is considered an exposed person.

The Bank may make additional requirements with respect to acquiring or verifying information under Article 8 before it is permitted to establish a business relationship.

7. Due diligence on legal persons

7.1. Acquiring information

When performing due diligence on legal persons, the correct name, ID-No, address, phone number and e-mail address, if applicable, shall be recorded, if the Bank does not already have this information on record.

No further information is required if it has been confirmed that the legal person in question is:

- A financial institution, life assurance company or similar legal person which has been granted an operating licence in the European Economic Area (EEA). The same applies to regulated financial institutions from countries outside the EEA which are subject to similar requirements as those stipulated in Act No. 64/2006;
- A company which has listed financial instruments on a regulated securities market within the EEA;
- An Icelandic central or local government authority.

In other cases, information on the following is also required:

- The name and address of each board director, managing director, authorized representative and others who represent the legal person when dealing with the Bank, in addition to confirmation that these people have the requisite authority to represent the legal person;
- detailed information on the management and ownership structures, including the names and addresses of all persons considered to be beneficial owners;
- information on the purpose of transactions.

Persons who are authorized to represent the legal person in dealings with the Bank shall prove their identity by showing approved identification documents, of which a copy should be taken, or sufficient electronic identification, if this has not already been done.

7.2. Verifying information

An independent assessment shall be made of whether the information on the legal person and beneficial owner is correct and sufficient.

The existence of a legal person shall be proven by presenting a certificate from the Register of Companies, or similar public register or information from a recognized database which retrieves

information from such an official register, showing the name, ID-No. and address of the legal person, or similar information.

- Information may not be older than three months when performing due diligence.
- In the event a legal person is unable to produce the aforementioned certificate it is sufficient to verify the name, ID-No. and address by printing this information from the website of the Register of Companies at the Icelandic Directorate of Internal Revenue.
- If the legal person is not registered on the website of the Register of Companies at the Icelandic Directorate of Internal Revenue, a request should be made for the articles of association, memorandum of association or similar document, which states the name and address, or confirmation of this by a competent authority, as applicable.

Any doubt over the existence of a legal person should be investigated, such as by making a request for confirmation by a public authority, acquiring information on previous banking transactions, visiting the customer or verifying by other means that the legal person has not ceased its activities.

Information provided on ownership should be compared with the latest information from a public register, a recognized database or annual financial statement, as applicable.

If the administrative or ownership structure is not clear from the material presented, a request shall be made for further details or material, such as the articles of association, memorandum of association or similar document, the last annual financial statement, information on another agreement between the owners and/or confirmation from a competent authority, as applicable.

If a natural person who is authorized to represent the legal person in dealings with the Bank, or who is considered to be the beneficial owner, is not resident in Iceland, it should be ascertained whether this person is considered to be an exposed person.

The Bank may make additional requirements with respect to acquiring or verifying information under Article 8 before it is permitted to establish a business relationship.

8. Enhanced due diligence

Enhanced due diligence requirements shall be made in the following cases owing to increased risk of money laundering and terrorist financing:

- Distance selling;
- The customer seems to be an exposed person as result of political connections or international sanctions;
- Cross-border correspondent banking business with persons from non-EEA states;
- Transactions which are in other respects considered to represent a greater risk, with respect to the nature of the customer, the nature of the transaction or services and/or due to links with risky areas.

It should be recorded specially that the customer is subject to enhanced due diligence requirements.

8.1. Distance selling

Commencing a business relationship through distance selling is conditional on the person in question making the first payment in their own name through an account opened in the customer's name with a credit institution in a state which makes at least as strict requirements as in Iceland in respect to measures against money laundering and terrorist financing.

The customer should prove their identity with a certified copy of an identification document confirmed by a notary public or qualified public authority or with adequate electronic identification. The same applies to those who are authorized to represent the legal person in dealings with the Bank.

8.2. Politically Exposed Persons

If a person appears to be an exposed person due to political connections or international sanctions, the necessary information should be acquired to establish whether this is the case.

Contractual relationships or business transactions with persons who are considered to be exposed due to political connections require the prior approval of the relevant managing director and compliance officer. The same applies for the permission to continue the business relationship if the customer subsequently becomes an exposed person due to political connections. Appropriate measures should also be taken to verify the origin of the financial assets which will be used in the person's transactions, such as by acquiring information on the person's assets and income.

Compliance should be notified immediately in accordance with Article 15 if it transpires that the person is subject to international sanctions and all transactions which such person are conditional on the approval of Compliance.

Due diligence of exposed persons shall be reviewed at least every 12 months.

The above also applies to contractual relationships or transactions with legal persons where the person authorized to represent the legal person or considered to be the beneficial owner appears to be an exposed person.

8.3. Correspondent banking

Establishing cross-border correspondent banking business with non-EEA states is conditional on the prior approval of the relevant managing director and compliance officer.

Due diligence of persons engaged in correspondent banking business shall be reviewed at least every 12 months.

It is not permitted to establish or continue correspondent banking business with shell banks or financial institutions which permit shell banks to use their accounts.

8.4. Other transactions considered to represent higher risk.

The compliance officer may decide that special additional measures should be taken when performing due diligence, either general measures or in respect of occasional transactions, where the transaction in question is considered to represent increased risk with respect to the nature of the customer, nature of the transaction or service and/or connections to risky areas.

Such measures may include the following:

- The requirement for more information on the customer and the origin of the capital and/or more enhanced requirements on verifying the information provided or the frequency of reviewing the information provided;
- The requirement that the first transaction in the business relationship is made in the name of the customer in question and from an account which they have opened in a functioning financial institution in a state which makes as strict requirements as in Iceland in respect to measures against money laundering and terrorist financing;

- The requirement for the prior approval of a supervisor and/or compliance officer.

9. Postponing verification of information

In the following cases it is permitted to postpone verifying the reliability of information. Note that this does not authorize the postponement of acquiring appropriate information, but only the verification of this information.

In cases where a natural person is not competent to manage their affairs due to their age, it is permitted to postpone verifying the reliability of information until the person becomes legally competent, provided there is little risk of money laundering or terrorist financing.

Compliance is permitted to grant a temporary postponement of verifying the reliability of information in respect of a permanent contractual relationship, where this is necessary in order not to disrupt the normal course of business and there is considered little risk of money laundering or terrorist financing. Compliance shall keep a record of applications for postponements and support for each postponement granted.

If a temporary postponement is granted, the reliability of the information shall be verified as quickly as possible, and no later than four weeks after postponement was granted, unless special circumstances justify a longer postponement.

If it has not been possible to verify the reliability of the information within the period granted, appropriate measures should be taken in accordance with Article 11.

10. Exemptions

In exceptional cases, if necessary and if there is little risk of money laundering or terrorist financing, the compliance officer can permit the verification of the reliability of certain information on a natural person by other means than described in these rules, provided the compliance officer is of the opinion that this method is equally reliable.

Compliance can also allow information on a natural person not to be verified if this is necessary owing to the health of this person and on condition that this person has been in a permanent business relationship with the Bank when these rules come into effect and there is little risk of money laundering or terrorist financing.

Compliance may also allow, in the absence of a permanent business relationship, information not to be verified, provided that it is confirmed that payment for a transaction will be debited from a business account in the name of the customer at a functional financial institution or similar legal persons who have been granted an operating licence in the European Economic Area (EEA), and there is little risk of money laundering or terrorist financing.

Finally, Compliance is permitted to grant an exemption from performing due diligence, if similar information is provided by a financial institution which has been granted an operating licence in a state which makes as strict requirements as in Iceland in respect to measures against money laundering and terrorist financing, and a written agreement has been made with the financial institution in question which guarantees that necessary information will be made available to the Bank immediately, if so requested.

Compliance should keep a record of how such authorization has been exercised and the reasoning provided in each case.

11. Response if reliability of information cannot be verified

If it is not possible to verify the reliability of the information provided, it is not permitted to perform a transaction or establish a permanent business relationship. If a business relationship has already been established, it must be terminated immediately.

Compliance should be notified of cases in which it has not been possible to verify the reliability of the information provided and will assess whether there are grounds to notify the police in accordance with Article 15.

CHAPTER III: REGULAR MONITORING AND REPORTING REQUIREMENTS

12. Regular monitoring

The Bank should conduct regular monitoring of contractual relationships with their customers to ensure they match the information provided.

It is the responsibility of each employee to be alert to whether transactions match the information provided 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.

In order to conduct successful regular monitoring it is important that information on the Bank's customers is updated for the duration of the business relationship and further information is acquired as necessary and that suspicious transactions are reported to the compliance officer in accordance with Article 15.

Regular monitoring shall ensure that the Bank fulfils its obligations according to the International Sanctions Act No. 93/2008 and related government directives.

13. Enhanced regular monitoring

In cases where enhanced requirements are made on due diligence, enhanced regular monitoring shall be performed in accordance with procedures approved by the compliance officer.

Enhanced regular monitoring may include:

- More frequent review of due diligence
- Enhanced regular monitoring with transactions by the relevant person.

Compliance is authorized to decide that certain persons shall temporarily be subject to enhanced regular monitoring, for example, due to notifications of suspicious transactions or investigations by the authorities.

14. Transactions requiring special caution

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

- A person is reluctant to provide information, provides unreliable information, or shows unusually keen interest in the performance of due diligence or monitoring by the Bank;
- A person repeatedly seeks to conduct their business so that the amounts involved are less than the equivalent of €15,000, the equivalent of ISK 150,000 in transfers or the equivalent of €1,000 in the case of foreign currency transactions.

- 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 transaction is connected to high risk countries or regions;
- Transactions are unusual, large or complex in relation to the normal activities or information provided on the customer, or the conduct of the customer or the transactions are unusual in any other way.

In the above circumstances, the employee shall assess whether there are grounds to notify Compliance in accordance with Article 15.

15. Reporting requirements, stopping transactions and confidentiality

All employees are obliged to notify Compliance in writing of any suspicious activities or transactions, if there is any suspicion that they are linked to illegal conduct. The report should state the name of the employee sending the report, the name and ID-No. of the person being reported and 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 crime may lie behind the activity.

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 to Compliance, and the transactions should not be carried out without consulting 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.

16. Investigations and reports to the police

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.

Compliance shall compile 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.

Compliance makes an independent assessment of the reports it receives and takes an independent decision 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. It should also state what the deadline is before which the Bank can 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.

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

CHAPTER IV: INTERNAL ORGANIZATION

17. Procedures

Managing directors are responsible for the implementation of these rules in the relevant division, with the appropriate procedures and processes.

18. Protection of employees

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

The Bank shall take appropriate measures to protect employees who report their suspicions from threats or other hostile actions which may be traced to such reports.

19. Employee screening

When hiring employees a check should be performed of the applicants' educational and professional background, 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.

20. 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 involved in providing financial services, directly or indirectly, should receive sufficient training in accordance with the following:

- New employees should attend a presentation for new employees and declare they will study the Bank's rules;
- Employees should receive on online presentation and pass an online test on the subject of these rules;
- All frontline employees should participate in 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 do so. Employees should also be informed of the key methods of money laundering and terrorist financing, where the main risks are, the main clues which may raise suspicion and how to respond, and should be kept up-to-date on the main developments in this area.

21. Storing information

Information on customers and transactions should be stored securely and in an organized manner, so that there is an adequate overview of information and 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.

Appropriate information should be stored for at least five years after the end of the business relationship or individual transactions occurred.

Compliance 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.

22. Compliance Officer

The Bank is responsible for ensuring that its employees comply with Act No. 64/2006 and these rules. The board confirms the appointment of a compliance officer as a money laundering reporting officer (MLRO) in accordance with Article 22 of Act No. 64/2006, and a deputy MLRO.

The compliance officer shall monitor the implementation of these rules and shall ensure that coordinated working methods are devised which support the implementation of measures against money laundering and terrorist financing in accordance with the law and relevant standards. The compliance officer shall investigate all reports of suspicious conduct pursuant to Article 15, send reports to the police pursuant to article 16 and be responsible for dealings with the authorities concerning measures against money laundering and terrorist financing and ensure the effectiveness of such dealings. The compliance officer shall also be responsible for employee training on the basis of a training schedule which should be reviewed on an annual basis.

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 authorization and obligations of the compliance officer are described in more duty in the Charter for Compliance.

23. Penalties

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

24. Publication, validity and review

These rules are published on the Bank's intranet and come into force upon publication.

The rules shall be reviewed as often as necessary, but not less than every two years.