LATVIJAS BANKA
EIROSISTĒMA

K. VALDEMĀRA IELA 2A • RĪGA • LV-1050 • LATVIJA • TĀLRUNIS +371 67022300 • FAKSS +371 67022420 • E-PASTS INFO@BANK.LV • WWW.BANK.LV

30 October 2017 Regulation No. 158
Riga

Requirements for the Prevention of Money Laundering and Terrorism Financing in Purchasing and Selling Cash Foreign Currencies

Issued pursuant to
Paragraph 1^1 of Section 7 and Paragraph 3 of Section 47 of the
Law on the Prevention of Money Laundering and Terrorism Financing

I. General provision

1. The Regulation establishes requirements to be met by capital companies holding a licence issued by Latvijas Banka for buying and selling cash foreign currencies (hereinafter, the capital company) to fulfil their duties under the Law on the Prevention of Money Laundering and Terrorism Financing in relation to the money laundering and terrorism financing risk assessment, the internal control system and its establishment, customer due diligence and monitoring of customer transactions.

II. Money laundering and terrorism financing risk assessment

2. The capital company, in accordance with its type of operation, shall carry out the money laundering and terrorism financing risk assessment and document this assessment to identify, assess, understand and monitor money laundering and terrorism financing risks intrinsic to its operation and customers. The money laundering and terrorism financing risk assessment shall be approved by the capital company's Board, where one exists, or by the highest administrative institution of the capital company.

3. The money laundering and terrorism financing risk is a possibility that the capital company may be used in money laundering or financing of terrorism.

4. The capital company, when carrying out the money laundering and terrorism financing risk assessment, shall take into account the risks identified by the European Commission in the European Union risk assessment, the risks identified in the National Report on Money Laundering and Terrorism Financing Risk Assessment as well as other risks specific to the operation of the respective capital company.

5. The capital company, when carrying out the assessment of money laundering and terrorism financing risk inherent in it, shall take into account the risks arising from the performed and planned transactions of purchasing and selling foreign currencies by the capital company, considering both the risk peculiar to the sector of purchasing and selling foreign currencies and the intrinsic risks of the capital company itself. At least

the following information shall be used in the assessment of the money laundering and terrorism financing risk inherent in the capital company:
5.1 the volume and value of transactions performed and planned by the capital company;
5.2 the volume and value of transactions performed by the capital company without identifying the customer;
5.3 the analysis of the factors affecting the money laundering and terrorism financing risk related to the capital company's customers, their states of residence (registration), customers' business or personal activity, the services and products used and their supply channels as well as the transactions performed; the analysis shall cover the following factors affecting the risk:
5.3.1 the customer risk inherent in the customer, including the situations where the customer is a legal person or legal arrangement, its legal form and the structure of owners as well as business or personal activity of the customer and its beneficial owner;
5.3.2 the country and geographical risks, including the risk where the customer or its beneficial user is associated with the country or territory whose economic, social, legal or political circumstances may point to a high money laundering and terrorism financing risk inherent in the country;
5.3.3 the risk of the services used by the customer, i.e. the risk that the customer can use the service of purchasing and selling cash foreign currencies for money laundering or terrorism financing;
5.3.4 the risk of the way services are provided is associated with the way the customer receives or uses the service of purchasing and selling cash foreign currencies.

6. The most important customer-related driving factors of the money laundering and terrorism financing risk are as follows:
6.1 business relationship with the customer is maintained or an occasional transaction with the customer is performed in unusual circumstances;
6.2 the customer is a legal person or legal arrangement that is a company managing private assets;
6.3 the customer is a legal person that issues or is entitled to issue bearer shares (equity) or has nominal shareholders;
6.4 the customer performs large-value transactions on a regular basis;
6.5 the structure of owners or participants of the customer, which is a legal person or legal arrangement, seems to be unusual or too complicated, taking into account its business model;
6.6 the customer is a legal person or legal arrangement whose structure of owners or participants makes it difficult to determine its beneficial owner;
6.7 the customer is an association, foundation or equivalent legal arrangement that does not make profit.

7. The most important driving factors of the money laundering and terrorism financing risk associated with the customer's business or personal activity are as follows:
7.1 the customer's business or personal activity is not related to the Republic of Latvia;
7.2 the customers' business activity is related to:
7.2.1 organisation of gambling;
7.2.2 delivery of cash collection services;
7.2.3 intermediation in real estate transactions;
7.2.4 trade in precious metals and precious stones;
7.2.5 trade in weapons and ammunition;
7.2.6 delivery of cash services.

8. The most important driving factors of the money laundering and terrorism financing risk associated with the country or geographical coverage are as follows:
8.1 the country or territory indicated in reliable sources, e.g. in a mutual assessment or precise assessment reports, or referred to in inspection reports as a country with no appropriate systems for the prevention of money laundering and terrorism financing, including the country that appears on the list of non-cooperating countries drawn up by the international Financial Action Task Force or about which the above organisation has published a statement saying that the respective country or territory has no legislative acts to combat money laundering or terrorism financing or mentioning that the relevant legislative acts of the country or territory have substantial deficiencies and therefore they fail to meet international standards;
8.2 the country or territory subject to sanctions, embargo or similar measures, including financial or civil restrictions imposed by, e.g. the United Nations, the European Union or the United States;
8.3 the country or territory indicated in a reliable source as a country having a considerable level of corruption and that of other criminal activities;
8.4 the country or territory indicated in a reliable source as a country or territory providing finance or support to terrorist activities or in which terrorist organisations indicated in a reliable source are active;
8.5 the country or territory included in the list of low-tax and tax-free countries and territories approved by the Cabinet of Ministers.

9. The driving factors of the money laundering and terrorism financing risk associated with the services used by the customer or related to the way services are provided are as follows:
9.1 occasional transactions without identifying the customer;
9.2 offsite business relationship or occasional transactions.

10. The most important factors mitigating the money laundering and terrorism financing risk which are related to the customer's state of residence (registration) where its business or personal activity is performed are as follows:
10.1 effective systems for the prevention of money laundering and terrorism financing are operational in the country;
10.2 the requirements established in the country in the field of combating money laundering and terrorism financing meet the international standards set by the organisations establishing standards for the prevention of money laundering and terrorism financing, and the country actually implements the above requirements;
10.3 the risk of corruption is low in the country;
10.4. the level of the criminal offences resulting in obtaining resources through criminal activity is low in the country.

11. The capital company, in accordance with the money laundering and terrorism financing risk inherent in it, shall revise and update the money laundering and terrorism financing risk assessment on a regular basis but at least once every three years. The capital company shall revise and update the money laundering and terrorism financing risk assessment in each case before it intends to introduce changes in its operational processes, management structure, the services and products provided, supply channels of services and products, pool of customers or geographical regions of operation, including prior to the introduction of new technologies or services.

III. The internal control system and its establishment

12. The capital company, based on its latest money laundering and terrorism financing risk assessment, shall establish the internal control system for the prevention of money laundering and terrorism financing (hereinafter, the internal control system), including the development and documentation of the respective policies and procedures which shall be approved by the capital company's Board, where one exists, or by the highest administrative institution of the capital company.

13. The internal control system is a set of measures implemented by the capital company, and it includes activities aimed at ensuring the implementation of the requirements laid down in the Law on the Prevention of Money Laundering and Terrorism Financing, providing adequate resources for the above and carrying out staff training to prevent, as far as possible, the involvement of the capital company in money laundering or terrorism financing.

14. When establishing the internal control system, the capital company shall incorporate therein and document the following:
14.1 the procedure for the assessment of the capital company's money laundering and terrorism financing risk and the procedure for the assessment, documentation and revision of the money laundering and terrorism risk associated with the customer, its state of residence (registration), the customer's business or personal activity, the services and products used and their supply channels and the money laundering and terrorism financing risk related to the transactions performed;
14.2 the procedure for and extent of customer due diligence to be carried out based on the customer's money laundering and terrorism financing risk assessment by the capital company and in compliance with the minimum customer due diligence requirements laid down in the Law on the Prevention of Money Laundering and Terrorism Financing and in other legislative acts;
14.3 the procedure for monitoring customer transactions;
14.4 the procedure for the identification of unusual and suspicious transactions;
14.5 the procedure under which the capital company shall refrain from conducting the transaction associated with money laundering or terrorism financing or there are reasonable grounds to suspect that the transaction or the funds involved therein are linked to money laundering or terrorism financing, or there are reasonable grounds to suspect that the funds involved in the transaction have been directly or indirectly derived from a criminal offence or related to terrorism financing or an attempt to commit this criminal offence.
14.6 the procedure under which the capital company shall report unusual and suspicious transactions to the Office for Prevention of Laundering of Proceeds Derived from Criminal Activity;
14.7 the procedure under which the capital company shall store and destroy the information and documents obtained as a result of customer due diligence and monitoring of the transactions performed by the customer;
14.8 the rights, obligations and responsibility of the capital company's staff as well as the standards of their professional qualification and adequateness when fulfilling the requirements stipulated by legislative acts regulating the prevention of money laundering and terrorism financing;
14.9 the procedure under which the capital company shall ensure anonymous internal reporting on infringements of requirements of legislative acts regulating the prevention of money laundering and terrorism financing and the assessment of such reports if,

taking into account the number of employees in the capital company, such reporting is possible;
14.10 an independent internal audit function to ensure the compliance of the capital company's internal control system with the requirements of the legislative acts regulating the prevention of money laundering and terrorism financing and to ensure the assessment of operational efficiency of the internal control system if, taking into account the number of employees in the capital company, such a function is possible;
14.11 the requirements and procedure for regular revision of policies and procedures in relation to the prevention of money laundering and terrorism financing in compliance with changes in legislative acts or in the capital company's operational processes, the services provided, management structure, pool of customers or regions of operation.

15. The capital company shall asses on a regular basis at intervals of no more than 18 months the operational efficiency of the internal control system, including the revision and updating of the money laundering and terrorism financing risk assessment related to the customer, its state of residence (registration), the customer's business or personal activity, the services and products used and their supply channels and the transactions performed and, where necessary, the capital company shall take measures to improve the operational efficiency of the internal control system, including the revision and specification of policies and procedures for the prevention of money laundering and terrorism financing. The capital company shall assess the operational efficiency of its internal control system and implement measures for the improvement of the operational efficiency of the internal control system in each case where it has a reason to consider that the internal control system has deficiencies. The capital company shall, at Latvijas Banka's request, remedy the deficiencies identified in the internal control system as well as before it intends to introduce changes in its operational processes, the management structure, services and products provided, supply channels of services and products, pool of customers or geographical regions of operation, including prior to the introduction of new technologies or services.

IV. General requirements for customer due diligence

16. The capital company shall carry out customer due diligence in the following cases:
16.1 before entering into business relationship with the customer;
16.2 before the execution of the occasional transaction whose value or the total amount of several apparently related transactions exceeds 1 500 euro;
16.3 where a transaction complies with at least one of the indications included in the list of indications of unusual transactions or in case of suspicion of money laundering, terrorism financing or an attempt thereof.
16.4 when engaging in a transaction with the customer in relation to which and in relation to whose business or personal activity, the state of residence (registration) where its business or personal activity is performed, the transactions conducted, the services used or the ways they are provided the capital company has identified significant factors of increased risk;
16.5 when engaging in a transaction with a politically exposed person, a family member of a politically exposed person or a close associate of a politically exposed person;
16.6 in case of suspicion that the previously obtained customer due diligence data are unreliable.

17. Customer due diligence is a set of measures based on risk assessment; the capital company shall carry out the following activities within this set of measures:
17.1 identify the customer and check the obtained identification data;

17.2 clarify the identification information on the customer's beneficial owner and, based on the risk assessment, make sure that the respective natural person is the customer's beneficial owner;
17.3 obtain information on the purpose and intended nature of the business relationship or occasional transaction;
17.4 conduct monitoring of the transactions performed by the customer, including scrutiny of transactions to ensure that the transactions conducted are consistent with the capital company's knowledge of the customer, its business activity, risk profile and the source of funds;
17.5 ensure the storage, regular assessment and updating of the documents, personal data and information obtained during the process of customer due diligence in accordance with the inherent risk at intervals of no more than five years.

18. The capital company, when determining the extent of and procedure for customer due diligence as well as the regularity of the assessment of the documents, personal data and information obtained during the customer due diligence, shall take into account the money laundering and terrorism financing risk factors describing the customer, its state of residence (registration), the customer's business or personal activity, the services and products used and their supply channels and the transactions performed.

19. When determining the extent and regularity of customer due diligence, the capital company shall take into account the following indicators affecting the money laundering and terrorism financing risk:
19.1 the purpose of business relationship;
19.2 the regularity of the transactions planned and performed by the customer;
19.3 the duration of business relationship and regularity of transactions;
19.4 the volume of the transactions planned and performed by the customer.

20. Within the framework of customer due diligence, the capital company shall as a minimum carry out the following activities:
20.1 check the lists of persons (developed by the countries recognised by the Cabinet of Ministers or drawn up by international organisations and published on the website maintained by the Office for Prevention of Laundering of Proceeds Derived from Criminal Activity) suspected of involvement in terrorist activities as well as check other information available to make sure that the customer or its beneficial owner is not involved in money laundering or terrorist activities;
20.2 obtain information on the customer's business or personal activity;
20.3 establish whether the customer or its beneficial owner is a politically exposed person, a family member of a politically exposed person or a close associate of a politically exposed person by using publicly available information and that provided by the customer;
20.4 establish, as far as possible, through publicly available information whether the customer, its authorised representative or its beneficial user has previously been punished for or suspected of fraudulent activities, money laundering, terrorism financing or an attempt thereof.

21. The capital company shall be able to prove that the extent of its customer due diligence is in compliance with the money laundering and terrorism financing risk involved.

22. Where the capital company is not able to carry out the customer due diligence measures referred to in Paragraphs 17.1–17.3 herein in the cases referred to in

Paragraph 16 herein and it has no grounds to apply the simplified customer due diligence procedure, the capital company shall not enter into business relationship with such a customer, shall put an end to the commenced business relationship as well as shall not perform an occasional transaction. The capital company shall document and assess any such case and notify the Office for Prevention of Laundering of Proceeds Derived from Criminal Activity of any suspected money laundering or terrorism financing activity.

V. Procedure for customer identification and verification of customer identification data

23. The capital company shall identify a natural person based on the following personal identification documents and shall make copies thereof:
23.1 regarding a resident: a passport or an identity card according to the Personal Identification Documents Law;
23.2 regarding a non-resident: a personal identification document valid for entering the Republic of Latvia.

24. When verifying a natural person's identity based on the customer's personal identification document, the capital company shall make sure that the personal identification document has not been included in the Invalid Document Register.

25. The capital company shall identify a legal person or a legal arrangement based on the documents referred to in the Law on the Prevention of Money Laundering and Terrorism Financing. The capital company may identify a legal person or a legal arrangement by obtaining information regarding the legal person or the legal arrangement from a publicly available, reliable and independent source.

26. Where, in addition to the documents submitted by the customer, the capital company uses other sources of information to identify the customer, the capital company shall document the used source of information and the data received from that source.

27. When identifying the customer, the capital company shall establish whether the customer enters the business relationship or performs the occasional transaction on its own behalf or on behalf of another person. Where the customer is represented by an authorised representative, the capital company shall identify the authorised representative in accordance with the procedure set out in Paragraph 23 herein and shall verify its right to represent the customer by obtaining a document or a copy of the relevant document attesting to its right to represent the customer.

VI. Determination of a beneficial owner and ascertainment of the appropriateness of the determined beneficial owner

28. Where customer due diligence has to be applied, the capital company shall determine the beneficial owner of the customer, and shall, on the basis of the risk assessment, carry out the necessary measures in order to ascertain that the determined beneficial owner is the beneficial owner of the customer.

29. When determining the beneficial owner of the customer, the capital company shall obtain the following information:

29.1 regarding a resident: name, surname, personal identity number, the date, month and year of birth, nationality, the country of residence as well as the proportion of the customer's beneficial interest or shares controlled directly or indirectly and owned by the person, including direct or indirect participation, in the total amount, as well as the type of the customer's control to be implemented directly or indirectly;
29.2 regarding a non-resident: name, surname, the date, month and year of birth, number and date of issue of the personal identification document, state and authority which has issued the document, nationality, the country of residence as well as the proportion of the customer's beneficial interest or shares controlled directly or indirectly and owned by the person, including direct or indirect participation, in the total amount, as well as the type of the customer's control to be implemented directly or indirectly.

30. The capital company may determine the beneficial owner in at least one of the following ways:
30.1 by receiving a statement on the beneficial owner confirmed by the customer;
30.2 by using information or documents from the information systems of the Republic of Latvia or foreign countries;
30.3 by determining the beneficial owner independently if the information on him/her cannot be obtained in any other way.

31. Where the capital company has employed all possible means of determining the beneficial owner and has established that it is not possible to identify any natural person that would correspond to the definition of the term "beneficial owner" provided for in the Law on the Prevention of Money Laundering and Terrorism Financing and any doubts that the legal person may have another beneficial owner have been ruled out, the capital company, by appropriately justifying and documenting the activities carried out to determine the beneficial owner of the customer, may establish that the beneficial owner of the legal person is a person holding a position in the highest administrative institution of the legal person.

VII. Simplified customer due diligence

32. Where money laundering and terrorism financing risk is low and measures have been taken to identify, assess and understand its own procedures and the money laundering and terrorism financing risks associated with the customer, in the cases referred to in Paragraph 33 herein the capital company has the right to perform simplified due diligence by way of the following:
32.1 customer identification procedures referred to in Section V herein;
32.2 customer due diligence measures referred to in Section IV herein to the extent appropriate for the business relationship or the specifics of the occasional transaction and the level of the money laundering and terrorism financing risks.

33. The capital company has the right to perform simplified due diligence in the following cases:
33.1 the customer is a derived public person of the Republic of Latvia, a direct or indirect public administration institution or a capital company controlled by government or local government with a low money laundering and terrorism financing risk exposure;
33.2 the customer is an economic operator whose shares are admitted to trading on the regulated market in one or several European Union countries;
33.3 when carrying out a transaction referred to in Paragraph 16.2 herein where:

33.3.1 the transaction does not correspond to indications listed on the list of indications of unusual transactions;
33.3.2 the transaction neither causes any suspicion nor there is any information available testifying to money laundering and terrorism financing or attempts to perform the above activities;
33.3.3 the customer's business is not established in high-risk third countries.

34. Simplified customer due diligence shall not be applied where, based on risk assessment, the capital company identifies that it has information on money laundering and terrorism financing, attempt to perform such actions, or an increased risk of such actions at its disposal, inter alia if risk increasing factors, as defined herein, exist.

35. When performing simplified customer due diligence, the capital company shall obtain and document information testifying to the fact that the customer meets the provisions of Paragraph 33 herein.

VIII. Enhanced customer due diligence

36. Enhanced customer due diligence means risk assessment-based actions that the capital company shall conduct in addition to customer's due diligence, inter alia to make sure once more that the natural person, identified as the beneficial owner, is the customer's beneficial owner, and to ensure enhanced monitoring of the customer's transactions.

37. The capital company has an obligation to perform enhanced due diligence in the following cases:
37.1 upon entering into and maintaining a business relationship or conducting an occasional transaction with a customer who has not participated in person in the identification procedure, except cases where the following conditions apply:
37.1.1 the capital company ensures appropriate measures mitigating money laundering and terrorism financing risks, inter alia development of policies and procedures and staff training regarding off-site identification;
37.1.2 customer's identification by way of technology solutions comprising video identification or a secure digital signature, or other technology solutions is carried out in the extent and according to the procedure established by the Cabinet of Ministers;
37.2 upon entering into and maintaining a business relationship or conducting an occasional transaction with a customer who is or whose beneficial owner is a politically exposed person, a family member of a politically exposed person or a person closely linked with a politically exposed person;
37.3 in other cases upon entering into and maintaining a business relationship or conducting an occasional transaction with a customer where a higher risk of monetary laundering or terrorism financing exists.

IX. Procedure for entering into and maintaining a business relationship with a politically exposed person, a family member of a politically exposed person and a close associate of a politically exposed person

38. The capital company shall document the procedure whereby it determines whether the customer or its beneficial owner is a politically exposed person, a family member of a politically exposed person or a close associate of a politically exposed person.

39. Before entering into a business relationship with a customer who is or whose beneficial owner is a politically exposed person, a family member of a politically exposed person or a close associate of a politically exposed person, the staff member of the capital company shall notify the Board (where one exists) of the capital company or a specifically authorised Board member of the capital company, or a staff member of the capital company with sufficient knowledge of the capital company's money laundering and terrorist financing risk exposure and sufficient seniority to take decisions affecting its risk exposure, on entering into business relationship with a politically exposed person, a family member of a politically exposed person or a close associate of a politically exposed person and receives approval from the Board of the capital company, the specifically authorised Board member of the capital company, or the staff member of the capital company meeting the above criteria on entering into a business relationship.

40. Where before entering into or during the business relationship it is identified that the customer or its beneficial owner is a politically exposed person, a family member of a politically exposed person or a close associate of a politically exposed person, the capital company shall take and document risk assessment-based measures to determine the sources of the funds and wealth characterising the financial situation of the politically exposed person, a family member of a politically exposed person or a close associate of a politically exposed person.

41. The capital company maintaining a business relationship with a politically exposed person, a family member of a politically exposed person or a close associate of a politically exposed person shall conduct ongoing monitoring of the customer's transactions.

42. On the basis of risk assessment, the capital company shall discontinue applying enhanced customer due diligence associated with its status of a politically exposed person, a family member of a politically exposed person or a close associate of a politically exposed person in the following cases:
42.1 the politically exposed person dies;
42.2 the politically exposed person is no longer entrusted with a prominent public function for at least 12 months and the person's business relationships no longer pose an increased risk of money laundering.

X. The right to discontinue customer due diligence

43. The capital company has the right to discontinue the customer due diligence where it has suspicion of money laundering or terrorism financing and it is reasonably deemed that further application of customer due diligence measures may reveal the capital company's suspicion to the customer.

44. Where the customer due diligence is discontinued as per Paragraph 43 herein, the capital company shall report a suspicious case to the Office for Prevention of Laundering of Proceeds Derived from Criminal Activity. In its report to the Office for Prevention of Laundering of Proceeds Derived from Criminal Activity, the capital company shall also point out its considerations serving as a basis for the conclusion that further application of customer due diligence measures may reveal the capital company's suspicion to the customer.

XI. Monitoring of customer transactions and detection of unusual and suspicious transactions

45. The capital company shall ensure ongoing monitoring of the customer transactions: business relationships and occasional transactions, including scrutiny of transactions to ensure that the transactions being conducted are consistent with the capital company's knowledge of the customer, the business or personal activities, risk profile, and the source of funds. The capital company shall update the information on the customer, its business or personal activities, risk profile and source of funds on an ongoing basis.

46. As part of the monitoring of customer transactions, the capital company shall analyse customer transactions on an ongoing basis to make sure that they do not cause suspicion of money laundering or terrorism financing.

47. The capital company shall document the procedure of customer transaction monitoring, inter alia defining the frequency of customer transaction monitoring, the actions/procedures to be performed as part of the customer transaction monitoring and type of registering the performance of the actions/procedures, as well as appoint a person responsible for the customer transaction monitoring.

48. When monitoring business relationships or occasional transactions, the capital company shall pay particular attention to the following:
48.1 an unusually large transaction for the customer; a complex transaction; transactions appearing to be mutually related; or a transaction with no apparent economic or explicitly lawful purpose;
48.2 a transaction with a person established in high-risk third countries.

49. On the basis of information obtained during customer due diligence and information provided by the Office for Prevention of Laundering of Proceeds Derived from Criminal Activity and other law enforcement authorities, the capital company shall establish enhanced monitoring measures for customer transactions, e.g.:
49.1 transactions with customers shall be exclusively subject to an approval by the Board (where one exists) of the capital company or a specifically authorised Board member of the capital company, or a staff member of the capital company with sufficient knowledge of the capital company's money laundering and terrorist financing risk exposure and sufficient seniority to take decisions affecting its risk exposure;
49.2 customer transaction limits;
49.3 enhanced analysis of customer transactions;
49.4 other type of monitoring measures or restrictions/limitations.

50. In line with its risk assessment of money laundering and terrorism financing, the capital company shall define and document indications of a suspicious transaction.

XII. Refraining from executing a transaction

51. The capital company shall document the procedure under which its employees shall act upon establishing that the transaction proposed by a customer or commenced by the capital company is associated with or there are substantiated suspicions that it is associated with money laundering or terrorism financing, or there are substantiated suspicions that the funds are directly or indirectly obtained as a result of a criminal offence or are associated with terrorism financing, or an attempt of a criminal offence.

52. Where a transaction is associated with or there are substantiated suspicions that it is associated with money laundering or terrorism financing, or there are substantiated suspicions that the funds are directly or indirectly obtained as a result of a criminal offence or are associated with terrorism financing, or an attempt of a criminal offence, the capital company shall take a decision to refrain from executing the transaction by retaining the funds and notifying the Office for Prevention of Laundering of Proceeds Derived from Criminal Activity thereof immediately but no later than on the next business day.

53. When refraining from executing a transaction, the capital company shall not carry out any actions with the funds involved in the transaction until the moment an order of the Office for Prevention of Laundering of Proceeds Derived from Criminal Activity is received to terminate refraining from executing a transaction.

54. Where the Office for Prevention of Laundering of Proceeds Derived from Criminal Activity has issued an order to freeze the retained funds, the capital company shall act pursuant to the procedure stipulated by Chapter V of the Law on the Prevention of Money Laundering and Terrorism Financing.

55. Where refraining from executing a transaction, in relation to which there are substantiated suspicions that it is associated with money laundering or terrorism financing, may serve as information that would assist the persons involved in money laundering or terrorism financing in avoiding liability, the capital company may execute the transaction, reporting it to the Office for Prevention of Laundering of Proceeds Derived from Criminal Activity immediately after the execution of the transaction.

XIII. Registering customer transactions, reporting unusual and suspicious transactions as well as storing and destructing information and documents

56. The capital company shall document the procedure for registering, storing and protecting the data on the capital company's customers, their beneficial owners and customer transactions as well as the procedure for providing data on unusual and suspicious transactions to the Office for Prevention of Laundering of Proceeds Derived from Criminal Activity.

57. Upon establishing an unusual or suspicious transaction, a capital company shall submit a report to the Office for Prevention of Laundering of Proceeds Derived from Criminal Activity pursuant to the requirements set out in the Law on the Prevention of Money Laundering and Terrorism Financing.

58. The capital company shall immediately submit the report referred to in Paragraph 57 herein to the Office for Prevention of Laundering of Proceeds Derived from Criminal Activity according to the procedure established by the Cabinet of Ministers Regulations prescribing the list of unusual transaction indications and the procedures for submitting reports on unusual or suspicious transactions, and approving the report form.

59. The capital company shall not be entitled to inform a customer or a third party that information on a customer or a transaction executed, proposed, commenced or deferred by a customer has been reported to the Office for Prevention of Laundering of Proceeds Derived from Criminal Activity.

60. The capital company shall ensure the availability of all information related to the internal control system of the capital company and the documents referred to in Paragraph 56 herein to Latvijas Banka.

61. The capital company shall register and keep records of the requests from the Office for Prevention of Laundering of Proceeds Derived from Criminal Activity on the capital company's customers, their beneficial owners and the transactions executed, proposed, commenced or deferred by the customers.

62. The capital company shall ensure the storage of the copies of the documents and information on a person obtained in the process of the customer due diligence and during the monitoring of the customer's transactions, including the reports submitted to the Office for Prevention of Laundering of Proceeds Derived from Criminal Activity, for a period of five years following the date on which the capital company has terminated the business relationship with the customer or the date on which it has executed the last registered occasional transaction.

63. Upon expiry of the deadline for the storage of documents and information referred to in Paragraph 62 herein, a capital company shall destroy the documents and information on a person, unless it receives an instruction to extend the above time period pursuant to the provisions stipulated in the Law on the Prevention of Money Laundering and Terrorism Financing. Where a capital company receives such an instruction, it shall destroy the documents and information on a person upon expiry of the deadline referred to in the instruction; the new deadline may not exceed that referred to in Paragraph 62 by more than five years.

XIV. Internal control system requirements for the rights, duties and the liability of employees

64. The capital company's board, where one exists, or the highest administrative institution of the capital company shall ensure efficient implementation of the internal control system in the day-to-day work.

65. The capital company's board, where one exists, or the highest administrative institution of the capital company shall appoint a board member or a responsible representative of the highest administrative institution for monitoring the prevention of money laundering and terrorism financing in the capital company, and the capital company shall notify Latvijas Banka to that effect within 30 days.

66. The capital company shall appoint one or several employees entitled to take decisions and directly liable for the compliance with the requirements of the Law on the Prevention of Money Laundering and Terrorism Financing and for ensuring the exchange of information with Latvijas Banka. The capital company shall notify Latvijas Banka of the appointment of a responsible employee within 30 days after the entry into force of the licence issued by Latvijas Banka for buying and selling cash foreign currencies or changes in the composition of employees.

67. The capital company shall be prohibited to disclose information regarding the appointed responsible employee to third parties.

68. The responsible employee of the capital company:

68.1 shall be familiar with the requirements of the legal acts governing the prevention of money laundering and terrorism financing and the risks related to money laundering and terrorism financing;
68.2 shall update the capital company's board or the highest administrative institution of the capital company regarding the operation of the internal control system on a regular basis and, where necessary, shall submit proposals for the improvement of the internal control system's operation.

69. The responsible employee of the capital company shall have the following responsibilities:
69.1 ensuring the operation of the capital company's internal control system;
69.2 informing and training the capital company's employees in matters related to the internal control system's operation as well as ensuring the efficiency of the training;
69.3 ensuring the monitoring of customer transactions;
69.4 reporting unusual and suspicious transactions to the Office for Prevention of Laundering of Proceeds Derived from Criminal Activity;
69.5 ensuring the storage and protection of the information and documents obtained in the process of the customer due diligence and during the monitoring of the customer's transactions, as well as their destruction upon expiry of the deadline for their storage;
69.6 registering, keeping records of and protecting the requests from the Office for Prevention of Laundering of Proceeds Derived from Criminal Activity on the capital company's customers and customer transactions.

70. The employee of the capital company executing transactions with customers shall have the following responsibilities:
70.1 carrying out the customer due diligence and registering the customer transactions;
70.2 identifying unusual or suspicious transactions and notifying the responsible employee of the capital company of the identified unusual and suspicious transactions.

XV. Internal control system requirements for ensuring the professional qualifications of the capital company's employees and standards for compliance

71. The capital company shall ensure the following:
71.1 training for the recently hired capital company's employees in matters related to the internal control system;
71.2 ongoing training for employees and possibilities to improve their professional skills in matters related to the internal control system on a regular basis.

72. The training referred to in Paragraph 71.2 herein shall be conducted at least once a year and cover the following subjects:
72.1 the legal acts governing the prevention of money laundering and terrorism financing;
72.2 the risks related to money laundering and terrorism financing;
72.3 the operating framework of the capital company's internal control system;
72.4 the identification of unusual and suspicious transactions.

73. The capital company shall document the data on the conducted training. The fact that the employee has participated in the training referred to in Paragraph 71 herein shall be confirmed by the signature of the employee who has received the training. The fact that the responsible employee of the capital company has verified the efficiency of the training and has assessed the level of knowledge of the employee who has received the

training with regard to matters referred to in Paragraph 72 herein shall be confirmed by the signature of the responsible employee.

XVI. Internal control system requirements for anonymous internal reporting on violations of the requirements of the legal acts governing the prevention of money laundering and terrorism financing

74. The capital company shall establish and document the procedure whereby the employees of the capital company may submit anonymous internal reports on violations of the requirements of the legal acts governing the prevention of money laundering and terrorism financing in the capital company.

75. The capital company may be exempt from the obligation to establish the procedure provided for in Paragraph 74 herein where, upon establishing the internal control system or assessing its operational efficiency, the capital company assesses that anonymous internal reporting on violations of the requirements of the legal acts governing the prevention of money laundering and terrorism financing is not possible in the capital company due to the number of employees. The capital company shall document the above assessment and its justification.

76. Where the capital company has established the procedure provided for in Paragraph 74 herein, it shall document the procedure for assessing the anonymous internal reports on violations of the requirements of the legal acts governing the prevention of money laundering and terrorism financing in the capital company.

XVII. Internal control system requirements for an independent internal audit function

77. The capital company shall establish and document the procedure for conducting an independent internal audit function in the capital company to ensure the compliance of the capital company's internal control system with the requirements of the legal acts governing the prevention of money laundering and terrorism financing and the assessment of the internal control system's operational efficiency.

78. The capital company may be exempt from the obligation to establish the procedure provided for in Paragraph 77 herein where, upon establishing the internal control system or assessing its operational efficiency, the capital company assesses that the introduction of an independent internal audit function is not possible due to the number of employees. The capital company shall document the above assessment and its justification.

XVIII. Final provisions

79. Regulation No. 141 "Requirements for the Prevention of Laundering the Proceeds from Criminal Activity (Money Laundering) and of Terrorist Financing when Purchasing and Selling Cash Foreign Currencies" of the Council of Latvijas Banka of 15 September 2014 (Latvijas Vēstnesis, 2014, No. 183; 2016, No. 45 and No. 52) shall be deemed invalid.

80. Capital companies shall ensure the compliance of their internal control systems with the requirements of the present Regulation and other legal acts governing the prevention of money laundering and terrorism financing until 1 January 2018. The assessments of

money laundering and terrorism financing risk approved by the capital companies and the documents describing the internal control systems' policies and procedures shall be submitted to Latvijas Banka until 10 January 2018.

81. The Regulation shall take effect simultaneously with the enactment of amendments to the Law on the Prevention of Money Laundering and Terrorism Financing, providing for the implementation of Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, and Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March of 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA.

Governor of Latvijas Banka Ilmārs Rimšēvičs